EUROPEAN UNION AGENCY
FOR CYBERSECURITY

2021 REPORT ON CSIRT-LE COOPERATION

A study of the roles and synergies among sixteen selected EU/EEA Member States

MARCH 2022

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[1]

Domenico Ferrara (ENISA), Pauline Massart (CEIS - Avisa Partners), Suzanne Mc Namara (CEIS - Avisa Partners), Silvia Portesi (ENISA)

This report is an updated and extended version of the ENISA *2020 Report on CSIRT-LE Cooperation: A Study of Roles and Synergies among Selected EU Member States/EFTA Countries*, available at https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation/, whose authors are (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:

- Persons and organisations listed in the Acknowledgements section of the ENISA *2020 Report on CSIRT-LE Cooperation: A study of roles and synergies among selected EU Member States/EFTA countries*, available at https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation/, of which this current report is and updated and extended version.

- 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:
  - Anita Veternik, State Prosecutor's Office, Slovenia;
  - Carlos Abad, Carlos Córdoba, CCN-CERT, Spain;
  - Eleliis Rattam, Prosecutor General's Office, Estonia;
  - Gorazd Božič, SI-CERT, Slovenia;
  - Jan Wikholm, NCSC-FI, Finland;
  - Jorge Chinea López, INCIBE-CERT, Spain;
  - Kamil Nieradkiewicz, CSIRT NASK, Poland;
  - Michaël De Laet, Federal Computer Crime Unit, Belgium;

[1] The authors are listed in alphabetical order by surname.

- Oskar Gross, Cybercrime Unit, Estonian Criminal Police, Estonia;
- Pasi Vainio, Prosecution District of Western Finland, Finland;
- Robrecht De Keersmaecker, Prosecutor-General's Office, Belgium;
- Teresa Magno, Eurojust, Italy, whose contributions are her personal views only and do not engage anybody else;
- Tuomas Soosalu, Prosecution District of Southern Finland, Finland;
- Tõnu Tammer, CERT-EE, Estonia.

- All of the subject matter experts/organisations who, in addition to ENISA experts, peer reviewed the report or parts of the report, or were involved in the validation process including:
  - CSIRTs Network;
  - Álvaro Azofra Martínez and Gert Jan van Hardeveld, Europol's EC3.

- The ENISA colleagues who provided input and reviewed the report.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-541-8 DOI: 10.2824/594421

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 is an extended and updated version of the *2020 Report on CSIRT-LE Cooperation: A Study of Roles and Synergies among Selected EU Member States/EFTA Countries* published in January 2021 (ENISA, 2021a) and referred to as "2020 Report on CSIRT-LE cooperation", and follows a number of previous reports published by the European Union Agency for Cybersecurity 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 addressed the legal and organisational framework, roles and duties of CSIRTs, LEAs and the Judiciary, 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. This report presents a detailed and updated analysis focusing on sixteen EU/EEA Member States namely Belgium, Czechia ([2]), Estonia, Finland, France, Germany, Ireland, Italy, Luxembourg, Norway, Poland, Portugal, Romania, Slovenia, Spain, and Sweden ([3]).

The data for this report were collected via desk research and interviews with subject-matter experts using the methodology developed and presented in the 2020 ENISA Report on CSIRT-LE cooperation. The data collected showed, among other things, that:

- The communities make efforts to avoid interferences 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.
- The main challenge experienced by the experts interviewed in cooperating with the other communities seems to remain the difficulty to sometimes "speak the same languages", especially between the CSIRTs (technical) and Judiciary (legal) communities.
- 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. Such activities help enhance overall the knowledge and competences required to respond to cybercrime.
- While there has been no significant impact of the COVID-19 pandemic on the cooperation and interaction between the three communities and their ability to function, in the long run the lack of networking opportunities fostered by face-to-face meetings might have an impact on the relationship between the three communities, which is mainly based on trust and personal contacts.

([2]) Czechia has been the short-form name for the Czech Republic since 2016.
([3]) While Czechia, France, Germany, Luxembourg, Norway, Portugal, Romania and Sweden were already analysed in the 2020 ENISA Report on CSIRT-LE Cooperation (ENISA, 2021a), the current report presents an analysis also focused on the additional Member States: Belgium, Estonia, Finland, Ireland, Italy, Poland, Slovenia and Spain.

1. INTRODUCTION

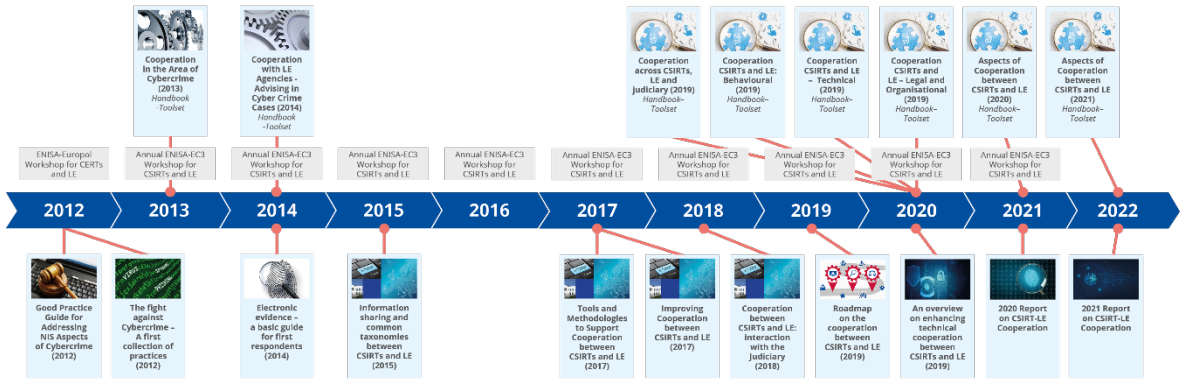
1.1. BACKGROUND OF THE REPORT

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.

This report is an extended and updated version of the *2020 Report on CSIRT-LE Cooperation: A study of roles and synergies among selected EU Member States/EFTA countries* (ENISA, 2021a) published in January 2021.The parts on countries already covered in the 2020 report (Czechia, France, Germany, Luxembourg, Norway, Portugal, Romania and Sweden) are reproduced in this report, with some minor changes.

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 ([4]).

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



This current report (as well as the 2020 report) and the ENISA training material on CSIRT-LE cooperation ([5]) are a set of deliverables complementing each other as follows:

- The present report analyses roles, duties, competences, synergies and potential interferences across the three communities (CSIRTs, LE and Judiciary) in sixteen additional MSs.

([4]) 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).
([5]) The ENISA training material on CSIRT-LE cooperation is available on the ENISA website under: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/legal-cooperation

- The training material helps a trainer explain these concepts, e.g. through scenarios and contains exercises for trainees based on these scenarios.

1.2. REPORT OBJECTIVES

The main objective of this report is to present 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. By facilitating the cooperation between the CSIRT and the LE communities and the interaction with the Judiciary, this work has the final aim to contribute to better respond to cybercrime, which, as reaffirmed at the Octopus Conference on Cybercrime organised by the Council of Europe in November 2021, affects significantly the individuals and 'often represents a serious interference with the rights and lives of victims' (Council of Europe, n.d.g).

1.3. REPORT SCOPE

The report focuses on the cooperation of national and governmental (n/g) CSIRTs ([6]) with LEAs, although most of the analysis is largely applicable to CSIRTs in general (i.e. other than n/g CSIRTs). Military CSIRTs are mentioned too but only if they play a specific role in CSIRT-LE cooperation in case of cybercrime (e.g. if they act as national CSIRTs).

No specific sector is targeted in this report and 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).

Following the methodology presented in the *2020 Report on CSIRT-LE Cooperation: A study of roles and synergies among selected EU Member States/EFTA countries* (ENISA, 2021a)([7]), an analysis has been conducted and presented in Chapter 2 below.

The analysis presented in this current report covers sixteen EU/EEA countries. Eight countries were already analysed and presented in the 2020 report: Czechia, France, Germany, Luxembourg, Norway, Portugal, Romania and Sweden. The additional countries analysed in the current report are Belgium, Estonia, Finland, Ireland, Italy, Poland, Slovenia and Spain.

The general geographical scoping of the report is limited to sixteen EU/EFTA countries. This selection of countries was based on the following criteria:

- geographical balance;
- balance of different political systems;
- balance of different legal systems;
- balance in terms of size (area and population) of the countries;
- balance in terms of maturity of the n/g CSIRTs;
- 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.

([6]) '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).
([7]) See in particular its Chapter on "Proposed methodology", p.16ff.

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]);
- 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.

1.5. DATA COLLECTION METHODS

The methodology used to collect data for this report is fully outlined in Chapter 3 “Proposed methodology” (p.16ff) of the 2020 Report on CSIRT-LE cooperation (ENISA, 2021a).

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;
- Segregation of Duties (SoD) matrix.

A summary of the desk research per country is included in Annex A of this report. A list of courses and training programmes for LE, Judiciary and CSIRTs (not exhaustive and not containing national training initiatives) is provided in Annex B of this report.

In addition to the desk research, the country profile analysis was based on interviews with CSIRTs, LE and some Judiciary representatives, which included also the filling in of the SoD matrix. Contributions from the interviewees are acknowledged in the report. However, the following points should be noted:

- Some interviewees requested not to be named in the report. In order to ensure consistency, the names of all the other interviewees have been omitted;
- Interviewees provided their contributions based on their knowledge and expertise and were mainly not acting as representatives of their country;
- Concerning Italy, due to an important ongoing reform and the creation of a new National Cybersecurity Agency, it was challenging to collect data via interviews with the CSIRTs and with the LE, at this specific point in time. Therefore, the analysis for

([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).
([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.

Italy has been conducted based on one interview only and on the data collected via desk research;

- Due to time constraint, few interviewees, provided data by filling the questionnaire in writing, instead of via a video/phone interview. Few others preferred to fill the SoD matrix and send it separately via email instead of filling it in during the interview.

The cut-off date for data collection was 3rd August 2021; however, some additional input received between August and October 2021 was also integrated in this report.

2. COUNTRY FOCUS

This chapter presents the analysis of the data collected by using the methodology outlined in the 2020 Report on CSIRT-LE cooperation published in January 2021 (ENISA, 2021a).

The analysis addressed the following MSs/EEA countries:

- Belgium;
- Czechia;
- Estonia;
- Finland;
- France;
- Ireland;
- Italy;
- Germany;
- Luxembourg;
- Norway;
- Poland;
- Portugal;
- Romania;
- Slovenia;
- Spain;
- Sweden.

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

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.

The parts on countries already covered in the 2020 report (Czechia, France, Germany, Luxembourg, Norway, Portugal, Romania and Sweden) are reproduced in this report, with some minor changes.

2.1. BELGIUM

Belgium is a 'federal constitutional monarchy in which the king is the head of state and the prime minister is the head of government in a multi-party system. Decision-making powers are not centralised, but divided between 3 levels of government: the federal government, 3 language-based communities (Flemish, French and German-speaking) and 3 regions (Flanders, Brussels Capital and Wallonia). Legally they all are equal, but have powers and responsibilities for different fields' (European Union, n.d.a).

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

Belgium published its National Cyber Security Strategy 2.0 2021-2025 in May 2021 (CCB, 2021) and legislation that transposes the EU NIS Directive (Law No 2019011507) in 2019 (CCB, 2019).

Belgium ratified the Budapest Convention in 2012.

2.1.1. Roles and duties

In Belgium, 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)
Centre for Cyber Security Belgium	Centre pour la Cybersécurité Belgique	CCB
- **Federal Computer Emergency Response Team**	Computer Emergency Response Team Fédérale	CERT.be
Police	Police / Politie	
- **Federal Computer Crime Unit**	Federal Computer Crime Unit	FCCU
- **Regional Computer Crime Units**	Regional Computer Crime Units	RCCU
- **Local Computer Crime Units**	Local Computer Crime Units	LCCU
Federal Public Service for the Economy	Service Public Fédéral Economie	
Public Prosecution Services	Ministère public	

2.1.1.1. National cybersecurity agency

Created in 2014, the **Centre for Cybersecurity Belgium** is the central authority for cybersecurity in Belgium, under the authority of the Prime Minister. It is in charge of the Belgian national cybersecurity policy and of the management of CERT.be, the national CSIRT (CERT.be, n.d).

The CCB's main tasks are inter alia:

- 'Monitoring, coordinating and supervising the implementation of Belgian policy on the subject; […]
- Ensuring coordination between the relevant government departments and governments, as well as the public authorities and the private or scientific sectors;
- Formulating proposals aimed at adapting the regulatory framework in the field of cyber security;
- Ensuring crisis management in case of cyber incidents in cooperation with the government's Coordination and Crisis Centre;

- Preparing, disseminating and supervising the implementation of standards, guidelines and security standards for the various information systems of the governments and public institutions; […]' (CCB, n.d.).

The Belgian NCSS states that the CCB, 'in collaboration with CERT.be, in its quality of national CSIRT, is in charge of detecting and analysing cybersecurity problems and vulnerabilities and of informing the users, with the support of Internet services providers' (CCB, 2021).

'All entities may report [to CCB], on a voluntary basis, incidents that have a significant impact on the continuity of the services they provide. This voluntary notification does not have the effect of imposing obligations on the notifying entity that it would not have been subject to if it had not made the notification. When processing a notification, the CCB may nevertheless give priority to mandatory notifications imposed by the NIS Act over voluntary notifications' (CCB, n.d. a).

By law, in the course of a cybercrime investigation, the CCB can be appointed as a judicial expert. The CCB then provides technical expertise to the Police and both the police and the CCB can share all the necessary information. Guidelines on how to appoint the CCB as an expert during criminal investigations is being set up by the Public Prosecution Services. Criteria are mentioned in the guidelines to determine in which situations the CCB can be appointed as an expert, for example the level of complexity or the severity of the impact of the incident.

However, one of the experts interviewed explained that the CCB has no obligation and can refuse to be appointed as an expert. Moreover, according to one of the interviewees, the CCB has in reality rarely been appointed as an expert.

As highlighted by one of the interviewees, the Belgian criminal procedure system is a written-evidence based system: written statements are read by the court during a trial, but witnesses are not called to court in person. The Belgian CSIRT can be called as a witness, but testifies only via written statements.

The **Cyber Emergency Plan** (CCB, n.d. c) describes who can report an incident and how the relevant stakeholders coordinate in the event of an incident, depending on the level of severity of the incident:

- Level 1: there is one attack, usually not too complex, with only one victim involved;
- Level 2: the incident is not necessarily complex but has an impact at the national level, with multiple victims;
- Level 3: the incident is a complex attack that leads to a very severe national crisis.

In case of very severe national crisis (complex cyberattack, with major impact on the Belgian citizens), reaching the level 3 of the Cyber Emergency Plan, the CCB acts as the coordinator of all the involved actors (the CCB, the Crisis Centre, intelligence agencies, the FCCU, the federal prosecutor).

2.1.1.2. CSIRTs

Belgium's national CSIRT, **CERT.be**, was established in 2009. It is the operational service of the CCB. Its task is to detect, observe and analyse online security problems and to inform target groups accordingly. It also publishes news on current cyberthreats, as well as various reports and guidelines on the matter.

CERT.be delivers services to operators of essential services (OES) and critical infrastructures, government services, public administrations, businesses and general public (CERT.be, n.d).

As a government service, according to article 29 of the Belgian Code of Criminal Procedure, the CSIRT should notify the prosecutions services of any crime it has knowledge of. Yet, an interviewee reported that there might be exception due to the sometimes uncertain nature of the information related to cyber incidents. Moreover, as there are a lot of many minor cyber incidents, not all of them are systematically reported. However, when a national cyber incident occurs, the CSIRT must immediately notify the Federal Prosecutor's Office.

CERT.be is a member of the CSIRTs Network.

2.1.1.3. LE

The **Federal Computer Crime Unit (FCCU)**, attached to the directorate for the fight against serious and organised crime (DJSOC) of the Federal Police, is responsible for investigations connected to cyberattacks and other cyber offences.

At the federal level, the FCCU handles cases related to critical infrastructures and Operators of Essential Services (OES). If the case has a more local impact, it is more likely to be handled by the Regional Computer Crime Units (RCCU) (see below). One of the interviewees explained that by law the FCCU has to deal with cases related to critical infrastructures, however the distribution of other cases between FCCU and RCCU is decided on a case-by-case basis in coordination with the Federal Prosecutor's Office.

The **Regional Computer Crime Units (RCCU)** 'investigate cyber attacks and provide technical and legal support in non-specific crime investigations. RCCU staffing numbers are set by regional directors of the federal judicial police and vary' considerably (Council of the European Union, 2017g, p. 32).

Local Computer Crime Units (LCCUs) have been created by some Local Police zones ([12]).

The **Federal Public Service for the Economy** has a team of 'investigators assigned to prosecutions related to economic offences committed via the Internet' (Council of the European Union, 2017g, p. 32).

The Police response within the Cyber Emergency Plan of the CCB is provided by the Quick Reaction Force (QRF), made of FCCU and RCCU staff. According to the interviewees, the QRF has been put into action a few times, for example during the cyberattack on the Tournai hospital (January 2021) (RTBF, 2021). Although the case was mostly handled at the regional level, the QRF was tasked to gather evidence during the first week following the attack. The QRF was involved in a few other cases but only as advisor, and was not deployed.

Finally, Belgium is part of the Europol's Joint Cybercrime Action Taskforce (J-CAT) (Europol, n.d.c).

2.1.1.4. Judiciary

The **Public Prosecution Service** is composed of public prosecutors, who 'prosecute offenders in court, lead criminal inquiries, pursue perpetrators and call for the court to sentence suspects' (Council of the European Union, 2017g, p. 29).

One of the interviewees reported that each of the fourteen prosecutor's office has at least one cybercrime prosecutor, however also dealing with cases related to other types of crime. At the federal level, the Federal Prosecutor's Services has a dedicated cyber unit consisting in three prosecutors specialised in cybercrime, but also dealing with cases related to other types of crime. No prosecutor is exclusively dealing with cybercrime cases.

In 2008, a decision was taken by the College of Principal Public Prosecutors to have a minimum of one judge specialised in cybercrime within the public prosecutor's office, the principal public

([12]) See for instance the LCCU created by the Politiezone Regio Tielt (Belgian Police, n.d.).

prosecutor's office and the Federal Prosecutor's office. Cybercrime judges are expected to undertake specialist cybercrime training. Moreover, 'the College of Principal Public Prosecutors has created a **cybercrime experts' network** [emphasis added] with representatives of the federal, principal and first-instance public prosecutor's offices, the federal police (FCCU), the CCD and, by invitation, examining judges, to increase the relevant expertise of the Public Prosecution Service [and] facilitate communications' (Council of the European Union, 2017g, p. 30).

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

2.1.2. Synergies and potential interferences

The experts interviewed assessed the cooperation among CSIRT, LE and the Judiciary as overall very good. Complementary synergies are existing and fostered by good communication between the three communities. The information flow between the CSIRT, the FCCU and the Judiciary is very efficient and enhanced by a trusting relation. An informal chat group is existing between the three communities, which allows each of them to be immediately aware in case of a cyber incident, each community is aware immediately.

The prosecutor leading the investigation must appoint the CSIRT as an expert to allow for full cooperation and information sharing with the Police. According to one of the interviewees, this mechanism can be used for either 'regular' cases or in the framework of the Cyber Emergency Plan, but tends to be used more for the latter.

Regarding the Cyber Emergency Plan, the NCSS foresees that it 'continues to be operationalised. Through optimal cooperation between the CCB's national Computer Emergency Response Team (CERT.be), the Integrated Police Services and the National Crisis Centre (NCCN), incidents are dealt with quickly and effectively and legal investigations are immediately integrated' (CCB, 2021).

One of the experts interviewed underlined that in general 'the CSIRT assists the FCCU in terms of analytical capability when they are appointed as experts in a cybercrime case'. One specific synergy identified during the interviews is the technical complementarity between the CSIRT and the LE. For example, the CSIRT gathers indicators of compromise (IoC), which can be very useful for the Police's investigation.

Another strong synergy, as specified by one of the interviewees, is that the FCCU can identify who is behind IP addresses, upon request from the Public Prosecutor, whereas the CSIRT cannot legally do it. This led to the development of a workflow around C2 services (control & command used for malware/ransomware): CERT.be had a list of active C2 services in Belgium, so they knew the IP addresses from which the threats emanated, but could not identify who they belong to. In coordination with the Public Prosecutor, the FCCU set up a workflow where they could identify who is behind the IP addresses which were in possession of the CSIRT.

Moreover, every three months, all the relevant actors (the CCB, CERT.be, the Federal Prosecutor, Military Intelligence, the FCCU and the Crisis Centre) meet to discuss recent cases.

No major interferences and/or overlaps were experienced by the experts interviewed. The good communication between the three communities allows them to find a solution to potential differences of interest.

It was however underlined that there may sometimes be 'duplication of analysis if the CSIRT and the police have access to the same evidence and start analysing them at the same time'. Moreover, the loss of digital evidence might sometimes be the result of the prevention of further damage following a cyber incident. One interviewee stated that the 'decision [to potentially delete evidence to mitigate damage] should be balanced, taking into consideration all aspects' and specified that 'in the majority of cases, priority is given to the prevention of further damage'.

OPTIMAL COOPERATION TO DEAL WITH INCIDENTS QUICKLY AND EFFECTIVELY

'Through optimal cooperation between the CCB's national Computer Emergency Response Team (CERT.be), the Integrated Police Services and the National Crisis Centre (NCCN), incidents are dealt with quickly and effectively and legal investigations are immediately integrated' (CCB, 2021).

According to another interviewee, as the situation starts to calm down after a period of close cooperation (e.g. at the height of a crisis), it can sometimes take longer for the Police to obtain evidence or reports from the CSIRT as the incident is no longer the CSIRT's main focus.

Finally, as it emerged from one of the interviews, from the victim's point of view, 'it can sometimes be unclear who is in charge and who they should provide the evidence to, as they are sometimes asked to provide evidence twice, by both the CSIRT and the police'.

Despite good cooperation, challenges exist. As emerged from the data collected via interviews, 'Mutual understanding […] is sometimes lacking, more specifically [on] what the other community can and cannot do. More specifically, the CSIRT can sometimes encounter difficulties in understanding the legal process' and framework, and the prosecutors may have difficulties in understanding the technical aspects. However, to ease this challenge: CSIRT representatives and prosecutors participate in common courses, such as the SANS courses, offered by the CCB to federal actors (LE, Judiciary). One of the interviewees explained that these courses are very beneficial as they give prosecutors 'a very good understanding of most of the technical aspects' of cybercrime cases, which also allows them 'to take appropriate legal measures'.

One recommendation made by one of the interviewees to address the challenges the three communities could have in understanding each other was to set up common guidelines for cooperation between the CSIRT, the LE and the Judiciary.

2.1.3. Examples of training

The CCB provides technical training, but also training on the role and duties of the CCB. There are also joint training opportunities between the prosecutors and the CCB staff, so the latter can learn more about the legal aspects of cybercrime. Moreover, the CCB offers opportunities for the Judiciary to participate in the SANS courses (according to one of the experts interviewed, some nine prosecutors have participated and completed the course to date).

'Through the Federal Public Service Policy and Support, the Centre for Cyber Security Belgium (CCB) provides a specialised range of cybersecurity training courses. This involves thorough basic training as well as more specialised training in a specific field for federal public officials' (CCB, n.d. b).

The FCCU has participated in several tabletop exercises with the CSIRT, the Judiciary and military intelligence. According to one interviewee, a large tabletop exercise took place a few years ago to test what would happen if a major cyberattack occurred during elections.

In addition, in 2019, the FCCU made a substantial contribution to European training projects on the dark web, organised under the aegis of the European Police College (CEPOL). Two sessions were organised, in which about sixty LEA representatives from different European countries took part. That same year, after an interlude of a few years, the FCCU organised a training course for the Computer Crime Unit functional certificate. Since then, around sixty people have taken the basic module (Federal Police, 2019).

For the Judiciary, the Belgian Institute for Judicial Training has set up a three-level cybercrime training for new prosecutors, to which CSIRT, FCCU and RCCUs representatives are invited on a regular basis as speakers:

1. Basic cybercrime training, for all judicial trainees;
2. Advanced training, for judges and prosecutors specialising in cybercrime;
3. Specialised courses, on topics like virtual currencies, specific investigation methods in a virtual environment, international cooperation, etc.

Moreover, one expert underlined that the Judiciary and LE representatives are encouraged to meet regularly within 'regional cybercrime task forces' to share experiences and enhance cooperation. Cybercrime policy guidelines are being elaborated: they will include a minimum training on cybercrime for prosecutors, as well as the obligation to participate in these 'cybercrime task forces' to share knowledge and best practices.

2.2. 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.b).

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). Czechia adopted late 2020 a new National Cybersecurity Strategy for 2021 – 2025 (NÚKIB, 2020a). To date, the new Action Plan for the NCSS is not available, however expected for late 2021.

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.

In addition, a document called "Concept for the development of the National office for Cyber and Information Security" was published in 2020 by the NÚKIB. It presents a long-term vision of the NÚKIB development, as well as a capacity development plan until 2027, including capacity building of the governmental CERT and regular training of the NÚKIB staff (NÚKIB, 2020).

Czechia ratified the Budapest Convention in 2013.

2.2.1. 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	

2.2.1.1. 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.

2.2.1.2. 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 has more room for manoeuvre 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).

2.2.1.3. 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 other organisational units.

2.2.1.4. 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.

2.2.2. Synergies and potential interferences

As in most countries, useful synergies and also at the same time reciprocal 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 inter-community 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. Such steps have improved the synergies among these communities. 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 synergy specifically identified during the interviews is that CSIRTs share with LE information obtained from a constituency or cooperating mechanisms 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 in court. In addition, one of the limitations of cooperation identified during the interviews is due to the need of 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 from their constituency. Another limitation identified is the lack of understanding, specifically between the experts from CSIRT and Leon one side, and the Judiciary, on the other side.

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.

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;
- 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.

2.2.3. 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 ([13]).

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.

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

2.3. ESTONIA

Estonia is 'a parliamentary republic. The head of government, the prime minister, is nominated by the president and approved by the Parliament. He/she is in charge of the executive power vested in government. The head of state, the President, is elected by Parliament or electoral college for 5 years. The Parliament has 101 members, elected every 4 years. The country is divided into 15 counties and 79 municipalities' (European Union, n.d.c).

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

The Estonian NCSS 2019-2022 is the third national cybersecurity strategy document (Estonian Ministry of Economic Affairs and Communications, 2019). It is based on lessons learned during the two previous strategy periods (2008-2013 and 2014-2017). The new Cybersecurity Act came into force in 2018 (Riigi Teateja, 2018a). It transposes requirements from the NIS directive and the GDPR into national legislation.

Estonia ratified the Budapest Convention in 2003.

2.3.1. Roles and duties

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

([13]) 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.

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)
Information System Authority	Riigi Infosüseemi Amet	RIA
- **CERT Estonia**	CERT Eestis	CERT-EE
Criminal Police	Kriminaalpolitsei	
- **Cybercrime Unit**	Küberkuritegude büroo	
Prosecutor's Office	Prokuratuur	

2.3.1.1. National cybersecurity agency

Under the responsibility of the Ministry of Economic Affairs and Communications, the Estonian Information Security Authority (RIA) is responsible for developing the national IT systems, managing and protecting the state Internet network and ensuring national cybersecurity of Estonia (RIA, n.d.).

RIA operates the Estonian national CSIRT, CERT-EE.

2.3.1.2. CSIRTs

Established in 2006, CERT-EE is a department of the Cyber Security Branch of the Information System Authority (RIA) and is funded by the state budget (RIA, n.d.a).

CERT-EE's primary constituents are Estonia's state institutions and local authorities, in addition to Operators of Essential Services (OES) and Digital Service Providers (DSP) in the context of the NIS directive, and critical IT infrastructure. The level of support provided by CERT-EE depends on the type and severity of the incident or issue, and on the impact on Estonian critical infrastructure.

'CERT-EE deals with security incidents that occur in Estonian networks, start there, or which it has been notified about by citizens or institutions either in Estonia or abroad' (RIA, n.d.a). CERT-EE's role is to:

- Monitor the state of information security in Estonia;
- Prevent security incidents and reduce security risks;
- Provide assistance and advice to institutions victims of cybersecurity incidents. CERT-EE can also facilitate contact with LEAs.

CERT-EE is the NIS Directive Single Point of Contact. Its role also covers awareness raising for government and non-government entities, and educating the nation and national IT sector on cyber threats.

As the Estonian Code of criminal procedure (Riigi Teateja, 2003) allows the involvement of experts in criminal proceedings, CERT-EE can be appointed as an expert body by the prosecutor in charge of the case. The CERT-EE T's representatives can also be called as witnesses to court as necessary.

CERT-EE is a member of the CSIRTs Network.

2.3.1.3. LE

Within the Criminal Police, cybercrime is tackled by the **Cybercrime Unit**, which was set up in 2016 (e-GA, 2021).

The Cybercrime Unit is responsible for the investigation of cybercriminal acts. It gathers and analyses intelligence on criminal offences. It used to be responsible for digital forensics, which is now the responsibility of a separate unit.

In 2020, the Cybercrime Unit opened the website 'cyber.politsei' (Politsei, n.d.) to report cybercrime to the Police. The website also gives information and tips on how to recognise phishing e-mails or restore access to personal accounts.

2.3.1.4. Judiciary

'The **Prosecutor's office** [emphasis added] is a government agency within the area of government of the Ministry of Justice which participates in the planning of surveillance necessary to combat and detect criminal offences, directs pre-trial criminal procedure and ensures the legality and efficiency thereof, represents public prosecution in court' (Riigi Teateja, 2018).

Until some years ago there were no specialised cybercrime courts or prosecutor's offices in Estonia (Council of the European union, 2017d). One of the experts interviewed specified that the prosecutor in charge of international cooperation also dealt with cybercrime. Moreover, District Prosecutors could be assigned to tackle cybercrime cases, while simultaneously working with other types of crime. The situation changed in 2019 and there is currently **one prosecutor specialised in cybercrime within the Prosecutor General's Office**, who deals exclusively with cybercrime cases.

Cybercrime connected to State security or of very high priority are prosecuted by the Prosecutor General's Office. The four District Prosecutor's Offices also have smaller units able to deal with cybercrime, to which the Prosecutor General's Office can give guidance. In some specific cases, the Prosecutor General's Office can take the decision to take over the case.

The cybercrime prosecutor gives guidance to the Police during the investigation and, once the investigation is completed, decides, based on the evidence collected, whether or not to start prosecution.

The Prosecutor General's Office is also responsible for informing the public about the risk of cybercrime.

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

2.3.2. Synergies and potential interferences

The situation in Estonia is specific as it is a small country in terms of size and population ([14]). Representatives from the three communities know each other well and have built a solid cooperation based on trust. As highlighted by one interviewee, 'the police and the prosecutor in charge of cybercrime work as a team', and there are no overlaps in their roles and duties. Phone calls are usually organised every day and meetings in person on a weekly basis to ensure smooth cooperation.

An example of synergy was given by one of the experts interviewed: in a recent case, the CSIRT went on site to assess the gravity of a cybersecurity compromise and the damage caused, from the victim's point of view. This assessment made by the CSIRT helped LE better understand the attackers' infrastructure and the victim's point of view. This combination of

([14]) Estonia is a country of 43,339 km^2 and 1.3 million inhabitants (European Union, n.d.q)

CSIRT and LE expertise allowed the two communities to draw a better and more comprehensive picture of the incident and its consequences.

One interviewee highlighted that there were cases where CSIRT representatives were allowed by the prosecutor to take part in the hearings of cybercrime perpetrators. This significantly fostered the CSIRT's understanding of the cases and ultimately helped them improve the way the two communities work together.

Despite this, the interviews highlighted that there may be a difference of interests among the communities: at the beginning of an investigation, the priority of both the Police and the Prosecutor's Office is to gather as much evidence as possible, sometimes before the CSIRT acts, whereas the CSIRT, responsible for (State) cybersecurity, aims to quickly stop the incident, recover the system and inform the public. The investigative procedures can be slower and more bureaucratic than the CSIRT's, which can be a challenge.

However, thanks to very good communication, no conflicting situations were experienced by the interviewees. In case of a disagreement between LE and the CSIRT, the prosecutor has the final say.

A STRONG COOPERATION BASED ON TRUST

As Estonia is a small country, representatives of the three communities know each other well and have built a solid cooperation based on trust.

2.3.3. Examples of training

Joint training opportunities are mostly bilateral and rarely involve all three communities. One of the interviewees mentioned that joint trainings are not especially necessary as 'real life is the best way to train on how to work together'.

The cybercrime prosecutor provides training to LE and other institutions responsible for cybercrime. The training covers topics like e-evidence or international cooperation. The Police also provides training to the Prosecutor's Office, on specific subjects, such as open source intelligence gathering.

One expert interviewed explained that informal joint events were organised regularly between the LE and the CSIRT before the COVID-19 pandemic. These events allowed each community to enhance their understanding of the other's work.

2.4. FINLAND

Finland is a 'parliamentary republic with a head of government, the prime minister, and a head of state, the President. The central government is based in Helsinki and the local governments in the 311 municipalities (towns and cities)' (European Union, n.d.p).

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

The latest Finnish NCSS was published in 2019 (Finnish Security Committee, 2019). It is based on the general principles of Finland's 2013 NCSS. The 2019 NCSS foresees the development of legislation enabling the fight against cybercrime.

The NIS Directive is transposed into Finnish law. The amendments to implement this directive entered into force in 2018.

Finland ratified the Budapest Convention in 2007.

2.4.1. Roles and duties

In Finland, 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 Security Centre	Kyberturvallisuuskeskuksen	NCSC-FI
National Bureau of Investigation	Keskusrikospoliisi	KRP
- **Cybercrime unit**	Poliisin Kyberrikostorjuntakeskus	
National Prosecution Authority	Syyttäjälaitos	

2.4.1.1. National cybersecurity agency/CSIRTs

The **National Cyber Security Centre of Finland (NCSC-FI)** carries out the CERT function (NCSC-FI, n.d.). It acts as both the national and governmental CSIRT.

The NCSC-FI was established in 2014. It is part of the Finnish Transport and Communications Agency (Traficom). 'NSCS-FI's CSIRT duties include:

- Addressing information security violations and threats against networks, communications and value-added services;
- Gathering information on such incidents;
- Disseminating information on information security matters' (Traficom, n.d).

As described in the NCSC-FI's RFC 2350, the NCSC-FI is 'the National CSIRT of Finland and the CSIRT for last-resort in cases where reporter cannot find more direct reporting contact in Finland. The NCSC-FI also acts as the Finnish governmental CSIRT. Telecommunications providers have a legal obligation to report major information security incidents, threats to information security and faults and disturbances to the NCSC-FI' (Traficom, n.d.a).

The NCSC-FI can be called to court as an expert to testify in a cybercrime case, however, according to one interviewee, this happens very rarely.

NCSC-FI is a member of the CSIRTs Network.

2.4.1.2. LE

The **Cybercrime unit** was established in 2015 as part of the National Bureau of Investigation (NBI). It is responsible for the investigation of the most serious cybercrime, internet and network intelligence, and maintenance of situational awareness. One of the experts interviewed explained that he NBI is also in charge of developing 'new investigation methods and provides technical, judicial and operational support to local police in cybercrime investigations'.

All police districts can investigate cybercrime, but the Cybercrime unit of the NBI 'is responsible for international, organised, technically challenging and larger cybercrime cases' (Council of Europe, n.d.c).

Police districts are responsible for the offences which occur in their region. They all have dedicated digital forensic experts. The ways districts conduct investigations of cybercrime vary

significantly as only few districts have investigators specialised in cybercrime (Council of Europe, n.d.c).

2.4.1.3. Judiciary

The **National Prosecution Agency** 'is involved at all stages of the processing a criminal matter: the pre-trial investigation, the consideration of charges and the trial' (National Prosecution Authority, n.d.). When the Police open an investigation, they request the naming of a prosecutor for the pre-trial investigation. In Finland, the prosecutor does not lead the investigation, but supports the Police during the investigation. Once the investigation is completed, the prosecutor decides whether or not to prosecute the case. In specific cases where the crime has been committed abroad but there are victims in Finland, the prosecutor is responsible for requesting a police investigation.

Within the National Prosecution Authority, 'the Prosecutor General's Office acts as the general administrative unit' (National Prosecution Authority, n.d.a). There are five prosecution districts: Southern Finland, Western Finland, Northern Finland, Eastern Finland and Åland (National Prosecution Authority, n.d.a).

In Finland, a prosecutor can specialise in certain types of crime (specialised district prosecutor), among which computer crime. Although there is no prosecutors or courts exclusively responsible of cybercrime cases, 'a group of prosecutors in local prosecution units prosecute most of such crimes' in addition to other tasks (Council of Europe, n.d.c). One expert interviewed explained that prosecutors 'began working on cybercrime related cases some seven or eight years ago'. There are currently five or six prosecutors specialised in cybercrime. The cases tend to be scattered, and one cybercrime prosecutor does not necessarily know what the others are doing. There are not many complex cybercrime cases.

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

BILATERAL SYNERGIES

The synergies are existing bilaterally, rarely involve the three communities. The LE and the CSIRT meet regularly to share information on ongoing cases. Regular trainings are organised between the LE and the Judiciary.

2.4.2. Synergies and potential interferences

The designated prosecutor leads the police investigation. The CSIRT does not usually interact with the judiciary: the cooperation between the CSIRT and the Judiciary is operated via the police, which interacts with both.

As highlighted during the interviews, weekly meetings are organised between the CSIRT, the Cybercrime unit of the NBI, the Police and other relevant organisations, where 'general information about ongoing cybercrime cases is shared'. The Cybercrime unit also receives weekly and monthly reports from the CSIRT. However, detailed information about ongoing criminal investigations is shared by the LE to the CSIRT only when considered necessary to prevent a cybercrime or to limit further damages.

One of the interviewees added that 'weekly and quarterly meetings [are organised] where information on phenomena and trends are shared and discussed between the CSIRT and the police'. This was presented as an example of excellent synergy.

Another example of complementarity is the Finnish Police's Net Tip-Off service ([15]), which allows citizens to anonymously report offences, even if not directly a victim. In certain situations, tip-offs can be forwarded to the CSIRT (for example, if there is not enough to warrant a Police investigation), which can then act within the scope of its duties (e.g. asking for a website to be taken down).

In addition, one expert specified that both the CSIRT and LE have highly-skilled personnel, which, when working together, make 'an extremely skilled team'. This specifically 'tailored task force' was used in a few cases where 'they have proven to be very creative and therefore very useful'. One case was given as an example, where specific forensics solutions were needed. A

([15]) https://poliisi.fi/en/net-tip

'task force' was set up with staff members from the CSIRT and LE, which found relevant evidence that quickly brought the criminal investigation on the right track.

The interviewees stated that they did not experience major interferences in the work of the CSIRT and LE, but mentioned a difference of interests between the two communities. Moreover, the legal framework allowing the two communities to share information was presented as sometimes restrictive, as each community would appreciate receiving more information from the other but is limited by law. One limitation was mentioned during the interviews: the CSIRT 'lacks proper specific procedures to preserve the chain of custody to hand e-evidence over to law enforcement and ensure it is applicable in court'.

Moreover, although prosecutors receive cybercrime training on a regular basis, one of the interviewees highlighted that more training would be beneficial for all the prosecutors to stay up-to-date with the technical aspects of cyber related criminal offence.

As 'cybercrime cases can be complex and very technical', one interviewee underlined that 'it is essential that we speak the same language and [that] the communication is clear, leaving no room for misinterpretations'. The prosecutors and judges should have a good understanding and awareness of the technical aspects to be prepared to such situation when it occurs.

Cybercrime prosecutors also experience organisational issues, as, according to one interviewee, they could further coordinate with each other. Additionally, some cases are sometimes handled by local prosecutors who are not specialised, which can affect the way the Police investigates.

Finally, according to same data collected during the interviews, judges 'tend to be reluctant to work with the police to avoid compromising the objectivity of the courts'. There is no legal framework for cooperation between judges and prosecutors, or between judges and Police.

2.4.3. Examples of training

The Police University College of Finland organises various courses, conferences and seminars for police staff. Cybercrime is one of the topics covered by these courses.

The Police University College runs various research, development and innovation (RDI) projects dedicated to enhancing cybercrime training of police forces. The most recent is "Cyber competence 2020" (2017-2020, funded by the Internal Security Fund of the European Union), which aimed to develop and increase 'the provision of cyber training and education at the Police University College of Finland to enable the launch of a specialist education study module in the prevention of cybercrime'. The purpose is to 'improve public authorities' knowledge of and skills in the prevention of cybercrime' (Police University College of Finland, n.d.). Research results in the cyber field will be used in the preparation of training. The education and training prepared in the project is targeted at civil servants employed by the key public authorities engaged in the prevention of cybercrime.

In 2013, the Police University College of Finland held the CEPOL course 15/2013 "Cybercrime vs. Cyber security", in which the NCSC-FI participated as an expert (CEPOL, 2013). In 2018, Finland hosted the CEPOL course 81/2018, in cooperation with EJTN, on "Forensic science and evidence - challenge for policing", of which the target audience was LE and judges/prosecutors (CEPOL, 2018). One part of the course was focusing specifically on digital evidence.

One of the interviewees highlighted that specialised cybercrime prosecutors are offered training both nationally and abroad, and are also tasked to train other prosecutors who do not handle cybercrime cases regularly. These courses 'are not mandatory but they have been very welcomed among other prosecutors.

The experts interviewed explained that the Police and the prosecutors regularly participate in joint trainings. Moreover, the Police has participated in prosecutors' training for several years, and prosecutors in police training too, where they learn about technical aspects such as

networks, communications or cryptocurrencies. Joint trainings are seen as beneficial, as they help 'harmonise terms, language and understanding of cyber and cybercrime'.

One expert explained that a joint cyber exercise bringing together 'the core of security in Finland' (Police, border controls, Finnish governmental ICT providers) is organised every year. The NCSC-FI has a supporting role in this training and provides threat intelligence and expertise as necessary. There are otherwise very few joint trainings between the CSIRT and the LE. The cooperation is developed by working on common cases rather than training together.

However, it was highlighted during the interviews that there are no joint trainings involving all three communities, although on expert underlined that this 'could help in integrating, unifying practices, understanding phenomena and, last but not least, taxonomy in cyber related issues'.

2.5. 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.d).

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). In February 2021, the French President announced an acceleration of the National Cybersecurity Strategy, which should include a strengthening of the cooperation between the Law Enforcement community and the judiciary (Présidence de la République française et du Palais del 'Élysée, p. statement at 3'7").

France ratified the Budapest Convention in 2006.

2.5.1. 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
- **Anticipation and Analysis Division**	Division de l'anticipation et de L'Analyse	D2A
- **CSIRT of the Judicial Police**	CSIRT Police Judiciaire	CSIRT PJ
▪ **E-evidence Unit**	Division de la preuve numérique	DPN
National Gendarmerie	Gendarmerie Nationale	
- **Directorate-General of the National Gendarmerie**	Direction Générale de la Gendarmerie Nationale	DGGN
○ **Intelligence Division**	Direction du renseignement	DR
○ **Institute for criminal research research**	Institut de recherche criminelle de la Gendarmerie nationale	IRCGN
○ **Research Sections**	Sections de Recherche	SR
○ **Centre for the Fight against Digital Crimes**	Centre de lutte contre les criminalités numériques	C3N
Central Criminal Intelligence Service of the National Gendarmerie	Service central de renseignement criminel de la Gendarmerie nationale	SCRCGN
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	

2.5.1.1. 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).

2.5.1.2. 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 France (CERT-FR, n.d.).

2.5.1.3. 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) ([16]), a cyber-intelligence unit. The Anticipation and Analysis Division (D2A) is the technical support of the OCLCTIC, with forensics and reverse capacities. The CSIRT-PJ is also embedded within the OCLCTIC. The SDLC operates sixteen digital investigation laboratories, which can support police services during digital investigations (French Senate, 2020).

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 Home Office.

Within the Directorate-General of the National Gendarmerie (Générale de la Gendarmerie Nationale – DGGN) there are the Intelligence Division (Direction du renseignement - DR) that produces analyses regarding cybercriminals trends, the Institute for criminal research (Institut de recherche criminelle de la Gendarmerie nationale - IRCGN) that has research labs not only cyber and that provides technical support for reverse engineering, the Research Sections (Sections de Recherche - SR) that can have specific cyber capacities and conduct dedicated investigation if incidents happen on their territory.

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

([16]) 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.

tasks, in the capacity of judicial Police (CSIRT-PJ, n.d.). However, the BL2C is not responsible for investigating cyberincidents impacting operators of essential services.

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) or when any national fundamental interest is threatened (if related to terrorism, for example).

Since 2009, the French National Directorate for Customs Intelligence and Investigations (Direction nationale du renseignement et des enquêtes douanières - DNRED) has its own internal structure to fight cybercrime (called "cyberdouanes" or "cellule Cyberdouane") under the scope of customs activities (such as collection and exploitation of data on illegal activities using Internet) (French Senate, 2020).

Finally, France is part of the Europol's Joint Cybercrime Action Taskforce (J-CAT) (Europol, n.d.c).

2.5.1.4. 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.

In early 2020, a structural reorganisation of the Paris Prosecutor's Office led to the renaming of the Cybercrime unit (from F1 to J3), which is under the responsibility of the Paris' circuit courts (Cour d'assises). J3 can investigate complex cybercrime cases at the national level (such as cases involving operators of essential services, ministries, etc.) (French Senate, 2020).

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.'

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

2.5.2. 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.'

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.

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.

A new legal measure (Article 706-105-1 – Code of Criminal Procedure) came into force in July 2021, opening the possibility of further cooperation and communication between the Paris Public Prosecutor and non-judicial services (Code of Criminal Procedure, 2021). Concretely, this measure enables the Paris Public Prosecutor, on his/her own initiative or when requested to do so, to communicate or share judicial information of any nature to relevant state services even if non-judicial. These services could be n/g CSIRTs. This can be done when necessary for the state's duties related to the security and defense of information systems. More precisely, this measure is available when the investigation falls under the scope of Article 706-72 which encompasses any offences against automated information processing systems (Code of Criminal Procedure, 2021a).

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

Furthermore, InterCERT France is a group gathering all organisations with Incident response Team (IRT) activities on French soil. InterCERT France’s objective is to strengthen the stakeholders’ capacity to detect and deal with security incidents. This initiative is driven by several working groups, including members from law enforcement or judiciary entities, which enhances the cooperation between CSIRT and LE (CERT-FR, n.d.).

Finally, ANSSI recently announced a funding and incubation framework to establish regional CSIRTs in France. These CSIRTs will work very closely with law enforcement, which should create a strong territorial network (ANSSI, n.d. b).

2.5.3. 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 (Council of the European Union, 2015).

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.

2.6. 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.f). 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), alongside the Digital Strategy 2025, which sets out legal measures and instruments to ensure the country's digital transformation (BMWi, 2016).

In May 2021, Germany endorsed an IT Security Act 2.0, extending reporting obligations and standards to be applied to critical infrastructures and reinforcing the BSI's mandate to set standards for Federal authorities and to monitor their compliance to afore-mentioned standards.

Germany ratified the Budapest Convention in 2009.

2.6.1. 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
Central Office for IT - Federal ministry of the Interior	Zentrale Stelle für Informationstechnik im Sicherheitsbereich	ZITiS

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

2.6.1.1. 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.'

2.6.1.2. 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 ([17]) 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).

Following the cyberattack against the Bundestag in 2015, Mobile Incident Response Teams (MIRTs) were established within the BSI (ENISA, 2017b). The MIRT provides on-site support to the federal administration and operators of critical infrastructures in the event of an cybersecurity incident and supports incident response. In particularly serious cases, the BSI can also provide on-site support with the CERT-Bund, then the MIRT operates as the mobile arm of the CERT-Bund. After an inital assessment of the situation and of the consequences, the MIRT carries out technical analyses and advises the organisation on how to deal with the incident (BSI, 2019).

2.6.1.3. 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.

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 sixteen 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.).

Established in April 2017, the **Central Office for IT of the Federal ministry of the Interior (ZITiS),** although not a LEA, takes on a central role in researching and developing cyber-related solutions. It is tasked with digital forensics, telecommunication surveillance, crypto analysis, big data analysis and fight against crimes, counter espionage, R&D of methods and the development of tools and strategies for security agencies (ZITiS, n.d.).

Finally, Germany is part of the Europol's Joint Cybercrime Action Taskforce (J-CAT) (Europol, n.d.c).

([17]) 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

2.6.1.4. 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.o).

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 within the 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.

2.6.2. 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.'

2.6.3. 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).'

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.

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.

2.7. IRELAND

Ireland is 'a parliamentary republic consisting of 26 counties. The head of government, the prime minister [(Taoiseach]), is appointed by the President after nomination by the Lower House (Dail) and exercises executive power. The head of state, the President, mostly has ceremonial powers. The Parliament has 2 chambers (an Upper and Lower House)' (European Union, n.d.r).

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

The current National Cyber Security Strategy was published in 2019 and covers the period 2019-2024. In terms of cybercrime, the strategy foresees supporting 'international cooperation to combat cybercrime and promote formal and informal cooperation in cyberspace, including by engaging in sustainable capacity building in third countries' (Department of Justice and Equality, 2020).

Ireland signed the Budapest Convention in 2002 and it is working towards its ratification (Department of Justice and Equality, 2020, p. 4).

Ireland adopted the legislation transposing the NIS directive (Statutory Instrument No. 360 of 2018) in 2018 (NCSC, n.d.b).

2.7.1. Roles and duties

In Ireland, 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 Security Centre	National Cyber Security Centre	NCSC
- **CSIRT-IE**	CSIRT-IE	CSIRT-IE
National Police	An Garda Siochana	
Garda National Cyber Crime Bureau	Garda National Cyber Crime Bureau	GNCCB
Director of Public Prosecutions	Director of Public Prosecutions	DPP

2.7.1.1. National cybersecurity agency

The **National Cyber Security Centre** (NCSC) of Ireland is the primary State cybersecurity authority (NCSC, n.d.b). It primarily focuses on securing government networks and securing critical national infrastructure. The Irish national and governmental CSIRT (CSIRT-IE) is part of the NCSC.

Since 2017, the NCSC 'has developed an extensive threat intelligence database that is used to assist [government] Agencies and Departments in protecting their networks' against high-end threats actors/cybercriminals (Government of Ireland, 2019).

The constituent base of the NCSC is around one hundred thirty members. This base includes government departments and agencies, and key entities across the financial sector, critical national infrastructure providers and other operators of essential services (OES). NCSC's constituency, which includes An Garda Siochana, the national Police, receive (email and text) alerts and advisory services as necessary.

In case of cybercrime, the NCSC provides incident response and technical analysis (it has specific expertise in infrastructure tracking and malware analysis).

The experts interviewed explained that there are secondment opportunities between the Garda National Cyber Crime Bureau and the NCSC.

2.7.1.2. CSIRTs

Established in 2011, **CSIRT-IE** is a body within the NCSC which provides assistance to the NCSC's constituents in responding to cybersecurity incidents at national level (NCSC, n.d.a).

CSIRT-IE's responsibilities include:

- 'Monitoring incidents at national level;
- Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;
- Responding to incidents;
- Providing dynamic risk and incident analysis and situational awareness' (NCSC, n.d.a).

In 2017, CSIRT-IE set up an integrated incident response and analytics platform. Today, CSIRT-IE has a more 'proactive position', thanks to 'the deployment and use of MISPs (Malware Information Sharing Platforms) to share threat intelligence directly with Critical National Infrastructure Providers, and the evolution and use of a series of tools to identify, parse and analyse open source intelligence (OSINT). CSIRT-IE 'has also developed, tested and deployed the 'Sensor' platform, now operational on the infrastructure of a number of Government Departments, to detect and warn of certain types of threat' (Government of Ireland, 2019).

According to one interviewee, the CSIRT could be called to court to testify in a cybercrime case, as it is possible to summon anyone as a witness.

CSIRT-IE is a member of the CSIRTs Network.

2.7.1.3. LE

Investigation of crime is the exclusive jurisdiction of **An Garda Siochana** (national Police), however the police can receive advice from the Director of Public Prosecutions, which is an independent entity.

The **Garda National Cyber Crime Bureau** (GNCCB) was established as the Cyber Crime Investigation Unit of An Garda Siochana in 1991, and re-established as the Garda National

Cyber Crime Bureau in 2017. It is 'tasked with the forensic examination of computer media seized during the course of any criminal investigation. […] The unit also conducts investigations into cyber dependent crime which are significant or complex in nature such as network intrusions, data interference and attacks on websites belonging to government departments, institutions and corporate entities' (GNCCB, n.d.). One interviewee underlined that since there are elements of digital forensics in the majority of investigations, it represents the largest part of the GNCCB's activities.

Two pilot regional cyber units were set up in 2017 (Council of the European Union, 2017e). As explained during the interviewees, there are currently four of these "satellite hubs" established throughout the country. Two more are planned to be set up in the near future. For the moment, they have a small number of staff, therefore the capacity to handle only a limited number of operations.

As mentioned above, there are secondment opportunities between the GNCCB and the NCSC.

2.7.1.4. Judiciary

Under Ireland's common law system, the **Director of the Public Prosecutions (DPP)** has no investigative functions and no power to direct An Garda Siochana in their investigations (DPP, n.d.) (Department of Justice and Equality, 2020). Once the investigation is complete, the DPP considers the file and directs the prosecution.

However, the DPP can advise An Garda Siochana during the investigation as well as provide guidance in case of complex prosecutions, while remaining independent. There are no investigation judges in Ireland.

There is no court, prosecution office or judge exclusively specialised in cybercrime (Council of the European Union, 2017e), however some prosecutors are specialised in cybercrime matters, although they also deal with other types of crime.

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

2.7.2. Synergies and potential interferences

Synergies exist as the CSIRT, LE and the judiciary have complementary roles and duties. In case of a cybercrime, LE is in charge of the investigation, while the CSIRT is in charge of incident response and technical analysis. It provides specific expertise in infrastructure tracking and malware analysis. The Judiciary is responsible for the prosecution and trial.

The experts interviewed highlighted that a Memorandum of Understanding (MoU) is currently being developed between the CSIRT and LE to provide a framework of cooperation.

As explained during the interviews, LE is in discussion with the Director of Public Prosecutions (DPP) to set up a training programme on cybercrime to share knowledge on the subject and understanding of each other's work. The same initiative has been proposed to judges.

One interviewee however underlined that the roles of each community and the processes could be better defined, as 'there is not enough legal definition to accurately articulate [these] roles'.

As highlighted during the interviews, the three communities sometimes have different priorities, especially the CSIRT and LE. The CSIRT's priority is to protect victims, while LE's is to identify and find the criminal. This can lead to interferences in their work.

Understanding technical language can be challenging for the Judiciary. In 2011, during the investigation of the hacking of an Irish political party's website by Anonymous, the DPP asked the Cybercrime Bureau to add a glossary of cyber terms at the back of each report and statement. This allows the DPP to better understand technical terms while working on the case.

A MOSTLY BILATERAL COOPERATION

Synergies are mostly bilateral (CSIRT-LE and LE-judiciary). The three communities actively work at overcoming challenges that could potentially impact their cooperation, especially thanks to trainings and exercises.

2.7.3. Examples of training

The ECTEG (European Cybercrime Training and Education Group) and the Irish UCD Centre for Cybersecurity and Cybercrime Investigation (UCD-CCI) have developed a Digital First Responders course which was provided to over two hundred police detectives in 2020. The training was delivered by the GNCCB and the UCD-CCI. The course covered the following topics: Online Investigation Techniques, Site Search Intelligence, Digital Forensic Challenges Encryption, Digital Forensic Challenges Virtual Machines, Internet Security (VPN), Search and Seizure Guidelines, How to deal with a live computer at search scene, Live data forensics using “First”, Post Search Analysis, Live Data Forensic (First Tool) Practical, Final Assessment (practical examination) (UCD-CCI, 2020).

Along with other European LEAs, An Garda Siochana contributes to the development of CEPOL's "First responders e-learning package" (E-First), focusing on essential IT forensics and IT crime knowledge. The aim is to provide a sound common reference for all LEA first responders (non-specialised field police officers), as well as digital forensic courses to more expert attendees (ECTEG, 2021).

In Ireland, judges and prosecutors attend national and international training events in the area of cybercrime on an ad hoc basis. One interviewee underlined that a joint training between the DPP and An Garda Siochana was organised a few years ago and that it was very useful. The DPP is currently setting up more trainings with law enforcement.

Some trainings and exercises are organised between the CSIRT and LE, but according to an interviewee the idea of having additional ones should be considered. Interviewees were unaware of trainings organised between the CSIRT and the Judiciary.

2.8. ITALY

Italy is ‘a parliamentary republic with a head of government - the prime minister - appointed by the President, and a head of state - the President. The Parliament is composed of 2 houses: the Chamber of Deputies and the Senate of the Republic. The country is subdivided into 20 regions. 5 of these have a special autonomous status, enabling them to pass legislation on some local matters’ (European Union, n.d.h).

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

A major national cybersecurity reform is currently ongoing in Italy, which includes the establishment in June 2021 of the National Cybersecurity Agency (see below).

The latest Italian Cybersecurity Action Plan was published in 2017 (Presidency of the Council of Ministers, 2017). It foresees the improvement of incident and cybercrime integrated response capabilities, as well as new legislative initiatives to create technical intervention teams to quickly support central administrations, operators of essential services and critical infrastructures in case of major cyber events.

In Italy, the NIS Directive was implemented by Legislative Decree no. 65/2018 (Official Journal of the Italian Republic, 2018).

Italy ratified the Budapest Convention in 2008.

2.8.1. Roles and duties

In Italy, 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 Cybersecurity Agency	Agenzia per la cybersicurezza nazionale	
- **Cybersecurity Unit (to be set up)**	Nucleo per la cybersicurezza	
- **Computer Emergency Response Team Italy**	CSIRT Italia	CSIRT Italia
State Police	Polizia di Stato	
- **Post and Communications Police**	Polizia Postale e delle Comunicazioni	
Financial Police	Guardia di Finanza	
Carabinieri Corps	Arma dei Carabinieri	
- **National Anti-crime Computer Centre for the Protection of Critical Infrastructure**	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche	CNAIPIC
Public Prosecutor's Office	Procura della Repubblica	

2.8.1.1. National cybersecurity agency

A major reform of national cybersecurity is currently ongoing in Italy. The legislative decree on the establishment of the **National Cybersecurity Agency** was approved by the Italian Council of Ministers on June 10th, 2021([18]). It states that the new National Cybersecurity Agency will be under the responsibility of the president of the Council of Ministers and the Delegate Authority for the Security of the Republic (Autorità delegata per la sicurezza della Repubblica). The legislative decree was converted into a law on August 4th, 2021 ([19]), which entered into force on August 5th, 2021 (Official Journal of the Italian Republic, 2021).

According to the decree, the Agency will, among other matters, be in charge of:

- Exercising the functions of national authority in the field of cybersecurity, to protect national interests from cyberthreats and ensure the resilience of services and essential functions of the State;
- Developing national capabilities for preventing, monitoring, detecting and mitigating, and coping with cybersecurity incidents and cyberattacks, also thanks to CSIRT Italia;
- Contributing to the enhancement of the security of Information and communications technology (ICT) systems of subjects included in the national cybersecurity perimeter, public administrations, operators of essential services and digital service providers;
- Exercising the functions of single national interlocutor for public and private entities in the field of security measures in the areas that fall under the scope of national cybersecurity, and network and information systems security (NIS Directive);
- Representing Italy in the European Cybersecurity Competence Centre (Senato della Repubblica, 2021).

[18]) Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale (D.L. 82/2021 – A.C. 3161)
([19]) https://www.gazzettaufficiale.it/eli/id/2021/08/04/21G00122/sg

A Cybersecurity Unit (Nucleo per la cybersicurezza) will be set up within the Agency and will closely cooperate with CSIRT Italia. CSIRT Italia will communicate to this Cybersecurity Unit any cases of breach or attempt to breach security, or loss of integrity which pose threats to the proper functioning of the networks and services. The Cybersecurity Unit can also receive such alerts from other CSIRTs established in Italy.

CSIRT Italia will also send incident notifications to the Cybersecurity Unit.

2.8.1.2. CSIRTs

CSIRT Italia was set up in 2019 under the responsibility of the Presidency of the Council of Ministers. The legislative decree of June 10th, 2021 on the creation of the National Cybersecurity Agency, will see CSIRT Italia become part of this Agency.

By the above-mentioned decree, CSIRT Italia will become the national and governmental CSIRT as it will exercise the functions of the national and governmental CSIRT (Senato della Repubblica, 2021). Before the adoption of the legislative decree on the establishment of the National Cybersecurity Agency, the role of national CSIRT was undertaken by a department of the Ministry for Economic Development, and the role of governmental CSIRT by CERT-PA (within the Agency for digital Italy-AGID).

CSIRT Italia's tasks are:

- Monitoring of incidents at the national level;
- Issuing early warnings, alerts, announcements and disclosure of information to interested parties regarding risks and incidents;
- Intervention in case of an incident;
- Risk and incident analysis;
- Participation in the CSIRTs network.

The decree foresees that operators of essential services (OES) must notify CSIRT Italia immediately in case of an incident having a significant impact on the continuity of the services provided. CSIRT Italia must immediately forward the notifications to the Cybersecurity Unit of the Agency and to the Post and Communications Police (Senato della Repubblica, 2021).

The decree underlines that incident notifications fall within the duties of CSIRT Italia and is part of the reporting obligations established by Article 331 of the Criminal Procedure Code, on the reporting by public officials and persons in charge of a public service (Senato della Repubblica, 2021).

CSIRT Italia is a member of the CSIRTs Network.

2.8.1.3. LE

By law (Interministerial Decree of 19 January 1999), the **Post and Communications Police** is the 'central body of the Ministry of the Interior responsible for the security of telecommunications services' in Italy (Polizia di Stato, n.d.). It is responsible for:

- Ensuring, at a general level, the integrity and functionality of the computer network, including the protection of critical infrastructures, the prevention of, and fight against, computer attacks on domestic strategic structures, and the security and regularity of telecommunications services;
- The fight against online Child Sexual Abuse Material (CSAM);
- Intelligence activity for the prevention of, and fight against, the use and forgery of means of payment (Post and Communications Police, n.d.).

The Central Service of the Post and Communications Police is based in Rome and coordinates twenty regional units and eighty local units. The local units are operational: they handle cases and emergencies which arise from complaints made by citizens through the hotline of the Post and Communications Police.

Within the Post and Communications Police, the Cybercrime Analysis Unit (Unità d'analisi del crimine informatico - UACI) is in charge of studying and analysing cybercrime phenomena in collaboration with major Italian universities.

Although 'specialised investigative tasks are assigned by law to the Post and Communications Police, [which is part of the State Police (Polizia di Stato, n.d.a)], other police forces […] [in particular], Arma dei Carabinieri [(Arma dei Carabinieri, n.d.)] and Guardia di Finanza [(Guardia di Finanza, n.d.))] may as a rule conduct investigations into cybercrime' (Council of Europe, n.d.d).

The **National Anti-crime Computer Centre for the Protection of Critical Infrastructure (CNAIPIC)** belongs to the Post and Communications Police. It is in charge of the prevention and repression of cybercrime actions targeting critical infrastructures (Post and Communications Police, n.d.a).

The CNAIPIC has an Operations Room, available 24/7, which acts as the single point of contact for critical infrastructures and any other actors engaged in the protection of critical infrastructures, including international actors.

Finally, Italy is part of Europol's Joint Cybercrime Action Taskforce (J-CAT) (Europol, n.d.c).

2.8.1.4. Judiciary

Under Law 48/2008 and the Code of Criminal Procedure, the **Public Prosecutor's Office,** 'attached to the Court of the main city of a Court of Appeal District […] holds jurisdiction to conduct the investigations into cybercrime' (Council of Europe, n.d.d). There are prosecutors specialised in cybercrime, but there are no specialised judges (Council of Europe, n.d.d).

Specifically in Milan, according to the Milan Prosecutor's Office's website, cybercrime was tackled by the High Tech Crime unit of the Counter-terrorism Department from 2012 to 2018, but currently falls under the competence of the **Fraud and Consumer Protection Department**, made up of 7 prosecutors. The Public Prosecutor's Office in Milan has also established a cybercrime victim support bureau (Milan Prosecutor's Office, 2013) (Milan Prosecutor's Office, 2015) (Milan Prosecutor's Office, 2018).

Cybercrime prosecutors are in charge of supervising the investigation and leading the prosecution of criminal offences. They cooperate with the Post and Telecommunications Police, whose role is to investigate cybercrime. Other police forces can also investigate cybercrime cases and cooperate with prosecutors, such as the Carabinieri and the Guardia di Finanza.

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

2.8.2. Synergies and potential interferences

In June 2021, the National Cybersecurity Agency was created by legislative decree and this might change the way the three communities cooperate.

As also highlighted during the data collection via the interview, synergies are possible when trust is established and each community 'is aware of the other's competences [and] understands the other's difficulties'. While no specific interferences with the CSIRT community were experienced, it was highlighted that however some difficulties may arise in the cooperation between the communities because their interests are sometimes different.

A key challenge mentioned during the interview was the need for more cybercrime training of the Judiciary: the Judiciary does receive training on cybercrime investigations, but not on a regular basis, especially as cybercrime raises fundamentally new issues and challenges.

RECENT CREATION OF THE NATIONAL CYBERSECURITY AGENCY

The creation of the National Cybersecurity Agency in June 2021 might impact the way the CSIRT, LE and judiciary communities cooperate to fight cybercrime.

2.8.3. Examples of training

The Interagency Law Enforcement Academy of Advanced Studies (Scuola di Perfezionamento per le Forze di Polizia) provides advanced training courses for police forces on "Instruments to prevent and counter cybercrime. Protection of National Critical Infrastructures" and "International cooperation in the fight against terrorism, against cybercrime and in the field of digital investigations" (Interagency Law Enforcement Academy of Advanced Studies, 2020). In addition, the programme of the second level crime analysis course includes one module on open source analysis, covering topics such as: open source intelligence (OSINT), research through the network, social networking and processing, deepweb and darkweb (Interagency Law Enforcement Academy of Advanced Studies, 2020).

Along with other European LEAs, the Post and Communications Police contributes to the development of CEPOL's "First responders e-learning package" (E-First), focusing on essential IT forensics and IT crime knowledge. The aim is to provide a common sound reference for all LEA first responders (non-specialised field police officers) as well as digital forensic courses to more expert attendees (ECTEG, 2021).

The Public Prosecutor's Office in Milan provides training courses. The teaching method, developed by LE investigators, combines lectures, labs and workshops. The course is based on the MOOC system as well as technical and didactic tutoring service, created specifically for all the investigators of the Milan Court of Appeal District (Milan Prosecutor's Office, n.d.).

The expert interviewed was not aware of any joint training opportunities on cybersecurity aspects. However, both LE and the Judiciary participate in training on digital forensics.

2.9. 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.i).

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). The fourth version is planned to be published in 2021([20]). In parallel, in February 2021, the ministry of Foreign and European Affaires' Directorate of Defence published the first Cyber Defence Strategy, which covers a 10-years period.

Luxembourg ratified the Budapest Convention in 2004.

2.9.1. Roles and duties

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

([20]) Not available at the cut-off date of the data collection. The cut-off date for data collection was 3rd August 2021; however, some additional input received between August and October 2021 was also integrated in this report

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
Public Prosecution and Judges	Ministère de la Justice	

2.9.1.1. 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.

2.9.1.2. 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 "includes and is limited to:

- The ministries, administrations and public services of the Government of Luxembourg including military organisations, and
- critical infrastructure operators' (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).

2.9.1.3. 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.

2.9.1.4. 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.

2.9.2. 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.

TRADITION OF ACHIEVING SYNERGIES

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

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.

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.

2.9.3. 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

2.10. 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.).

Norway ratified the Budapest Convention in 2006.

2.10.1. 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
- **National Cybercrime Centre**	Nasjonalt cyberkrimsenter	NC3
Norwegian National Security Authority	Nasjonal sikkerhetsmyndighet	NSM
Norwegian National Cyber Security Centre	Nasjonalt cybersikkerhetssenter	NCSC
- **Norwegian Centre for Information Security**	Norsk center for informasjonssikiring	NorSIS
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

2.10.1.1. 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.).

In addition, the NSM established partnerships with other entities such as the Norwegian Centre for Information Security (NorSiS), an independent organisation (established in 2002 as a project and founded in 2010 by governmental request, who collect and disseminate cybersecurity knowledge among Norwegian companies, local government and individuals. Among its activities, NorSIS coordinates, on behalf of the Ministry of Justice, the National Security Month, the pan-European exercise to protect EU infrastructure against coordinated cyber attacks.

2.10.1.2. CSIRTs

Norway has an officially recognised national and governmental CSIRT (NSM, n.d.). The NSM is responsible for NorCERT, which handles severe cyberattacks against critical infrastructures and information.

The main activities of NorCERT are ‘response to cyber threats in [… the NorCERT] 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.).

2.10.1.3. 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), set up in January 2019, 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). The NC3 provides assistance to the police district, conducts its own cybercrime investigations while developing national Police’s cyber expertise. It aims to become "the national centre of expertise and

knowledge in terms of technology-related policing, with about 150 employees" (Politiet, n.d. a) by the end of 2022. The NC3 is structured around 6 sections (incoming request, online police presence, Internet crimes against children, cybercrime, digital forensics, investigative support) and 3 underlying units (Intelligence, technique development, digital support). 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.

Finally, Norway is part of the Europol's Joint Cybercrime Action Taskforce (J-CAT) (Europol, n.d.c).

ESTABLISHED SYNERGIES

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

2.10.1.4. 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.

2.10.2. 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.

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 command and control (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.

2.10.3. 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, for example by organising a Security Hackathon and workshops. 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.

2.11. POLAND

Poland is 'a parliamentary republic with a head of government - the prime minister - and a head of state - the president. The government structure is centred on the council of ministers. The country is divided into 16 provinces, largely based on the country's historic regions. Administrative authority at provincial level is shared between a government-appointed governor,

an elected regional assembly and an executive elected by the regional assembly' (European Union, n.d.s).

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

The current NCSS is the Cybersecurity strategy of the Republic of Poland for 2019-2024 (NASK, 2019). The Strategy highlights the necessity of cross-border cooperation of LEAs and CSIRTs and that, as time is a critical factor in procedural actions and operational investigations, efficient and reliable information-sharing channels between LEAs of different countries are required.

The NIS Directive was fully implemented in Poland on 21 November 2018, when the Regulation on serious incidents thresholds applicable to operators of essential services (Dz.U. 2018 poz. 2180) was published. The implementation of the directive began when Poland adopted the Act on the National Cybersecurity System (Dz.U.2018.1560) on 5 July 2018 (Polish Parliament, 2018).

In 2015, the National Security Bureau (BBN) published the Polish Cybersecurity Doctrine (National Security Bureau, 2015).

Poland ratified the Budapest Convention in 2015.

2.11.1. Roles and duties

In Poland, 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)
Internal Security Agency	Agencja Bezpieczeństwa Wewnętrznego	
- **Governmental Computer Security Incident Response Team**	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego	CSIRT-GOV
CSIRT NASK	CSIRT NASK	CSIRT NASK
- **CERT Poland**	CERT Polska	CERT Polska
National Police Headquarters	Komenda Główna Policji	
- **Cybercrime Bureau**	Biuro do Walki z Cyberprzestępczością	
Central Forensic Laboratory of the Police	Centralne Laboratorium Kryminalistycznego Policji	CLKP
General Public Prosecutor's Office	Prokuratura Krajowa	

2.11.1.1. National cybersecurity agency

Poland does not have a dedicated cybersecurity agency. Two entities deal with cybersecurity at governmental and national levels.

The **Internal Security Agency** (Agencja Bezpieczeństwa Wewnętrznego) 'is a government institution which protects the internal security of the Republic of Poland and its citizens' (Internal Security Agency, n.d.). It tackles crimes such as 'terrorism, espionage, breach of State secrets, […] crimes connected with production of and trade in goods, technologies and services of strategic importance for the State's security, illegal production and possession of and trade in arms', etc. (Internal Security Agency, n.d.). The Internal Security Agency operates CSIRT-GOV, the Polish governmental CSIRT.

The **NASK** is a national research institute (see below) under the supervision of the Chancellery of the Polish Prime Minister. It operates the Polish national CSIRT.

2.11.1.2. CSIRTs

The Act on the national security system, which implements the NIS Directive into the Polish legal system, appoints three institutions to serve as response teams (NASK, n.d.):

- The Internal Security Agency, via **CSIRT-GOV**;
- The NASK (Research and Academic Computer Network - Naukowa i Akademicka Sieć Komputerowa), via **CSIRT NASK**;
- The Ministry of National Defence, via CSIRT-MON (which is not described here as from the data collected did not emerged that it plays a role in the cooperation between CSIRTs and LE in fighting cybercrime).

The Polish national CSIRT**, CSIRT NASK**, operates in accordance with the Act on the national security system. It is responsible for handling incidents from the public and private sectors, local governments and other entities which are not part of the central government or of a critical infrastructure (NASK, n.d.)**.** CSIRT NASK can be called to court as an expert witness for cybercrime cases. According to one of the interviewees, CSIRT NASK is often appointed as an expert witness by judges. Its testimonies are provided in the form of written reports. By law, it could be called to court physically, however in practice, this is very rare.

Additionally, as NASK is a national research institute, it conducts research and develops capabilities and tools for efficient monitoring and handling of security incidents. For example, CSIRT NASK maintains the "Warning List" (CERT.PL, 2020), a service which provides a frequently updated list of dangerous/malicious domains. Many Internet service providers, including telecom operators, use this tool so the Internet users receive a warning message when trying to access a domain used for phishing or malware distribution. CSIRT NASK also maintains and develops MWDB (CERT.PL), a Malware Analysis Platform, Database and Community, to which cybersecurity professionals can request access.

CSIRT NASK can also provide advice to LE, such as on the data which might be useful for an investigation and the actions which should be taken or procedures which should be followed to gather more information.

CERT Poland operates within CSIRT NASK. It was established in 1996 as the first Polish CERT. Active 24/7, it coordinates responses to incidents occurring in the Polish civilian cyberspace reported by OES, digital service providers, local authorities and individuals. It also monitors online threats and carries out expert and forensic computer analyses, using its analytical and R&D facilities to identify malware and vulnerabilities, assessing and measuring the scale of threats and mitigating them (CERT Polska, n.d.) (Trusted Introducer, n.d.).

CERT Poland is a member of the CSIRTs Network.

A team called "Dyżurnet.pl" also operates within CSIRT NASK. The Dyżurnet.pl team is a point of contact which 'responds to anonymous reports received from Internet users about potentially illegal material, mainly related to sexual abuse of children' (NASK, n.d.a).

CSIRT-GOV is under the responsibility of the Head of the Internal Security Agency. It acts as the governmental CSIRT responsible for coordinating the process of responding to computer incidents occurring in the area indicated in Art. 26 (7) of the Act of 5 July 2018 on the national cybersecurity system (public administration bodies and critical infrastructures) (Polish government, 2019) (CSIRT-GOV, n.d.).

2.11.1.3. LE

Established in 2016, the **Cybercrime Bureau** of the National Police Headquarters (Policja, n.d.):

- Supervises, coordinates and supports activities aiming to combat cybercrime conducted by the National Police Headquarters in cooperation with the Central Police Investigation Bureau;
- Coordinates the activities of the Police in preventing and fighting cyberthreats;
- Cooperates with the Office for International Police Cooperation;
- Conducts and supports R&D projects on new solutions to fight cybercrime.

The Cybercrime Bureau is composed of the following departments:

- Intelligence Department;
- Operations Department;
- Forensics Department.

Investigations are conducted by the Operations Department of the Cybercrime Bureau.

The Cybercrime Bureau supervises cybercrime units in the field. There is a regional cybercrime unit in each voivodeships (regions) of Poland.

The **Central Forensic Laboratory of the Police** is responsible for the development and the supervision of forensic activities within the Polish Police (Central Forensic Laboratory of the Police, n.d.). Its tasks include the examination of computer hardware and digital services:

- Identification of computer hardware and peripheral devices;
- Determination of the application of computer devices, their performance and memory size;
- Analysis of data saved on digital devices;
- Data recovery from digital devices.

Finally, Poland is part of Europol's Joint Cybercrime Action Taskforce (J-CAT) (Europol, n.d.c).

2.11.1.4. Judiciary

Criminal investigations and prosecutions are carried out under the responsibility of prosecutors. The **Public Prosecutor's Office** consists of the Prosecutor General, the National Prosecutor and deputy Prosecutors General (Public Prosecutor's Office, n.d.). There are also regional Public Prosecutor's Offices.

Within the Prosecutor General's Office, 'several prosecutors have been designated to provide coordination and support' in cases involving cyberattacks/incidents (Council of the European Union, 2017f). There is a division for cybercrime (Cybercrime, IT and Analysis department) within the General Prosecutor's Office and cybercrime departments in the regional Offices.

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

2.11.2. Synergies and potential interferences

The cooperation between the three communities was assessed overall by the interviewees as good, especially as the three communities have different roles and duties.

As highlighted during the interviews, CSIRT NASK cooperates daily with LE. It was mentioned during the interviews that the CSIRT's hotline is often used by LE in the course of an investigation, which is 'extremely useful, as many police units (especially in smaller municipalities) might not have a dedicated cybercrime unit'. In such cases, the CSIRT 'can provide advice on the data that might be useful for an investigation, on the actions that should be taken or procedures that should be followed to gather more information, etc.'. However, LE must submit a formal request to the CSIRT to receive specific information related to a cybercrime case.

One example of a successful synergy between the national CSIRT, the LE and the Judiciary is the case involving the Vortex ransomware, used for several attacks across Poland. The cooperation between the national CSIRT, the Cybercrime Bureau of the National Police Headquarters and the Warsaw Prosecutor's Office led to the arrest of a criminal who used this ransomware. They also managed to secure the encryption keys and CSIRT NASK could develop and publish a decryption tool for this type of ransomware (CERT Polska, 2018).

One of the experts interviewed underlined that LE and the Judiciary could benefit from more training regarding new technologies and technical aspects of cybercrime, as not all police departments have units specifically dedicated to fighting cybercrime, and judges and prosecutors could improve their understanding of the specificities of cyberspace.

It was also mentioned during the interviews that 'cybercrime-fighting entities would greatly benefit from a central system that would be a single source of knowledge (including IoCs) regarding cybercrime incidents being investigated'. This could be especially useful to identify the victims of a widespread attack and to make it one single case. Currently, it is difficult for local police departments to link one complaint or one notification of a suspected crime to a wider campaign. They often ask the national CSIRT to share information on a specific incident, which allows the CSIRT to identify other potential victims.

AN EXAMPLE OF TRAINING TO FOSTER SYNERGIES

CSIRT NASK provides training and workshops to police officers and prosecutors on cybercrime related topics, such as the darkweb, cryptocurrencies, and OSINT.

2.11.3. Examples of training

The national CSIRT, CSIRT NASK, organised and led a series of training for police officers as part of a CyberPol([21]) programme. Training covered fighting cybercrime and children's safety in the cyberspace.

CSIRT NASK also provides training and workshops to police officers and prosecutors on cybercrime related topics, such as the darkweb, cryptocurrencies, and OSINT. However, CSIRT NASK does not provide training to judges.

Additionally, the Cybercrime Bureau of the National Police Headquarters organises trainings for the prosecutors to enhance their knowledge in cybercrime matters.

The experts interviewed were not aware of a training initiative involving the three communities.

2.12. 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.k).

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

([21]) https://www.cyberpol.info

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).

Portugal ratified the Budapest Convention in 2010.

2.12.1. Roles and duties

In Portugal, the following authorities and departments, in particular[22], 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
Portuguese National Cybersecurity Centre	Centro Nacional de Cibersegurança	CNCS
National Communications Agency	Autoridade Nacional de Comunicações	ANACOM ([23])
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
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		

2.12.1.1. National cybersecurity 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.

([22]) The authorities and departments presented here are the main authorities/departments responsible for preventing, analysing and fighting cyber incidents/cybercrime. Other authorities/departments not presented here might play a role on an ad hoc basis.
([23]) For a description of the role of ANACOM see below Section 2.12.2.

2.12.1.2. CSIRTs

Portugal has an officially recognised national CSIRT**, CERT.PT** (CNCS, n.d.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.d.a) (CNCS, n.d.e). 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 CSIRTs Network.

2.12.1.3. 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.a). The Judicial Police also relies on its Central Investigation Section for IT and Telecommunications.

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.

2.12.1.4. 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, while the Cybercrime Office of the Public Prosecution Service is in charge of coordinating internally with the Public Prosecution Service, to provide specific training and to

establish communication with internet service providers to facilitate collaboration during criminal investigations.

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

2.12.2. 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) (CNCS, n.d.f).

SYNERGIES IN MULTIPLE LEVELS

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

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.a). 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.

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) the 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.

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.

2.12.3. 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 recent project "Homeland Security Fund" (Fundo para a Segurança Interna) of the Judicial Police aims to develop its internal capacity, in particular its know-how regarding the collection of cybercrime evidence (Policia judiciaria, 2018). Launched in April 2020 and expected to be finalised by the end of 2021, the project includes the certification of experts within the Judicial Police, the creation of an internal trainer pool, the conduct of trainings as well as the decentralisation of the training infrastructure.

In addition, the Portuguese Judicial Police is a co-founding member of ECTEG (European Cybercrime Training & Education Group) and participate actively to its activities, such as the e-First project in 2019 held on its facilities. The project targets as final product the delivery of a self-training platform available 24/7 specialised on cybersecurity and cybercrime.

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 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 e.g. on cybercrime law, digital forensics and ethics.

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.

2.13. 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.l).

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).

Romania ratified the Budapest Convention in 2004.

2.13.1. 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		

2.13.1.1. 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).

2.13.1.2. 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.). The beneficiaries of the CORSI-STS are public high-level authorities, such as the Parliament, the Presidency, the overnment, defence related entities, central and local administration and judicial related entities.

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.).

2.13.1.3. 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, 2020c).

Finally, Romania is part of the Europol's Joint Cybercrime Action Taskforce (J-CAT) (Europol, n.d.c).

2.13.1.4. 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.)

Within the Prosecutor's Office, which is under the responsibility of the High Court of Cassation and Justice, the Service for Preventing and Combating Cyber-Crime is specifically dedicated to fighting cybercrime and is made of two different units: the Office for Countering Cybercrime and the Office for Countering Crimes Committed with Credit Cards and other Electronic Payment Instruments. The service for Prevention and Combatting Cybercrime conducts investigation in case of cybercrime and acts as the permanent point of contact for the network created under the Budapest Convention.

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.

2.13.2. Synergies and potential interferences

'National cyber security system 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.

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).

SYNERGIES IN FIGHTING CYBER THREATS

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

2.13.3. 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.

2.14. SLOVENIA

Slovenia is 'a parliamentary democratic republic with a head of government, the prime minister, and a head of state, the president, who is directly elected. The government holds executive and administrative authority. The prime minister and ministers are elected by the Parliament. Slovenia has no regions, but is subdivided into 212 municipalities' (European Union, n.d.m).

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

The Slovenian Cyber Security Strategy was published in 2016 (Slovenian government, 2016). It foresees the enhancement of the capacity of the Police and the Judiciary to fight cybercrime, with a focus on digital forensics. This includes appropriate training of all LEAs operating in this field. The Strategy also underlines that knowledge in cybercrime is necessary for the 'successful prosecution of classic types of crime', which increasingly use the Internet. Objective 5 of the National Cybersecurity Strategy on the fight against cybercrime 'foresees actions on regular training on cybersecurity for law enforcement participating in the development of cyber capacities for public security and in combating cybercrime' (Slovenian government, 2016) (Council of Europe, n.d.a).

The Slovenian National Assembly adopted the Act on Information Security in 2018, which implements the NIS Directive into the Slovenian legal system (PISRS, 2018).

Slovenia ratified the Budapest Convention in 2004.

2.14.1. Roles and duties

In Slovenia, 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)
Information Security Administration	Uprava Republike Slovenije za informacijsko varnost	URSIV
SI-CERT	SI-CERT	SI-CERT
SIGOV-CERT	SIGOV-CERT	SIGOV-CERT
Criminal Police Directorate	Uprava kriminalistične policije	
- **Computer Investigation Centre**	Center za računalniško preiskovanje	
State Prosecutor's Office	Vrhovno državno tožilstvo Republike Slovenije	

2.14.1.1. National cybersecurity agency

The **Information Security Administration** (URSIV) is the competent national body for information security. It is under the responsibility of the Ministry of Public Administration. It was established in 2020 after the vote of the Information Security Act (2018) (Slovenian governement, 2021).

The URSIV is the central coordinating body at the strategic level of the national information security system and the single point of contact of the state for international cooperation in this field and with the European network of CSIRTs. The URSIV keeps the government and the National Security Council (SNAV) of the state informed in case of increased threat which could lead to a critical incident or cyberattack (Slovenian governement, 2021).

2.14.1.2. CSIRTs

SI-CERT is the Slovenian national CSIRT, while SIGOV-CERT is the governmental one.

Established in 1995, **SI-CERT** is the national CSIRT of Slovenia as defined in the Act on Information Security (Art. 28) (PISRS, 2018). SI-CERT is part of ARNES (Academic and Research Network of Slovenia) within the Sector of National Internet Infrastructure (SI-CERT,

n.d) (SI-CERT, n.d.a). It is the 'main contact point for reporting network security incidents involving systems and networks located in Slovenia' (Council of Europe, n.d.a).

SI-CERT performs risk and incident handling in accordance with Article 28 of the Information Security Act (PISRS, 2018), which defines following responsibilities:

- Offer of support, help and cooperation in case of incident;
- Sharing of data about risks and vulnerabilities with the affected systems' administrators, and issues warnings;
- Cooperation with CSIRT groups and security operation centres in Slovenia and CSIRT groups in other EU Member States;
- Raising the awareness of users in the area of cybersecurity;
- Cooperation with the competent national authority and offer of information upon request.

SI-CERT is a member of the CSIRTs Network.

SIGOV-CERT is the Slovenian governmental CERT of Slovenia. It is a young structure, created in 2019. Its constituency includes all networks, information systems and users of those systems managed by the Ministry of Public Administration of Slovenia. However, the Ministry of the Interior, the Ministry of Defence and the Slovenian Intelligence and Security Agency are responsible for ensuring the security of their networks and information systems (Slovenian government, 2021).

2.14.1.3. Judiciary

The State prosecution services of Slovenia are composed of:

- The **State Prosecutor General's Office**, which supervises and coordinates the work of eleven District State Prosecutors' Offices (State Prosecutor's Office, n.d.);
- The **Specialised State Prosecutor's Office**, which deals with the most complex criminal offences (State Prosecuror's Office, n.d.a).

State prosecutors operate at four levels:

- Supreme state prosecutors;
- Higher state prosecutors;
- District state prosecutors;
- Local state prosecutors.

State prosecutors perform their tasks in accordance with the Criminal Procedure Act (Policija, 2007). They can exercise their authority to give guidance and obligatory instructions to the Police during the investigation. The cooperation between the Slovenian Police and the prosecutors is ruled by the 'Decree on the cooperation of the State Prosecutorial Service, the Police and other competent State bodies and institutions in the detection and prosecution of perpetrators of criminal offences and the operation of specialised and joint investigation teams' (Official Journal of the Slovenian Republic, 2010).

State Prosecutors usually do not directly contact entities other than the Police, which means that direct contact/communication with CSIRTs is relatively rare.

'There are no separate departments for prosecution of cybercrime [within the State prosecution services], but some state prosecutors are specialised' in this area (Council of Europe, n.d.a).

If a case is related to both cybercrime and criminal organisations, it can fall under the competence of the Specialised State Prosecutor's Office, otherwise any of eleven District State Prosecutor Offices can be competent.

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

2.14.2. Synergies and potential interferences

According to the data collected via the interviews, synergies exist between the three communities, based on their specific roles and duties.

The CSIRT community can provide technical expertise to LE and the Judiciary, specifically on how the systems and networks work and on malware analysis, while LE provides investigative skills and knowledge in digital forensics. The Judiciary can provide legal support to the CSIRT about relevant provisions related to criminal offences and procedures.

Interviewees did not identify major interferences in the roles and duties of the three communities, however they highlighted that the communities have different interests and 'speak different languages', which can be challenging. An example was given by one of the experts interviewed, who experienced a situation where the CSIRT's interest was to inform its constituency of an incident, while the Police's interest was not to reveal the incident while investigating. In such cases however, LE and the CSIRT community usually coordinate to find the best way to act.

Another challenge highlighted during the interviews is the difficulty the communities may have in understanding each other. On the one hand for example, prosecutors and judges may encounter difficulty in understanding the technical details of a criminal offence in a cybercrime related case; on the other hand, a CSIRT representative may 'find difficult to understand what a prosecutor or judge needs from a legal point of view, and how the technical data/information could be used during criminal proceedings'. During the interviews it was suggested that this challenge could be addressed by organising joint seminars so the three communities could exchange knowledge and experience.

2.14.3. Examples of training

SI-CERT and LE representatives participate in the annual workshop organised by ENISA and Europol's European Cybercrime Centre (EC3). One interviewee explained that input provided during one of these workshops by European counterparts on how they cooperate was very beneficial: since then, the SI-CERT and the Slovenian Computer Investigation Centre try to organise informal workshops every three months to enhance their cooperation. Due to the pandemic, these workshops are currently organised online.

Additionally, once a year, the Computer Investigation Centre organises a joint meeting, to which the CSIRT community is invited.

During these joint events, the two communities exchange best practices and lessons learned. They present relevant cases and discuss them.

The experts interviewed were not aware of joint events or trainings involving the three communities, although such initiatives would, according to them, be very beneficial.

JOINT EVENTS TO FOSTER COOPERATION

Participation in yearly ENISA and EC3 workshops inspired SI-CERT to organise more joint workshops with Slovenian LE to enhance their cooperation.

2.15. SPAIN

Spain is 'a parliamentary democracy and constitutional monarchy with a head of government, the prime minister, and a head of state, the Monarch. A council of ministers is the executive branch and is presided over by the prime minister. Spain is a unitary state, composed of 17 autonomous communities and two autonomous cities with varying degrees of autonomy' (European Union, n.d.n).

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

The NCSS published in 2019 follows the 2017 NCSS and 2013 NCSS (CCN-CERT, 2019). It sets out a number of measures to 'reinforce capabilities or investigation and prosecution of cybercrime, to guarantee citizens security and protect rights and freedoms in cyberspace' (Line of actions 3) (CCN-CERT, 2019).

The NIS Directive has been implemented in 2018 by the Royal Decree 12/2018 (Spanish Official Journal, 2018).

Spain ratified the Budapest Convention in 2010.

2.15.1. Roles and duties

In Spain, 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 Cryptology Center	Centro Criptologico Nacional	
- **CSIRT of the National Cryptology Center**	Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional	CCN-CERT
National Cybersecurity Insitute	Instituto Nacional de Ciberseguridad	INCIBE
- **National Cybersecurity Insitute-CERT**	Instituto Nacional de Ciberseguridad-CERT	INCIBE-CERT
Office for Cyber Coordination	Oficina de Coordinación Cibernética	OCC
National Police	Policia Nacional	
- **Technological Investigation Unit**	Unidad de Investigación Tecnológica	UIT
○ **Central Brigade for Technological Research**	Brigada Central de Investigación Tecnológica	BCIT
Guardia Civil	Guardia Civil	
- **Group of Telematic Crime - Central Operational Unit**	Grupo de Delitos Telemáticos - Unidad Central Operativa	GDT
General Prosecutor's Office	Fiscal General del Estado	

2.15.1.1. National cybersecurity agency

Set up in 2002, the **National Cryptology Centre** (CCN) belongs to the **National Intelligence Centre** (CNI). Its role is to guarantee ICT security in public administration entities and security for systems which process, store or send out classified information (CCN, n.d.) (Council of the European Union, 2016). The CCN operates the CCN-CERT, the Spanish governmental CSIRT (CCN, n.d.).

If a cybercrime is detected during an intelligence investigation, the CNI contacts the Spanish LEAs to take actions. For cases falling under the scope of the NIS Directive, the Spanish Royal Decree 43/2021 (Spanish Official Journal, 2021a), which specifies how the CSIRTs, competent authorities and LEA should act in case of a major cyber incident, establishes that the CNI has to implement a common national platform for incident notifications: when a victim reports such a cyber incident to a CSIRT, it is reported on this national platform, accessible by the competent authorities and LEAs, where the latter can share information on the incident. The CNI does not usually communicate with the Judiciary. The LE acts as an intermediary.

Moreover, the CNI provides resources and training to the Spanish public sector on cybercrime related matters.

The Spanish **National Cybersecurity Institute (INCIBE)** was established in 2014. It provides cybersecurity services to businesses and professionals, and to the general public. Its role is also to raise awareness on risks and to promote mechanisms for the prevention of and reaction to cybersecurity incidents (INCIBE, n.d.) (Council of the European Union, 2016).

2.15.1.2. CSIRTs

In Spain the **CCN-CERT** is the governmental CSIRT**,** while **INCIBE-CERT** the national one.

The **CCN-CERT** belongs to the CCN. It was established in 2006. Its role is to handle cyber incidents affecting its constituency (classified systems and systems belonging to public administrations, companies and organisations of strategic interest).

When a incident related to cybercrime arises, CCN-CERT recommends to the victim(s) to report the crime to the LE and provides technical supports. It also disseminates to its constituency, including LEAs, new indicators of compromise (IOCs) obtained during the course of the investigation. If required by a judge, CCN-CERT can provide technical reports to the Police and/or support further technical investigations, especially in digital forensics (e.g. of mobile devices).

In cases of a major cyber incidents, the CCN-CERT acts as a national coordinator of the regional CSIRTs[24]. As regional CSIRTs are closer to victims, the CCN-CERT can decide to let them handle the incident, except in cases of cyberespionage, where only the CCN-CERT can be in charge and interact with victims.

CCN-CERT regularly and directly interacts with the National Police and Guardia Civil cybercrime units. One of the experts interviewed explained that CCN-CERT has Intrusion Detection Sensors (IDS) deployed in about 300 public organisations in Spain (central government, regional governments, etc.).

Private entities, including OES and digital services operators, belong to **INCIBE-CERT**'s constituency.

INCIBE-CERT can give technical support to Law enforcement and the Judiciary, but always in coordination with the Office of Cyber Coordination (OCC). The OCC can request any relevant information on the incidents from the CSIRTs. Criteria are established to determine which incidents must be communicated to the OCC depending on their impact (high/very high/critical).

INCIBE-CERT can be requested by the National Police and the Guardia Civil (which have cybercrime units) to provide technical support, the OCC must be informed of such requests.

[24] There are several regional CSIRTs in Spain, such as AndaluciaCERT, Catalonia-CERT, and CSIRT.gal.

One of the experts interviewed mentioned that digital 'forensics tasks are usually run by private companies. […] However, LE can ask INCIBE-CERT for its opinion on the forensics reports'.

INCIBE-CERT can be asked also by the Judiciary to provide technical reports, however this is rare. As emerged from the interviewed, it has happened that INCIBE was called upon to testify in court, but in general only written reports are communicated to the judges.

2.15.1.3. LE

The **National Police** and the **Guardia Civil** have their own cybercrime units. Some regional and local police forces also have cybercrime units (Council of Europe, n.d.e). It is the role of LE to communicate incidents to the Prosecutor's Office.

The Spanish national Police has a **Technological Investigation Unit (UIT)**. The UIT was created in 2012 within the General Directorate of the Police. It is responsible for investigating and prosecuting cybercrime at national level and acts as the 'E-Crime Prevention and Response Center' of the Police (Policia, n.d.). The UIT is made up of two brigades:

- The Central Brigade for Technological Research (BCIT);
- The Central Cybersecurity Brigade.

The BCIT is in charge of investigating all forms of crime related to computer activities (cyberattacks, threats or insults on the Internet, child sexual abuse, and frauds).

The **Group of Telematic Crime** (GDT) of the Central Operational Unit of the Guardia Civil was created in 1996 to investigate crimes committed on the Internet. Its competence now covers cybercrime, defined as criminal behaviours carried out through and against information systems. Technological Research Teams (Equipos de Investigación Tecnológica - EDITE) were created in each Spanish province to support the GDT's work.

Within CNPIC (National Critical Infrastructure Protection and Cybersecurity Centre), the **Office for Cyber Coordination (OCC)** was first created as the Cybernetic Coordination Unit about ten years ago, and renamed into OCC in 2020. On the one hand, OCC is responsible for the technical coordination with the n/g CSIRTs (INCIBE-CERT and CCN-CERT), on the other hand, it acts as the point of contact (PoC) with the Law enforcement cybercrime units of Spanish LEAs (Council of Europe, n.d.e).

Regional police forces interact with the OCC through the Intelligence Center for Counter-Terrorism and Organised Crime (CITCO) of the Spanish Ministry of the Interior. Furthermore, in March 2021 the Home Office approved the Strategic Plan Against Cybercrime, which reflects different cooperation tools between national LEAs and regional police forces coordinated by OCC (Ministry of Home Affairs, 2021).

Finally, Spain is part of Europol's Joint Cybercrime Action Taskforce (J-CAT) (Europol, n.d.c).

2.15.1.4. Judiciary

The **General Prosecutor's Office** has a cybercrime unit and a network of specialised prosecutors. The General Prosecutor's Office delimited what is to be understood as cybercrime in its Instruction 2/2011 of 11 October 2011 'Concerning Specialised High Prosecutors on Computer-related Crimes and the Sections for computer-related crimes of the Prosecutor's offices' (General Prosecutor's Office, 2011).

The cybercrime unit is coordinated by a prosecutor supported by two deputy prosecutors. In each region, a Provincial Prosecutor´s Office is responsible for the respective provincial unit. Every specialised unit has the number of prosecutors considered necessary depending on the volume of relevant cases.

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

2.15.2. Synergies and potential interferences

Existing synergies are mostly bilateral: between CSIRT and LE, and between LE and the Judiciary. CSIRTs do not usually interact with the Judiciary. The cooperation was assessed by the interviewees as good, overall.

EXISTING SYNERGIES

The existing synergies, ensuring good cooperation, could benefit from more joint trainings and better knowledge of each other tasks.

As part of the implementation of the NIS Directive, the OCC has been designated as the National Competent Authority for the OES for the private sector (European Commission, n.d.c) (Spanish Official Journal, 2021a) (Spanish Official Journal, 2018a). In addition, as part of the implementation of the 2013 Directive on Attacks against Information Systems, OCC has been designated as the operational national PoC. Therefore, the OCC receives all incident reports from OES. Its staff analyses the information received and sends it to the relevant LE units. The OCC also does cyber intelligence.

According to the Royal decree 43/2021 (Spanish Official Journal, 2021a), the reference CSIRTs (CCN-CERT and INCIBE-CERT) must report incidents presenting characteristics of a crime to the OCC. Criteria are established to determine which incidents must be communicated to the OCC depending on their impact (high/very high/critical impact). CCN and INCIBE share ticketing tools (one each, although a common tool is planned to be implemented within two years) to report incidents. The OCC analyses all information received from the CSIRTs and completes a report, and updates it with any new elements received. It can request any relevant information on the incidents from the CSIRTs. The OCC coordinates with LE and shares the report with them via encrypted email.

CSIRTs provide technical expertise to LE, whereas LE and the Judiciary are in charge of investigating and prosecuting crimes. As highlighted during the interviews, cooperation has proven to be necessary in several situations requiring quick action, such as taking down domains, sending request to preserve evidence in other countries, and seizing servers. One example of synergy was the successful cooperation between LE and the CCN-CERT during the incident at the Spanish National Employment Office in March 2021.

One interviewee explained that in 2020, a new working group on cybersecurity was established at the national level as a technical group dedicated to the implementation of cybersecurity measures, in which the Judiciary, at both regional and national levels, is involved.

Although no major interferences were experienced by the interviewees, some challenges due to a difference of interests between the communities were identified. For example, when an incident occurs, LE needs to preserve the system(s) impacted to conduct investigations, whereas the CSIRT wants to act quickly to solve the incident, which it cannot do while the Police is working. In such cases, LE and the CSIRT usually agree that LE make a copy of the server to preserve evidence. This allows the CSIRT to start solving the incident with less delay.

Challenges related to the lack of technical skills in LE units and the lack of knowledge of legal procedures in the CSIRTs were also highlighted during the interviews. According to one of the experts interviewed, more training opportunities for the CSIRTs to have better knowledge of the legal procedures related to the fight against cybercrime would be useful. On the other hand, training of judiciary representatives would also be useful to improve their understanding of the CSIRTs' scope of work. To address these challenges, INCIBE's legal department reviews the requests received from judges before sending them to the technical department, so they are better understood, and the other way around.

The following recommendations were formulated during one interview to address potential challenges in the cooperation between the three communities:

- To broaden the legal scope allowing the three communities to exchange information;
- To set up common formal procedures to exchange information and send requests;

- To set up more IT and cybersecurity training for LE/Judiciary;
- To improve the LE/Judiciary's knowledge of the CSIRTs' functions and tasks.

2.15.3. Examples of training

One of the experts interviewed highlighted that the OCC recently received a budget for technical training: in September 2021, it will organise a technical training for OCC and LE units, which will focus on certified ethical hackers and OSINT techniques.

Furthermore, the OCC and INCIBE have an agreement for the CyberEx exercise (INCIBE, 2021), conducted with OES' technical team. CyberEx focuses on cyber incident handling.

As the governmental CSIRT, CCN-CERT is responsible for training civil servants and cybersecurity experts in Spain. Every year, it organises about twenty courses on technical issues (e.g. IDS, digital forensics courses, and collection of e-evidence). LE representatives participate in these courses. CCN-CERT also provides specific courses to the National Police and the Guardia Civil in the Police Academy and Guardia Civil Academy. Although CCN-CERT provides training to LE, it does not participate in joint trainings with them.

CCN-CERT also has a very large portfolio of cybersecurity tools, norms and publications available for the public sector, including LE and the Judiciary.

Finally, CCN-CERT organises workshops on cybersecurity related matters within the group CSIRT.es, which gathers CERTs from private and public sector, as well as LEAs.

INCIBE-CERT provides technical training to LE and the Judiciary:

- The Cybersecurity Summer BootCamp (INCIBE, n.d.a), organised annually since 2016 by INCIBE and the Organization of American States (OAS). It provides both strategic and practical trainings. The Cybersecurity Summer bootcamp goes from basic to medium level. It gives LE and the Judiciary (prosecutors and judges) knowledge and reference on topics like malware analysis, and OSINT. CCN-CERT representatives and private companies' representatives are usually invited as speakers. The Cybersecurity Summer bootcamp is assessed as very useful for the Judiciary to enhance their technical knowledge. As LE have a better understanding of the technical aspects, they come to the Cybersecurity Summer bootcamp to enhance specific skills, such as malware analysis;
- A "Basic Cybersecurity for Security Forces and Bodies" MOOC, designed for LE: it is a basic course presenting the tasks of the police forces in fighting cybercrime: prevention, awareness and protection of citizens against cybercrime (INCIBE, n.d.c). According to one of the interviewees, about 1,780 participants already attended this MOOC;
- An "Advanced Cybersecurity for Security Forces and Bodies" MOOC, designed for LE: an advanced course which covers advanced and specific topics such as malware, open source intelligence and the deep web (INCIBE, n.d.c). According to one of the interviewees, about 1,820 students were enrolled.

In addition, the Spanish Police Studies Institute (Instituto de estudios de la Policía) has developed a Master's in cybercrime, aimed at chief inspectors, inspectors or sergeants who are the heads of groups or units tackling cybercrime. The first edition was initiated in October 2016.

Finally, the Spanish National Police School (Escuela Nacional de Policía) and ECTEG created the C1b3rWall Academy in 2018, which led to the Congress on Digital Security and Cyberintelligence, organised in 2019 at the headquarters of the National Police School (ECTEG, 2020). The C1b3rWall Academy currently offers online training dedicated to LEAs on topics such as cryptography, security and infrastructures, digital forensic analysis, legal hacking, blue team, red team, and cryptocurrencies (ECTEG, 2020).

2.16. 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.t).

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.) (Comprehensive cyber security action plan 2019–2022, 2019).

Sweden ratified the Budapest Convention in 2021.

2.16.1. Roles and duties

In Sweden the following authorities and departments, in particular ([25]), 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)
Swedish Civil Contingencies Agency	Myndigheten för samhällsskydd och beredskap	MSB
CERT-SE	Sveriges nationella Computer Security Incident Response Team	CERT-SE
National Centre for Security in Control Systems for Critical Infrastructure	Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet	NCS3
Swedish Post and Telecom Authority	Post-och telestyrelsen	PTS
Swedish Police Authority	Polismyndigheten	
- **Swedish Police CERT**	Polisens CERT	PM CERT
Swedish Prosecution Authority	Åklagarmyndigheten	
Swedish Economic Crime Authority	Ekobrottsmyndigheten	
Swedish National Courts Administration	Domstolsverket	

2.16.1.1. 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 2.16.1.

([25])The authorities and departments presented here are the main authorities/departments responsible for preventing, analysing and fighting cybercrime. Other authorities/departments not presented here might play a role on an ad hoc basis.

The National Centre for Security in Control Systems for Critical Infrastructure is in charge of raising awareness and disseminating knowledge and experience of cybersecurity. Established in 2008, it works in collaboration with the MSB.

2.16.1.2. CSIRTs

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

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

PM-CERT, the Swedish Police CERT is responsible for protecting the Police's IT infrastructure and network.

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.).

2.16.1.3. 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), which includes a Cybercrime unit.

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). 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).

Finally, Sweden is part of the Europol's Joint Cybercrime Action Taskforce (J-CAT) (Europol, n.d.c).

2.16.1.4. 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.

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

2.16.2. 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, 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'.

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).'

A CULTURE OF SYNERGY

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

2.16.3. 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 SC3 organises some training also for the prosecutors.

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.).

2.17. FINAL REMARKS

2.17.1. 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 and the technical expertise, 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 (prosecutors or 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, who provides technical reports and whose delegates may be invited as expert witnesses before the courts.

The interviewees provided examples of training activities involving more than one community, sometimes in the form of workshops or joint exercises. These joint training initiatives help enhance the competences required to respond to cybercrime. As one of the interviewees mentioned, joint trainings help the three communities to ‘harmonise terms, language and understanding […] of cyber and cybercrime’. The three communities can then 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. This also ‘helps them better understand their own role in the broader picture’. 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. This is especially important as the interviews showed that each community tends to lack a precise understanding of the others’ tasks. In fact, in most countries, interviewees of the different communities provided different answers in some entries of the SoD matrix.

Moreover, 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)). They also need to be familiar with existing architecture including:

- The Blueprint for a Coordinated Response to Large Scale Cybersecurity Incidents and Crises (‘the Blueprint’) (European Commission, 2017), the CSIRTs network and the

European Cyber Crises Liaison Organisation ('EU CyCLONe') network ([26])), as well as the European Cybercrime Centre ('EC3') and the Joint Cybercrime Taskforce ('J-CAT') at the European Union Agency for Law Enforcement Cooperation ('Europol'), the EU Law Enforcement Emergency Response Protocol ('EU LE ERP') and the 24/7 Points of Contact Network under the Council of Europe Convention on Cybercrime ([27]) (European Commission, 2021, p. Recital (5));

- The NIS Cooperation Group, the EU Intelligence and Situation Centre ('EU INTCEN'), the Cyber Diplomacy Toolbox (Council of the European Union, 2017h) and cyber defence-related projects launched under the Permanent Structured Cooperation (PESCO) ([28]) (European Commission, 2021, p. Recital (5));
- ENISA that, as foreseen in the Cybersecurity Act (Article 7 par. 1), supports 'operational cooperation among Member States, Union institutions, bodies, offices and agencies, and between stakeholders' (European Parliament and Council of the European Union, 2019) (European Commission, 2021, p. Recital (5));
- Integrated Political Crisis Response ('IPCR') arrangements via which the EU is able to 'coordinate its political response to major crises' (European Commission, 2021, p. Recital (5)).

Finally, the communities need to develop their competences and build organisational and intercultural skills to liaise effectively with their counterparts from other EU/EEA Member States.

2.17.2. Differences of interests between the communities

Although the majority of interviewees experienced no major interferences in the cooperation between the three communities, one of the main challenges identified was the difference of interests between the communities, due to their distinct roles and duties.

For example, at the beginning of an investigation, the priority for both LE and the Judiciary is to gather as much evidence as possible while keeping the case from the public, and to catch the perpetrator(s), while the CSIRT's work is to immediately stop the incident and mitigate damage. CSIRTs often want to quickly inform their constituency and to announce that the incident or attack has been stopped.

Furthermore, restoring a system after a cyberattack sometimes means losing precious evidence, which means that LE must make a copy of the said system prior to the CSIRT's intervention. This can take up to a few days as it must be done following legal procedures, and thus impacting the CSIRT's response, which does not follow the same timescale as that of the legal process. However, as underlined by one of the experts interviewed, 'this is all about maintaining the balance between handling the incident and investigating it by helping each other and without interfering with each other's work'.

Some organisational issues were also highlighted, especially the lack of resources allocated to the fight against cybercrime, often resulting in a lack of capacity to efficiently deal with every

([26]) The 'EU CyCLONe aims at enabling rapid cyber crisis management coordination in case of a large-scale cross-border cyber incident or crisis in the EU by providing timely information sharing and situational awareness amongst competent authorities and is supported by ENISA, which provides the secretariat and tools. EU CyCLONe operates at the "operational level', which is the intermediate in between technical and strategic/political levels.
The goals of EU CyCLONe are to:

- establish a network to enabling the cooperation of the appointed national agencies and authorities in charge of cyber crisis management;
- provide the missing link between the EU CSIRTs Network (technical level) and the EU political level.

Due to its importance in the EU cybersecurity landscape, the European Commission proposal for the revised NIS Directive envisions in Article 14 the formal establishment of the European Cyber Crises Liaison Organisation Network (EU – CyCLONe)' (ENISA, 2021m).
([27]) 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).
([28]) As stated in the Footnote 7 of the Commission Reccomandation (EU) 2021/1086 on building a Joint Cyber Unit (European Commission, 2021), 'In particular, the PESCO projects on 'cyber rapid response teams and mutual assistance in cyber security' coordinated by Lithuania and on 'cyber and information domain coordination centre' coordinated by Germany'.

reported incident (CSIRTs and LE) and sometimes leading to an important lack of knowledge of cybercrime related matters (Judiciary).

2.17.3. 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). Luckily, 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 sixteen 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 as online meetings tend to be less time-consuming than in-person meetings.

Most of the interviewees highlighted that meetings in person occurred less frequently, although in some countries 'Face-to-face meetings continued to take place to discuss sensitive matters'. 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'. Some meetings and court hearings were suspended and this represented a challenge, although it was mentioned during an interview that in one of the countries analysed online courts were arranged and this new practice allowed to drastically diminish the backlog.

In general, 'the pandemic crisis did not negatively impact the effectiveness of the cooperation' between the CSIRT, LE and judiciary communities. Most of the interviewees noted that at the peak of the crisis, the COVID-19 restrictions '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 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.'

Interviewees however unanimously underlined that in-person meetings provide more opportunities to network and develop trust. Concerns were expressed by the interviewees regarding establishing trust with new members of the communities in a merely virtual environment. The fact that such meetings cannot take place due to COVID-19 restrictions might in the long run impact the cooperation among the communities as people get to know each other less than if they regularly met in person.

3. CONCLUSIONS AND WAYS FORWARD

3.1. CONCLUSIONS

This report is an updated and expanded version of the *2020 Report on CSIRT-LE Cooperation: A Study of Roles and Synergies among Selected EU Member States/EFTA Countries* published in January 2021 (ENISA, 2021a).

Data for this report has been collected via desk research, interviews and compilation of a Segregation of Duties (SoD) matrix. This report addresses the cooperation between CSIRTs and LE and their interaction with the Judiciary, by discussing their roles, synergies and interferences, competences and training initiatives.

The analysis in this report focused on Belgium, Czechia, Estonia, Finland, France, Germany, Ireland, Italy, Luxembourg, Norway, Poland, Portugal, Romania, Slovenia, Spain and Sweden.

Using the analysis of the data collected, the conclusions summarised below were drawn.

- 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. A Second Additional Protocol to the Cybercrime Convention, on enhanced co-operation and disclosure of electronic evidence adopted by the Committee of Ministers of the Council of Europe in November 2021 'should be opened for signature in May 2022' (Council of Europe, n.d.f). 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 **LEAs' activities related to 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 and between LE and CSIRTs.

- Normally 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 cooperation with other communities, particularly the CSIRT community, is very important to support preventive strategies. In particular, the responsibility of cybercrime prevention is shared with CSIRTs since in most of the cases they are the first of the three members detecting cyber incidents of criminal nature within their constituents.
- CSIRTs and LEAs **need to cooperate to decrease the risk of evidence being compromised or destroyed**.
- CSIRTs and LE may 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 and how to enhance protection against future cybercrimes.
- **CSIRTs** may be called **as witnesses in court**, although this is not practised in all the countries analysed. Moreover, when it happens, CSIRTs often provide **written reports** and are rarely physically called to court.
- 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 **trainings** within each community. Most of the joint trainings involve two of the communities (e.g. CSIRTs and LE, or LE and the Judiciary); however, there is a need for further initiatives and for trainings and exercises that involve the three communities together.
- **Secondment opportunities** between the CSIRTs and the LE **are rare**. The reason why varies depending on the country (e.g. lack of resources, organisational aspects, and/or level of maturity of the CSIRTs).
- 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 face-to-face 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 in some instance the norm and the communities adapted to the new way of working**. Establishing trust with new members of the communities in a merely virtual environment can be challenging,** but alternating virtual and physical meetings and/or organise hybrid meetings (meetings with some participants in person and some participating remotely), when possible, might help. 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.

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.

3.2. WAYS FORWARD

3.2.1. Possible extension of the analysis to additional countries

This report could be further expanded to cover all the remaining EEU/EEA Member States[29].

With some adaptation of the methodology presented in the 2020 ENISA Report on CSIRT-LE cooperation (ENISA, 2021a) the analysis could be extended also to additional countries other than EU/EEA Member States.

3.2.2. 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 with the support of Europol's EC3 has developed a handbook and a toolset which has been published in January 2021 (ENISA, 2021). Such material has been piloted through two training sessions (in August and October 2021) and further improved by ENISA in 2021 based on the feedback received. In these pilot sessions representatives from Member States (from CSIRTs, LE and Judiciary) and some European Union Institutions, Bodies and Agencies (EUIBAs) discussed, also based on scenarios, topics related to the cooperation across the three communities and learned more about these communities, including their needs and potential synergies they could exploit.

Additional training material could be developed in the future based on the results of an analysis extended to the remaining EU/EEA Member States[30], and possibly also other countries, e.g. Western Balkans [31].

3.2.3. 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 EU/EEA Member State that could offer such competences, would help CSIRTs, LE and the Judiciary become more aware of the skills and strengths of other communities in their country, and also across the EU and EEA 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).

3.2.4. 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 authorities could easily consult to obtain information on which authorities play a role in the response to cyber incidents of criminal nature These support systems can aid in decision-making and in taking actions in cases where the evidence is located in several countries.

3.2.5. Develop common platforms to share information between LE and CSIRT communities

Developing a common information sharing platform at national level could facilitate information exchange between the three communities during the investigation of a cyber related criminal

[29] The EU/EEA Member States not covered in this report are: Austria, Bulgaria, Croatia, Cyprus, Denmark, Greece, Iceland, Hungary, Latvia, Liechtenstein, Lithuania, Malta, Netherlands, and Slovakia.
[30] See previous footnote.
[31] For more information on Western Balkans, see for instance (European Commission, n.d. b)

offence. This could also help harmonise information sharing processes and as a consequence limit the potential delays to the police investigation and the CSIRT intervention.

3.2.6. Organise joint training and exercises for the three communities

Wherever possible initiatives involving all three communities should take place at national and cross-countries level. Examples of these initiatives are the two pilot training sessions organised by ENISA in 2021 and described above.

Joint training 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.

4. REFERENCES

Åklagarmyndigheten. (n.d.). Retrieved September 2020, from https://www.aklagare.se/en/

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

ANACOM. (n.d a). Retrieved September 2020, from https://www.anacom.pt/render.jsp?contentId=1133069

ANSSI. (2018). *CERT-FR description – RFC 2350* . Retrieved November 29, 2021, from https://cert.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. b). *Programme d'incubation de CSIRT*. Retrieved November 2021, from https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/programme-dincubation-de-csirt/

ANSSI. (n.d.). *The French National Digital Security Strategy*. Retrieved September 2020, from https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/

Arma dei Carabinieri. (n.d.). Retrieved November 19, 2021, from https://www.carabinieri.it/

Belgian Police. (n.d.). *Recherche locale & Computer Crime Unit – Police Locale Regio Tielt*. Retrieved January 04, 2022, from https://www.police.be/villagepolicier/fr/police-locale/recherche-locale-computer-crime-unit-police-locale-regio-tielt

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

BMWi. (2016). Retrieved June 2021, from https://www.de.digital/DIGITAL/Redaktion/EN/Publikation/digital-strategy-2025.pdf?__blob=publicationFile&v=9#:~:text=The%20Digital%20Strategy%202025%20programme,which%20areas%20require%20immediate%20action%20(Consulted%20on%20June%2018,%202021)

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

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

BSI. (n.d.). Retrieved September 2020, 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 September 2020, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=4

BSI. (2019). *The State of IT Security in Germany in 2019*. Retrieved June 2021, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2019.pdf?__blob=publicationFile

BSI. (n.d. a). Retrieved November 29, 2021, from RFC-2350: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KRITIS/rfc2350_CERT-Bund_txt.asc?__blob=publicationFile&v=1

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

CCB. (2019). *THE EUROPEAN NIS DIRECTIVE IS TRANSPOSED INTO BELGIAN LAW*. Retrieved June 2021, from https://ccb.belgium.be/en/news/european-nis-directive-transposed-belgian-law

CCB. (2021). *National Cybersecurity Strategy*. Retrieved 2021 June, from https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf

CCB. (n.d. a). *Incident Handling By CERT.be: General Conditions*. Retrieved June 25, 2021, from https://www.cert.be/en/incident-handling-certbe-general-conditions

CCB. (n.d. b). *Government*. Retrieved June 05, 2021, from https://ccb.belgium.be/en/government

CCB. (n.d. c). *Critical infrastructure*. Retrieved 11 24, 2021, from https://ccb.belgium.be/en/critical-infrastructure

CCB. (n.d.). *Organisation*. Retrieved June 04, 2021, from https://ccb.belgium.be/en/organisation

CCIS. (n.d.). Retrieved September 2020, from https://www.ntnu.edu/ccis

CCN. (n.d.). Retrieved June 2021, from https://www.ccn-cert.cni.es/en/about-us/mission-and-objectives.html

CCN-CERT. (2019). *National Cybersecurity Strategy of Spain*. Retrieved May 2021, from https://www.ccn-cert.cni.es/en/about-us/spanish-cybersecurity-strategy-2013.html

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

Central Forensic Laboratory of the Police. (n.d.). *Computer examination*. Retrieved from https://clkp.policja.pl/cfl/examinations-and-proje/examinations-in-cflp/computer-examination/90842,Computer-examination.html

CEPOL. (2013). *Finland hosts a CEPOL course on how to combat cybercrime* . Retrieved from https://www.cepol.europa.eu/media/blog/finland-hosts-cepol-course-how-combat-cybercrime

CEPOL. (2018). *Training catalogue 2018*. Retrieved from https://www.cepol.europa.eu/sites/default/files/Training%20Catalogue%202018.pdf

CERT Polska. (2018). *Annual report on the activities of CERT Polska*. Retrieved July 2021, from https://www.cert.pl/en/uploads/docs/Report_CP_2018.pdf

CERT Polska. (n.d.). Retrieved July 2021, from https://cert.pl/en/about-us/

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

CERT.be. (n.d). Retrieved June 2021, from CERT.be: https://cert.be/en

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

CERT.PL. (2020). *Lista ostrzeżeń przed niebezpiecznymi stronami.* Retrieved September 29, 2021, from https://cert.pl/posts/2020/03/ostrzezenia_phishing/

CERT.PL. (n.d.). MWDB. Retrieved September 27, 2021, from https://mwdb.cert.pl (password required)

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-FR. (n.d.). *INTERCERT-FR*. Retrieved November 2021, from CERT-FR: https://www.cert.ssi.gouv.fr/csirt/intercert-fr/

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 September 2020, from https://cert.ro/vezi/document/RFC2350-CERT-RO

CERT-RO. (n.d.b). *Cyber security strategy of Romania*. Retrieved September 2020, from https://cert.ro/vezi/document/NCSS-Ro

CERT-SE. (2015). Retrieved September 2020, from RFC2350: https://www.cert.se/rapporter/RFC_2350_CERT-SE.pdf

CIRCL. (2020, 08 16). *CIRCL*. Retrieved September 2020, 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.d.a). *CERT.PT*. Retrieved September 2020, from https://www.cncs.gov.pt/en/certpt_en/

CNCS. (n.d.b). *Centro Nacional de Cibersegurança*. Retrieved September 2020, 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/

CNCS. (n.d.e). *CERT.PT.* Retrieved November 29, 2021, from https://www.cncs.gov.pt/pt/certpt/

CNCS. (n.d.f). *Sobre Nós.* Retrieved November 29, 2021, from https://www.cncs.gov.pt/pt/sobre-nos/#missao

Code of Criminal Procedure. (2021). *Article 706-105-1*. Retrieved November 2021, from https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043881787

Code of Criminal Procedure. (2021a). *Article 706-72*. Retrieved November 2021, from https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311575/2021-09-19

Comprehensive cyber security action plan 2019–2022. (2019, March). Retrieved November 29, 2021, from Swedish Civil Contingencies Agency (MSB): https://rib.msb.se/filer/pdf/28898.pdf

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. (2020a, March 27). *Cybercrime and COVID-19*. Retrieved November 29, 2021, from News: https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/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. (2020c, August 21). *Romania National Police*. Retrieved September 2020, 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. (n.d.a). *Country Wiki - Slovenia*. Retrieved July 2021, from https://www.coe.int/en/web/octopus/-/slovenia?p_p_col_id=column-4&p_p_lifecycle=0&p_p_mode=view&p_p_state=normal

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 Europe. (n.d.c). *Country Wiki - Finland.* Retrieved from https://www.coe.int/en/web/octopus/-/finland?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 Europe. (n.d.d). *Country Wiki - Italy*. Retrieved July 2021, from https://www.coe.int/en/web/octopus/-/italy?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 Europe. (n.d.e). *Country Wiki - Spain*. Retrieved June 2021, from https://www.coe.int/en/web/octopus/-/spain?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 Europe. (n.d.f). *Second Additional Protocol to the Cybercrime Convention adopted by the Committee of Ministers of the Council of Europe*. Retrieved November 26, 2021, from https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe

Council of Europe. (n.d.g). *Octopus Conference 2021 - Key messages*. Retrieved November 26, 2021, from https://rm.coe.int/octopus-conference-2021-key-messages-v18nov2021/1680a494e6

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://data.consilium.europa.eu/doc/document/ST-7588-2015-REV-2-DCL-1/en/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. (2016). *7th Round of Mutual Evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on Spain.* Retrieved July 2021, from https://data.consilium.europa.eu/doc/document/ST-6289-2016-REV-1-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 September 8, 2020, 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 September 2020, 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

Council of the European union. (2017d). *Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on Estonia.* Retrieved June 2021, from https://data.consilium.europa.eu/doc/document/ST-10953-2015-DCL-1/en/pdf

Council of the European Union. (2017e). *Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Ireland.* Retrieved July 2021, from https://data.consilium.europa.eu/doc/document/ST-7160-2017-REV-1-DCL-1/en/pdf

Council of the European Union. (2017f). *Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Poland.* Retrieved July 2021, from https://data.consilium.europa.eu/doc/document/ST-14585-2016-REV-1-DCL-1/en/pdf

Council of the European Union. (2017g). *Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of the European policies on preventing and combating cybercrime' - Report on Belgium.* Retrieved June 2021, from https://data.consilium.europa.eu/doc/document/ST-8212-2017-REV-1-DCL-1/en/pdf

Council of the European Union. (2017h, June 19). *Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") of 19 June 2017 (9916/17).* Retrieved November 26, 2021, from https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf

CSIRT-GOV. (n.d.). Retrieved August 2021, from https://csirt.gov.pl/cer

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 September 2020, 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

Department of Justice and Equality. (2020). *Cybercrime: Current Threats and Responses.* Retrieved June 2021, from https://www.justice.ie/en/JELR/Cybercrime_-_Current_Threats_and_Responses.pdf/Files/Cybercrime_-_Current_Threats_and_Responses.pdf

Domstol. (n.d.). Retrieved September 2020, from https://www.domstol.no/en/the-courts-of-justice/The-ordinary-courts-of-Norway/The-Supreme-Court/

DPP. (n.d.). Retrieved June 2021, from https://www.dppireland.ie/about-us/

ECTEG. (n.d.). Retrieved September 2020, from https://www.ecteg.eu/running/first-responders/

ECTEG. (2020). *C1b3rwall Academy*. Retrieved from https://www.ecteg.eu/c1b3rwall-academy-en/

ECTEG. (2021). *E-First: First responders e-learning package*. Retrieved July 2021, from https://www.ecteg.eu/course-packages/first-responders/

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

EFTA. (n.d.). *EEA Agreement*. Retrieved September 2020, 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

e-GA. (2021). *National Cyber Security in Practice* . Retrieved from https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf

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/

Ekobrottsmyndigheten. (n.d.). Retrieved September 2020, from https://www.ekobrottsmyndigheten.se/en/

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. (2017b). *National Cyber Security Strategy 2016.* Retrieved June 2021, from https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/170426-bsi-enisa-nlo-presentation-v2.pdf

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. (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. (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. (2021a). *2020 Report on CSIRT-LE Cooperation: A study of roles and synergies among selected EU Member States/EFTA countries.* Retrieved from https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation/

ENISA. (2021m, May 19). *EU Member States test rapid Cyber Crisis Management (Press Release).* Retrieved November 26, 2021, from https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-rapid-cyber-crisis-management

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

Estonian Ministry of Economic Affairs and Communications. (2019). *National Cyber Security Strategy of Estonia*. Retrieved June 2021, from https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Eurojust. (n.d.b). *European Judicial Cybercrime Network*. Retrieved September 2020, from http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx

European Commission. (2017, September 12). *Commission Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises.* Retrieved November 26, 2021, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2017.239.01.0036.01.ENG&toc=OJ%3AL%3A2017%3A239%3ATOC

European Commission. (2021, June 23). *Commission Reccomandation (EU) 2021/1086 on building a Joint Cyber Unit.* Retrieved November 26, 2021, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021H1086&rid=16

European Commission. (n.d. b). *Western Balkans*. Retrieved November 26, 2021, from https://ec.europa.eu/info/research-and-innovation/strategy/strategy-2020-2024/europe-world/international-cooperation/western-balkans_en

European Commission. (n.d.c). *Implementation of the NIS Directive in Spain*. Retrieved July 2021, from https://digital-strategy.ec.europa.eu/en/policies/nis-directive-spain

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 September 2020, 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. (2019, April 17). *Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 52.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

European Union. (n.d.a). *Country profile - Belgium*. Retrieved 2021 June, from https://europa.eu/european-union/about-eu/countries/member-countries/belgium_en

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

European Union. (n.d.c). *Estonia*. Retrieved June 2021, from https://europa.eu/european-union/about-eu/countries/member-countries/estonia_en

European Union. (n.d.d). *France*. Retrieved September 2020, from https://europa.eu/european-union/about-eu/countries/member-countries/france_en

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

European Union. (n.d.f). *Germany*. Retrieved July 2021, from https://europa.eu/european-union/about-eu/countries/member-countries/germany_en

European Union. (n.d.g). *National Judicial System - France*. 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). *Italy*. Retrieved July 2021, from https://europa.eu/european-union/about-eu/countries/member-countries/italy_en

European Union. (n.d.i). *Luxembourg*. Retrieved September 2020, from https://europa.eu/european-union/about-eu/countries/member-countries/luxembourg_en

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

European Union. (n.d.k). *Portugal*. Retrieved September 2020, from https://europa.eu/european-union/about-eu/countries/member-countries/portugal_en

European Union. (n.d.l). *Romania*. Retrieved September 2020, from https://europa.eu/european-union/about-eu/countries/member-countries/romania_en

European Union. (n.d.l.). Retrieved September 2020, from https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-se-en.do?member=1

European Union. (n.d.m). *Slovenia*. Retrieved July 2021, from https://europa.eu/european-union/about-eu/countries/member-countries/slovenia_en

European Union. (n.d.n). *Spain*. Retrieved June 2021, from https://europa.eu/european-union/about-eu/countries/member-countries/spain_en

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

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

European Union. (n.d.q). *Size and population* . Retrieved from https://europa.eu/european-union/about-eu/figures/living_en#size

European Union. (n.d.r). *Ireland.* Retrieved June 2021, from https://europa.eu/european-union/about-eu/countries/member-countries/ireland_en

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

European Union. (n.d.t). *Sweden*. Retrieved September 2020, from https://europa.eu/european-union/about-eu/countries/member-countries/sweden_en

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 September 2020, from https://nsm.no/om-oss/historien-om-nsm/felles-cyberkoordineringssenter-fcks-etableres

Federal Police. (2019). *Rapport annuel de la police fédérale*. Retrieved from https://rapportannuel.policefederale.be/securite/securite-en-ligne/

FinansCERT. (n.d.). Retrieved September 2020, from http://www.finanscert.no/engelsk.html

Finnish Security Committee. (2019). Retrieved July 2021, from National Cybersecurity Strategy of Finland: https://turvallisuuskomitea.fi/wp-content/uploads/2018/09/Cyber-Strategy-for-Finland.pdf

FM-CERT. (n.d.). Retrieved September 2020, from https://www.forsvarsmakten.se/sv/

French Senate. (2020). *Cybercriminalité : un défi à relever aux niveaux national et européen.* Retrieved June 2021, from http://www.senat.fr/rap/r19-613/r19-613_mono.html#toc163

General Prosecutor's Office. (2011). Retrieved June 2021, from https://www.fiscal.es/memorias/estudio2016/INS/INS_02_2011.html

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

GNCCB. (n.d.). *Garda National Cyber Crime Bureau (GNCCB).* Retrieved July 2021, from https://www.garda.ie/en/about-us/organised-serious-crime/garda-national-cyber-crime-bureau-gnccb-/

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

GOVCERT.LU. (n.d.a). *About us*. Retrieved November 29, 2021, from https://www.govcert.lu/en/constituency/

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

Government of Ireland. (2019). Retrieved June 2021, from National Cyber Security Strategy: https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf

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

Guardia di Finanza. (n.d.). Retrieved November 19, 2021, from https://www.gdf.gov.it/

HCPN. (n.d.). Retrieved September 2020, from https://hcpn.gouvernement.lu/en/service.html

HelseCERT. (n.d.). Retrieved September 2020, 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

INCIBE. (2021). *CyberEx*. Retrieved from https://www.incibe-cert.es/en/international-cyberex

INCIBE. (n.d.). *INCIBE*. Retrieved July 2021, from https://www.incibe-cert.es/en/what-incibe-cert

INCIBE. (n.d.a). *Cybersecurity Summer BootCamp 2021*. Retrieved from https://www.incibe.es/en/summer-bootcamp

INCIBE. (n.d.c). *Ciberseguridad Básica para Fuerzas y Cuerpos de Seguridad*. Retrieved from https://www.incibe.es/formacion/ciberseguridad-para-fuerzas-y-cuerpos-de-seguridad

Interagency Law Enforcement Academy of Advanced Studies. (2020). *Academic Year 2020/2021 - ADVANCED TRAINING COURSE*. Retrieved from https://scuolainterforze.interno.gov.it/wp-content/uploads/2020/11/A.Y.-2020-2021-XXXVI-advanced-training-course.pdf

Interagency Law Enforcement Academy of Advanced Studies. (2020). *PROGRAM OF THE 2nd LEVEL CRIME ANALYSIS COURSE*. Retrieved August 2021, from https://scuolainterforze.interno.gov.it/wp-content/uploads/2020/11/2nd-LEVEL-CRIME-ANALYSIS-COURSE.pdf

Internal Security Agency. (n.d.). Retrieved July 2021, from https://www.abw.gov.pl/en/about-isa/13,About-ISA.html

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

ITU. (n.d.). *Cyberwellness Profile Romania*. Retrieved September 2020, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Romania.pdf

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/

Milan Prosecutor's Office. (2013). *Reati informatici.* Retrieved July 2021, from https://www.procura.milano.giustizia.it/reati-informatici.html

Milan Prosecutor's Office. (2015). *Guidelines to fight cybercrimes and protect victims.* Retrieved July 2021, from https://www.procura.milano.giustizia.it/files/Guidelines-to-fight-cybercrimes-and-protect-victims.pdf

Milan Prosecutor's Office. (2018). *BILANCIO DI RESPONSABILITÀ SOCIALE 2018.* Retrieved July 2021, from https://www.procura.milano.giustizia.it/files/brs-procura-milano-2018.pdf

Milan Prosecutor's Office. (n.d.). *The High Tech Crime Unit*. Retrieved July 2021, from https://www.procura.milano.giustizia.it/the-high-tech-crime-unit.html

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 September 2020, from https://www.interieur.gouv.fr/Le-ministere/DGSI/Missions/La-mission-judiciaire-specialisee

Ministry of Home Affairs. (2021). *Ministry of Home Affairs approves Strategic Plan to Combat Cybercrime*. Retrieved August 2021, from https://www.lamoncloa.gob.es/lang/en/gobierno/news/Paginas/2021/20210309cybercrime.aspx

MSB. (n.d.). Retrieved September 2020, from https://www.msb.se/en/

NASK. (2019). *National Cybersecurity Strategy of Poland*. Retrieved from https://cyberpolicy.nask.pl/wp-content/uploads/2020/01/Strategia-cyberbezpieczeństwa-rp-na-lata-2019-2024.pdf

NASK. (n.d.). *CSIRT NASK*. Retrieved July 2021, from https://en.nask.pl/eng/activities/csirt-nask/3424,CSIRT-NASK.html

NASK. (n.d.a). *Report processing*. Retrieved from https://en.nask.pl/eng/activities/csirt-nask/report-processing/3413,Report-processing.html

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

National Prosecution Authority. (n.d.). *The National Prosecution Authority*. Retrieved from https://syyttajalaitos.fi/en/the-national-prosecution-authority

National Prosecution Authority. (n.d.a). *Prosecution Districts.* Retrieved from https://syyttajalaitos.fi/en/prosecution-districts

National Security Bureau. (2015). *Cybersecurity Doctrine of Poland*. Retrieved from https://en.bbn.gov.pl/en/news/400,Cybersecurity-Doctrine-of-the-Republic-of-Poland.html

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 June 2020, 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 June 2020, 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 September 2020, from https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

NCSC. (n.d.a). *CSIRT-IE*. Retrieved July 2021, from https://www.ncsc.gov.ie/CSIRT/

NCSC. (n.d.b). *National Cybersecurity Strategy of Ireland.* Retrieved June 2021, from https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf

NCSC-FI. (n.d.). *CERT.* Retrieved from https://www.kyberturvallisuuskeskus.fi/en/our-activities/cert

NFC. (n.d.). *Swedish National Forensic Centre (NFC).* Retrieved September 29, 2021, from https://nfc.polisen.se/en/#:~:text=The%20Swedish%20National%20Forensic%20Centre%2C%20NFC%2C%20is%20an,and%20analyzes%20on%20behalf%20of%20the%20judicial%20authorities.

NIM. (n.d.). Retrieved September 2020, from http://www.inm-lex.ro/

Norwegian Ministeries. (n.d.). *National Cybersecurity Strategy for Norway*. Retrieved September 2020, from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf

NPUC. (n.d.). Retrieved September 2020, from https://www.politihogskolen.no

NSM. (n.d.). Retrieved September 2020, from National Security Authority: https://nsm.no/about-nsm/about-the-norwegian-national-security-authority/

NÚKIB. (2020). *Concept for the development of the National office for Cyber and Information Security*. Retrieved June 2021, from

https://nukib.cz/download/publikace/strategie_akcni_plany/Koncepce_rozvoje_NUKIB.pdf

NÚKIB. (2020a). *National Cybersecurity Strategy*. Retrieved from https://www.nukib.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdf

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

Official Journal of the Italian Republic. (2018). *Legislative Decree 65/2018*. Retrieved July 2021, from https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg

Official Journal of the Italian Republic. (2021). *Legge 4 agosto 2021, n. 109.* Retrieved September 2021, from https://www.gazzettaufficiale.it/eli/id/2021/08/04/21G00122/sg

Official Journal of the Slovenian Republic. (2010). *Decree on the cooperation of the State Prosecutorial Service, the Police & other competent State bodies and insitutions in the detection and prosecution of perpetrators of criminal offences and the operation of specialised and joint investigation teams*. Retrieved August 2021, from https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/100420

Økokrim. (n.d.). Retrieved September 2020, from https://www.okokrim.no

OSCE. (n.d.). *Country Profile - Sweden.* Retrieved September 2020, from https://polis.osce.org/country-profiles/sweden

OSCE. (n.d.a). *Country Profile - Luxembourg.* Retrieved September 2020, from https://polis.osce.org/country-profiles/luxembourg

OSCE. (n.d.b.). *Country Profile Norway*. Retrieved September 2020, from https://polis.osce.org/country-profiles/norway

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

PISRS. (2018). *Act on Information Security*. Retrieved July 2021, from http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

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

Police University College of Finland. (n.d.). *Cyber competence 2020*. Retrieved from https://polamk.fi/en/cyber-competence-2020

Policia judiciaria. (2018). *Cyber Training*. Retrieved September 2020, from https://www.policiajudiciaria.pt/projetos-financiados/cyber-training-2/

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

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

Policia. (n.d.). *Comisaría General de Policía Judicial*. Retrieved May 2021, from https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial.php

Policija. (2007). *Criminal Procedure Act*. Retrieved June 2021, from https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf

Policja. (n.d.). *Cybercrime Bureau*. Retrieved August 2021, from https://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html

Polisen. (n.d.). Retrieved September 2020, from https://polisen.se/en/

Polisen. (n.d. a). Retrieved September 2020, from https://polisen.se/om-polisen/organisation/

Polish government. (2019). *Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)*. Retrieved August 2021, from https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt

Polish Parliament. (2018). *Act of 5 July 2018 on the National Cybersecurity System*. Retrieved from https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf

Polishögskolan. (n.d.). Retrieved September 2020, 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 September 2020, from https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/

Politiet. (n.d. a). Retrieved September 2020, from https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/national-cybercrime-centre/

Politiet. (n.d.b). Retrieved September 2020, from https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/national-cybercrime-centre/

Politiet. (n.d.c). Retrieved September 2020, from (https://www.politiet.no/en/om/organisasjonen/andre/national-police-directorate/om-pod/role-of-the-national-police-directorate/)

Politsei. (n.d.). *Cyber Politsei*. Retrieved from https://cyber.politsei.ee/

Polizia di Stato. (n.d.). *Polizia Postale e delle Comunicazioni Riferimenti normativi.* Retrieved July 2021, from https://www.poliziadistato.it/statics/27/polizia-postale-e-delle-comunicazioni---riferimenti-normativi.pdf

Polizia di Stato. (n.d.a). *Polizia di Stato*. Retrieved November 19, 2021, from https://www.poliziadistato.it/

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

Post and Communications Police. (n.d.). *Attività e organizzazione*. Retrieved July 2021, from https://www.commissariatodips.it/profilo/attivita-e-organizzazione/index.html

Post and Communications Police. (n.d.a). *CNAIPIC.* Retrieved July 2021, from https://www.commissariatodips.it/profilo/cnaipic/index.html

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

Présidence de la République française et du Palais del 'Élysée. (n.d.). Accélération de la stratégie nationale en matière de cybersécurité. Retrieved September 27, 2021, from https://www.pscp.tv/Elysee/1BdxYYPzznyxX?t=59s

Presidency of the Council of Ministers. (2017). *The Italian Cybersecurity Action Plan*. Retrieved July 2021, from https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf

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

Public Prosecutor's Office. (n.d.). Retrieved August 2021, from https://pk.gov.pl

RIA. (n.d.). Retrieved June 2021, from https://www.ria.ee/en.html

RIA. (n.d.a). *CERT-EE*. Retrieved June 2021, from https://www.ria.ee/en/cyber-security/cert-ee.html

Riigi Teateja. (2003). *Estonian Code of Criminal procedure*. Retrieved June 2021, from https://www.riigiteataja.ee/en/eli/530102013093/consolide

Riigi Teateja. (2018). Retrieved from https://www.riigiteataja.ee/en/eli/510072018002/consolide

Riigi Teateja. (2018a). *Cybersecurity Act*. Retrieved June 2021, from https://www.riigiteataja.ee/en/eli/523052018003/consolide

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

RTBF. (2021, Janvier 18). *Attaque informatique au CHwapi: les opérations non urgentes reportées, les consultations maintenues*. Retrieved November 2021, from https://www.rtbf.be/info/regions/hainaut/detail_le-chwapi-victime-d-une-attaque-informatique-en-pleine-pandemie?id=10676223

Senato della Repubblica. (2021). *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale (D.L. 82/2021 – A.C. 3161)*. Retrieved September 2021, from http://documenti.camera.it/leg18/dossier/pdf/D21082.pdf

SI-CERT. (n.d). Retrieved August 2021, from https://www.cert.si/en/about-si-cert/

SI-CERT. (n.d.a). *RFC2350*. Retrieved August 2021, from https://www.cert.si/o-nas/rfc2350/

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

Slovenian governement. (2021). *O Uradu vlade za informacijsko varnost*. Retrieved June 2021, from https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/o-uradu-vlade-za-informacijsko-varnost/

Slovenian government. (2016). *National Cybersecurity Strategy of Slovenia*. Retrieved June 2021, from https://www.gov.si/assets/ministrstva/MJU/DID/Strategija-kibernetske-varnosti.pdf

Slovenian government. (2021). *Informacijska varnost*. Retrieved June 2021, from https://www.gov.si/teme/informacijska-varnost/

Spanish Official Journal. (2018). *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información*. Retrieved May 2021, from https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257

Spanish Official Journal. (2018a). *Royal Decree 12/2018*. Retrieved from https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

Spanish Official Journal. (2021a). *Royal Decree 43/2021*. Retrieved from https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192

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

State Prosecuror's Office. (n.d.a). *Specialised State Prosecutor's Office*. Retrieved July 2021, from https://www.dt-rs.si/specialised-state-prosecutors-office

State Prosecutor's Office. (n.d.). *Supreme State Prosecutor's Office of the Republic of Slovenia*. Retrieved July 2021, from https://www.dt-rs.si/en

SUNet-CERT. (n.d.). Retrieved September 2020, from https://www.cert.sunet.se/english/index.html

Swedish Government. (n.d.). *A national cyber security strategy*. Retrieved November 29, 2021, from https://www.government.se/legal-documents/2017/11/skr.-201617213/

Swedish National Courts Administration. (n.d.). Retrieved September 2020, 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 November 2020, 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.). *The Police Academy of the Czech Republic in Prague*. Retrieved November 29, 2021, from https://www.polac.cz/g2/view.php?anglicky/index.html

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

Traficom. (n.d). Retrieved from https://www.kyberturvallisuuskeskus.fi/en/our-activities/cert

Traficom. (n.d.a). Retrieved from https://www.kyberturvallisuuskeskus.fi/en/our-activities/cert/rfc-2350

Trusted Introducer. (n.d.). *CERT Polska*. Retrieved July 2021, from https://www.trusted-introducer.org/directory/teams/cert-polska.html

UCD-CCI. (2020). *Digital First Responder Training*. Retrieved July 2021, from https://www.ucd.ie/cci/projects/digitalfirstresponderstraining/

UiO-CERT. (n.d.). Retrieved September 2020, 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 September 2020, 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

ZITiS. (n.d.). *Aufgaben & Ziele.* Retrieved June 2021, from https://www.zitis.bund.de/DE/ZITiS/Aufgaben/aufgaben_node.html;jsessionid=8FBF47E6366ACCF71510E0E44371359E.2_cid377

A ANNEX: BRIEF SUMMARY OF DESK RESEARCH CONDUCTED – COUNTRY SPECIFIC MATERIAL

A.1.1. Belgium

Belgium	
References	**Links**
Constitution and constitutional organs	
Constitution	https://www.senate.be/doc/const_fr.html
Council of State	http://www.raadvst-consetat.be/?lang=fr
The Constitutional Court	https://www.const-court.be/fr/
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/country-wiki/-/asset_publisher/AZnxfNT8Y3ZI/content/belgium?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3D101_INSTANCE_AZnxfNT8Y3ZI%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_pos%3D1%26p_p_col_count%3D2?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_AZnxfNT8Y3ZI&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
Law of 28 November 2000 on computer crime	https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2000112834
Law of 29 May 2016 on the retention of data in the electronic communications sector	http://www.ejustice.just.fgov.be/eli/loi/2016/05/29/2016009288/justel
Law of 25 December 2016 containing several modifications of the Criminal Code and the Criminal Procedure Code with the aim to improve the special investigation methods and several other methods concerning the Internet and electronic communications	http://www.ejustice.just.fgov.be/eli/loi/2016/12/25/2017030017/justel
The Code of Economic Law of 23 February 2013	https://economie.fgov.be/en/legislation/code-economic-law

National Cyber Security Strategy	
National cybersecurity strategy	https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/belgium
Country profile from the Organisation for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/belgium
Federal police	https://www.police.be/5998/fr
Federal Computer Crime Unit	https://www.politie.be/politiedorp/nl/federale-politie/federal-computer-crime-unit
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/16/EN/national_justice_systems?BELGIUM&member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/230
Fiche Belges on e-evidence from the EJN	https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/New%20Fiches%20Belges%20on%20electronic%20evidence%20-%20BELGIUM.pdf
Federal Public Prosecutor's Office	https://www.om-mp.be/fr/votre-mp/parquet-federal/press-release
CSIRTs	
CERT.be	https://cert.be/en
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Belgium
Overview of FIRST members around the world – Belgium	https://www.first.org/members/map#country%3ABE
Trusted Introducer (TI) European database of CSIRTs – see entries related to Belgium	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
Country profile from the European Judicial Training Network (EJTN) – Judicial Training Institute	https://www.ejtn.eu/About-us/Members/Belgium/
Institute for judicial training	https://www.igo-ifj.be/fr
Other documents	
Council of the European Union – report on Belgium	https://data.consilium.europa.eu/doc/document/ST-8212-2017-REV-1-DCL-1/en/pdf

A.1.2. 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	https://www.nukib.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.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.1.3. Estonia

Estonia	
References	**Links**
Constitution and constitutional organs	
Constitution	https://www.riigiteataja.ee/en/eli/530102013003/consolide
Supreme Court of Estonia	https://www.riigikohus.ee/en/supreme-court-estonia
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/-/estonia?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%20(Retrieved%20June%2029,%202021)
Penal Code	https://www.riigiteataja.ee/en/eli/522012015002/consolide
Code of Criminal Procedure	https://www.riigiteataja.ee/en/eli/530102013093/consolide
Electronic Communications Act (data retention)	https://www.riigiteataja.ee/en/eli/501042015003/consolide
Personal Data Protection Act	https://www.riigiteataja.ee/en/eli/523012019001/consolide
Cybersecurity Act	https://www.riigiteataja.ee/en/eli/523052018003/consolide
Emergency Act	https://www.riigiteataja.ee/en/eli/ee/513062017001/consolide
National Cyber Security Strategy	
National cybersecurity strategy	https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/estonia
Country profile from the Organisation for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/estonia
Estonian Police	https://www.politsei.ee/en
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/16/EN/national_justice_systems?ESTONIA&member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/269
Fiche Belges on e-evidence from the EJN	https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/EE%20electronic%20evidence%20fb.pdf
Prosecutor's Office	https://www.prokuratuur.ee

CSIRTs	
CERT-EE	https://www.ria.ee/en/cyber-security/cert-ee.html
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Estonia
Overview of FIRST members around the world – Estonia	https://www.first.org/members/map#country%3AEE
Trusted Introducer (TI) European database of CSIRTs – see entries related to Estonia	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
Country profile from the European Judicial Training Network (EJTN) – Supreme Court of Estonia, Training Department	https://www.ejtn.eu/About-us/Members/Estonia-Supreme-Court-of-Estonia/
Police and Border Guard College	https://www.sisekaitse.ee/en/police-and-border-guard-college?language_content_entity=en
Other documents	
Council of the European Union – report on Estonia	https://data.consilium.europa.eu/doc/document/ST-10953-2015-DCL-1/en/pdf

A.1.4. Finland

FINLAND	
References	**Links**
Constitution and constitutional organs	
Constitution	https://oikeusministerio.fi/en/constitution-of-finland
Supreme Court	https://korkeinoikeus.fi/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/-/finland?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
Coercive Measures Act	https://www.finlex.fi/fi/laki/kaannokset/2011/en20110806_20131146.pdf
Criminal Investigation Act	https://tbinternet.ohchr.org/Treaties/CAT/Shared%20Documents/FIN/INT_CAT_ADR_FIN_21164_E.pdf
Criminal Code	https://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf
National Cyber Security Strategy	
National Cyber Security Strategy	https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/finland
Country profile from the Organisation for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/finland
Cyber Crime Centre	https://poliisi.fi/mita-keskusrikospoliisi-tekee
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/16/EN/national_justice_systems?FINLAND&member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/272
Fiche Belges on e-evidence from the EJN	https://www.ejn-crimjust.europa.eu/ejnupload/Evidence/FB_Eevidence_FI.pdf
Prosecutor's Office	https://syyttajalaitos.fi/en/prosecutor-general
CSIRTs	
National Cyber Security Centre	https://www.kyberturvallisuuskeskus.fi/en/our-activities/cert

ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Finland
Overview of FIRST members around the world – Finlan	https://www.first.org/members/map#country%3AFI
Trusted Introducer (TI) European database of CSIRTs – see entries related to Finland	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
Country profile from the European Judicial Training Network (EJTN) – The National Courts Administration	https://www.ejtn.eu/About-us/Members/Finland1/
Police University College	https://polamk.fi/en/the-police-university-college-in-brief
Other documents	
Council of the European Union – report on Finland	

A.1.5. 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.1.6. 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.1.7. Ireland

IRELAND	
References	**Links**
Constitution and constitutional organs	
Constitution	http://www.irishstatutebook.ie/eli/cons/en/html
Supreme Court	http://www.supremecourt.ie
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/country-wiki/-/asset_publisher/AZnxfNT8Y3ZI/content/ireland?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3D101_INSTANCE_AZnxfNT8Y3ZI%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_pos%3D1%26p_p_col_count%3D2?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_AZnxfNT8Y3ZI&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
Criminal Justice Act, 2017	http://www.justice.ie/en/JELR/Pages/Criminal_Justice_Act_2017
Child Trafficking and Pornography Act, 1998	http://www.irishstatutebook.ie/eli/1998/act/22/enacted/en/html
Copyright and Related Rights Act, 2000	http://www.irishstatutebook.ie/eli/2000/act/28/enacted/en/html
Criminal Justice (Theft and Fraud Offences) Act, 2001	http://www.irishstatutebook.ie/eli/2001/act/50/enacted/en/html
Communications (Retention of Data) Act 2011	http://www.irishstatutebook.ie/eli/2011/act/3/enacted/en/html
Criminal Justice (Offences Relating to Information Systems) Act 2017	http://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/html
National Cyber Security Strategy	
National Cyber Security Strategy	https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/ireland
Country profile from the Organisation for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/ireland
An Garda Siochana	https://www.garda.ie/en/
Garda National Cyber Crime Bureau	https://www.garda.ie/en/about-us/organised-serious-crime/garda-national-cyber-crime-bureau-gnccb-/
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/16/EN/national_justice_systems?IRELAND&member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/314

Director of Public Prosecutions	https://www.dppireland.ie/about-us/
CSIRTs	
National Cyber Security Centre	https://www.ncsc.gov.ie
CSIRT.IE	https://www.ncsc.gov.ie/CSIRT/
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Ireland
Overview of FIRST members around the world – Ireland	https://www.first.org/members/map#country%3AIE
Trusted Introducer (TI) European database of CSIRTs – see entries related to Ireland	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
European Judicial Training Network (EJTN) – Committee for Judicial Studies Institute	https://www.ejtn.eu/About-us/Members/Ireland/
UCD Centre for Cybersecurity and Cybercrime Investigation	https://www.ucd.ie/cci/
Other documents	
Council of the European Union – report on Ireland	https://data.consilium.europa.eu/doc/document/ST-7160-2017-REV-1-DCL-1/en/pdf

A.1.8. Italy

ITALY	
References	**Links**
Constitution and constitutional organs	
Constitution	https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf
Counstitutional Court	https://www.cortecostituzionale.it/jsp/consulta/istituzioni/la_corte_costituzionale_italiana_EN.do
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/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/italy?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/
National Cyber Security Strategy	
National Cyber Security Strategy and Action Plan	https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/italy
Country profile from the Organisation for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/italy
Polizia Postale e delle Comunicazioni	https://www.commissariatodips.it/index.html
Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche	https://www.commissariatodips.it/profilo/cnaipic/index.html
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/16/EN/national_justice_systems?ITALY&member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/295
Public Prosecutor's Office (Procura della Repubblica)	https://www.procura.palermo.giustizia.it/compiti.aspx
CSIRTs	
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Italy
Overview of FIRST members around the world – Italy	https://www.first.org/members/map#country%3AIT
Trusted Introducer (TI) European database of CSIRTs – see entries related to Italy	https://www.trusted-introducer.org/directory/country_LICSA.html

Training	
European Judicial Training Network (EJTN) – Scuola Superiore della Magistratura	https://www.ejtn.eu/About/EJTN-Affiliates/Members/Italy/
Interagency Law Enforcement Academy of Advanced Studies	https://scuolainterforze.interno.gov.it

A.1.9. 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.1.10. 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.1.11. Poland

POLAND	
References	**Links**
Constitution and constitutional organs	
Constitution	https://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm
Constitutional Tribunal	https://trybunal.gov.pl
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/-/poland?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%20(Consulted%20July%201,%202021)
Penal Code	https://www.legislationline.org/download/id/7354/file/Poland_CC_1997_en.pdf
Code of Criminal Procedure	https://www.legislationline.org/download/id/4172/file/Polish%20CPC%201997_am%202003_en.pdf
Act on the Protection of Personal Data	https://uodo.gov.pl/en/594
National Cyber Security Strategy	
National Cyber Security Strategy	https://cyberpolicy.nask.pl/wp-content/uploads/2020/01/Strategia-cyberbezpieczeństwa-rp-na-lata-2019-2024.pdf
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/poland
Country profile from the Organization for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/poland
Cybercrime Bureau - National Police Headquarters	https://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html
Central Forensic Laboratory of the Police	https://clkp.policja.pl/cfl/examinations-and-proje/examinations-in-cflp/computer-examination/90842,Computer-examination.html
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/16/EN/national_justice_systems?POLAND&member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/351
Fiche Belges on e-evidence from the EJN	https://www.ejnforum.eu/cp/e-evidence-fiche/351/0
General Public Prosecutor's Office	https://pk.gov.pl
CSIRTs	

CSIRT NASK	https://en.nask.pl/eng/activities/csirt-nask/3424,CSIRT-NASK.html
CERT Poland	https://cert.pl/en/about-us/
CSIRT-GOV	https://csirt.gov.pl/cer
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Poland
Overview of FIRST members around the world – Poland	https://www.first.org/members/map#country%3APL
Trusted Introducer (TI) European database of CSIRTs – see entries related to Poland	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
European Judicial Training Network (EJTN) – National School of Judiciary and Public Prosecution	https://www.ejtn.eu/About-us/Members/Poland/
Police Training Centre	http://www.csp.edu.pl
Other documents	
Council of the European Union – report on Poland	https://data.consilium.europa.eu/doc/document/ST-14585-2016-REV-1-DCL-1/en/pdf

A.1.12. 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.1.13. 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.1.14. Slovenia

SLOVENIA	
References	**Links**
Constitution and constitutional organs	
Constitution	https://www.us-rs.si/media/constitution.pdf
Constitutional Court	https://www.us-rs.si/?lang=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/-/slovenia?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%20(Consulted%20on%20June%2025,%202021)
Personal Data Protection Act	https://rm.coe.int/16806af30c
Electronic Communications Act	https://www.legislationline.org/download/id/5561/file/Slovenia_Electronic%20Communications%20Act_2014_en.pdf
Electronic Commerce and Electronic Signature Act	http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1973
Information Security Act	http://www.pisrs.si/Pis.web/pregledPredpisa?sop=2018-01-1350
National Cyber Security Strategy	
National Cyber Security Strategy	https://www.gov.si/assets/ministrstva/MJU/DID/Strategija-kibernetske-varnosti.pdf
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
Slovenian Police	https://www.policija.si/eng/
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
State Prosecutor's Office	https://www.dt-rs.si/sl
CSIRTs	
SI-CERT	https://www.cert.si/en/about-si-cert/

SIGOV-CERT	https://www.gov.si/teme/informacijska-varnost/
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Slovenia
Overview of FIRST Members around the world – Slovenia	https://www.first.org/members/map#country%3ASI
National CSIRT profile from the Trusted Introducer (TI) European database of CSIRTs - Slovenia	https://www.trusted-introducer.org/directory/teams.html#url=c%3DSI%26q%3D
Training	
European Judicial Training Network (EJTN) – Ministry of Justice of the Republic of Slovenia, Judicial Training Centre	https://www.ejtn.eu/About/EJTN-Affiliates/Members/Slovenia/
Police Academy	https://www.policija.si/eng/744-about-the-police/organization/general-police-directorate/police-academy

A.1.15. Spain

SPAIN	
References	**Links**
Constitution and constitutional organs	
Constitution	https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf
Counstitutional Court	https://www.tribunalconstitucional.es/en/tribunal/historia/Paginas/Tribunal-Constitucional-de-Espania.aspx
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/-/spain?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
Law 34/2002, 11th July, on information society services and electronic commerce	https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
Organic Law 3/2018 , 5th December ,on the Protection of Personal Data and the Guarantee of Digital Rights	https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673
Law 25/2007, 18th October on the conservation of data relating to electronic communications and public communications networks.	https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243
Royal Decree 12/2018, 7th September on security of networks and information systems.	https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257
National Cyber Security Strategy	
National Cyber Security Strategy	https://www.ccn-cert.cni.es/en/pdf/documentos-publicos/3812-national-cybersecurity-strategy-2019/file.html
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/spain
Country profile from the Organisation for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/spain
Office for Cyber Coordination	https://www.csirt.es/index.php/es/miembros/cnpic
Technological Investigation Unit - National Police	https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial.php
Group of Telematic Crime - Central Operational Unit - Guardia Civil	https://www.gdt.guardiacivil.es/webgdt/la_unidad.php
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/16/EN/national_justice_systems?SPAIN&member=1

Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/373
General Prosecutor's Office	https://www.fiscal.es
CSIRTs	
CCN-CERT	https://www.ccn-cert.cni.es/en/
INCIBE-CERT	https://www.incibe-cert.es/en/
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map
Overview of FIRST members around the world – Spain	https://www.first.org/members/map#country%3AES
Trusted Introducer (TI) European database of CSIRTs – see entries related to Spain	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
European Judicial Training Network (EJTN) – Escuela Judicial Consejo General del Poder Judicial, Centro de Estudios Jurídicos	https://www.ejtn.eu/About/EJTN-Affiliates/Members/Spain/
INCIBE – Cybersecurity Summer BootCamp	https://www.incibe.es/en/summer-bootcamp
INCIBE - MOOC "Basic Cybersecurity for Security Forces and Bodies"	https://www.incibe.es/formacion/ciberseguridad-para-fuerzas-y-cuerpos-de-seguridad
INCIBE - MOOC "Advanced Cybersecurity for Security Forces and Bodies"	https://www.incibe.es/formacion/ciberseguridad-avanzada-para-fuerzas-y-cuerpos-de-seguridad
Other documents	
Council of the European Union – report on Spain	ttps://data.consilium.europa.eu/doc/document/ST-6289-2016-REV-1-DCL-1/en/pdf

A.1.16. 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/9th-enisa-ec3-workshop
Pilots of the ENISA 2020 training material on CSIRT-LE coooperation	For information contact: CSIRT-LE-cooperation@enisa.europa.eu
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/9th-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=f0f6e006dc9e858d6dbcb8c5f27fc1f2bfb1d23e006422431174 79&_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=uriserv:OJ.L_.2016.194.01.0001.01.ENG);
- 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. Belgium

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

- Law of 28 November 2000 on computer crime;
- Law of 15 May 2006 modifying the articles 259bis, 314bis, 504quater, 550bis and 550ter of the Criminal Code;
- Law of 29 May 2016 on the retention of data in the electronic communications sector;
- Law of 25 December 2016 containing several modifications of the Criminal Code and the Criminal Procedure Code with the aim to improve the special investigation methods and several other methods concerning the Internet and electronic communications;
- Law of 13 April 1995 containing provisions to combat trafficking in human beings and child pornography;
- The Code of Economic Law of 23 February 2013;
- Law of 7 May 1999 on gambling games;
- Law of 30 July 1981 on the punishment of racism and xenophobia;
- Law of 23 March 1995 on the punishment on the denying, minimizing, justifying or approving of the genocide committed by the German National Socialist regime during the Second World War;
- 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG).

C.3. Estonia

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

- Penal Code;
- Constitution of Estonia;
- Criminal Procedure Code;
- Electronic Communications Act (data retention);
- Personal Data Protection Act;
- Cybersecurity Act;
- Emergency Act;
- 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG).

C.4. Finland

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

- Coercive Measures Act (further information is available in the relevant section of the following website: https://finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf);
- Criminal Investigation Act (further information is available in the relevant section of the following website: https://finlex.fi/en/laki/kaannokset/2011/en20110805_20150736.pdf);
- Criminal Code (further information is available in the relevant section of the following website: https://finlex.fi/en/laki/kaannokset/1889/en18890039_20150766.pdf);
- 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG).

C.5. 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG);
- 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.6. 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG);
- 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.7. Ireland

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

- Criminal Justice Act, 1994, 1997, 2001;
- Child Trafficking and Pornography Act, 1998;
- Copyright and Related Rights Act, 2000;
- Criminal Justice (Theft and Fraud Offences) Act, 2001;
- Communications (Retention of Data) Act 2011;
- Criminal Justice (Offences Relating to Information Systems) Act 2017;
- Criminal Law (Sexual Offences) Act 2017;
- 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG).

C.8. Italy

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

- Law on copyright (Law of 22 April 1941, no. 633) that also lays down criminal sanctions in relation to alleged violations on the Internet (Article 171 et seq.);
- Criminal-law protection of credit cards under Article 55 of Legislative Decree of 21 November 2007 no. 231;
- Italian Personal Data Protection Code – Legislative Decree no.196 of 30 June 2003, also laying down provisions on data retention (Article 132) including provisions on the requests from foreign investigative authorities (Article 132, paragraph 4-ter);
- Electronic Communications Code (Legislative Decree 1 August 2003, no. 259) including the related obligations for Italian telecommunications companies pursuant to Article 96 (so-called mandatory assistance for purposes of justice);
- 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG).

C.9. 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG);
- 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.10. 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.11. Poland

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

- Penal Code from 06 June 1997, amended in 2003
- Code of Criminal Procedure from 06 June 1997, amended in 2003;
- Law on Data Protection from 1997, as amended in 2015;
- 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG).

C.12. 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG);
- 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.13. 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG);
- 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.14. Slovenia

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

- Personal Data Protection Act;
- Electronic Communications Act;
- Electronic Commerce Market Act;
- Electronic Commerce and Electronic Signature Act;
- Information Security Act (further information is available in the relevant section of the following website: https://nio.gov.si/nio/asset/zakon+o+informacijski+varnosti+zinfv?lang=en);
- 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG).

C.15. Spain

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

- Law 34/2002, 11th July, on information society services and electronic commerce, regulates which service providers are established in Spain;
- Organic Law 3/2018, 5th December, on the Protection of Personal Data and the Guarantee of Digital Rights;
- Royal Legislative Decree 1/1996, 5th April, 1996, approving the revised text of the Law on Intellectual Property, regularizing, clarifying and harmonizing the legal provisions in force on the subject. (Law 2/2019, 1th March, which amends the revised text of the Intellectual Property Law, approved by Royal Legislative;
- Decree 1/1996, 12th of April and which incorporates into Spanish law Directive 2014/26/EU of the European Parliament and Council, of February 26, 2014, and Directive (EU) 2017/1564 of the European Parliament and Council, of September 13, 2017);
- Law 25/2007, 18th October on the conservation of data relating to electronic communications and public communications networks;
- Law 9/2014, 9th May, General of Telecommunications;
- Royal Decree 1889/2011, 30th December, regulating the functioning of the Intellectual Property Commission;
- Law 8/2011, 28th April establishing measures for the protection of critical infrastructures;
- Royal Decree 12/2018, 7th September on security of networks and information systems;
- 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG).

C.16. 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=uriserv:OJ.L_.2016.194.01.0001.01.ENG);
- 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 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)
BBN	National Security Bureau
BCIT	Central Brigade for Technological Research (Brigada Central de Investigación Tecnológica)
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")
CC server	Command and control server
CCB	Center for Cyber Security Belgium (Centre pour la Cybersécurité Belgique)
CCIS	Norwegian Center for Cyber and Information Security
CCN-CERT	National Cryptology Center - CSIRT of the National Cryptology Center (Centro Criptologico Nacional - Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional)
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.be	Computer Emergency Response Team for Belgium

CERT-EE	Computer Emergency Response Team for Estonia (CERT Eestis)
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-PA	Computer Emergency Response Team - Public Administration
CERT Poland	Computer Emergency Response Team Poland
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
CSAM	Child Sexual Abuse Material
CIRCL	Computer Incident Response Center Luxembourg
CITCO	Intelligence Center for Counter-Terrorism and Organised Crime
CLKP	Central Forensic Laboratory of the Police (Centralne Laboratorium Kryminalistycznego Policji)
CNAIPIC	National Anti-crime Computer Centre for the Protection of Critical Infrastructure
CNPIC	National Critical Infrastructure Protection and Cybersecurity Centre
CNCS	National Cybersecurity Centre (Centro Nacional de Cibersegurança)
CNI	National Intelligence Centre
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-IE	Computer security incident response team of Ireland
CSIRT-GOV	Governmental Computer Security Incident Response Team
CSIRT Italia	Computer Emergency Response Team Italy
CIRT NASK	Computer Security Incident Response Team run by Naukowa i Akademicka Sieć Komputerowa
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)
DJSOC	Directorate for the fight against serious and organised crime
DPP	Director of Public Prosecutions
DSP	Digital Service Providers
EC3	European Cybercrime Centre
ECTEG	European Cybercrime Training and Education Group
EDITE	Equipos de Investigación Tecnológica
EEA	European Economic Area
E-First	First responders e-learning package
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
EUIBAs	EU Institutions, Bodies and Agencies
Eurojust	European Union Agency for Criminal Justice Cooperation
ESDC	European Security and Defence College
EU CyCLONe	EU Cyber Crisis Liaison Organisation Network
Europol	European Union Agency for Law Enforcement Cooperation
FCCU	Federal Computer Crime Unit
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
GDT	Group of Telematic Crime - Central Operational Unit (Grupo de Delitos Telemáticos - Unidad Central Operativa)
GIRP – FID	General Inspectorate of Romanian Police – Fraud Investigations Directorate (Inspectoratul General al Poliţiei Române)
GNCCB	Garda National Cyber Crime Bureau
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
IAEA	International Atomic Energy Agency
ICT	Information and communication technology
IDS	Intrusion Detection Sensors
IGPR	General Inspectorate of Romanian Police (Inspectoratul General al Poliţiei Române)
ILSTA	Institute for Legal Support and Technical Assistance
INCIBE	National Cybersecurity Insitute (Instituto Nacional de Ciberseguridad)
INCIBE-CERT	National Cybersecurity Insitute-CERT (Instituto Nacional de Ciberseguridad-CERT)
IoC	Indicators of compromise
ISP	Internet Service Provider
IT	Information technology
J-CAT	Joint Cybercrime Action Taskforce
JSON	JavaScript Object Notation
KYPO	Kybernetický polygon
LCCU	Local Computer Crime Units
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)
MWDB	Malware data base
NASK	Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy
NBI	National Bureau of Investigation
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)
NCSC	National Cyber Security Centre
NCSC	Norwegian National Cyber Security Centre (Nasjonalt cybersikkerhetssenter)
NCSC-FI	National Cyber Security Centre of Finland
NCSP	National Cybersecurity Services Platform
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)
OAS	Organization of American States
OCC	Office for Cyber Coordination (Oficina de Coordinación Cibernética)
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
OES	Operators of essential services
OSCE	Organisation for Security and Cooperation in Europe
OSINT	Open source intelligence
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
RCCU	Regional Computer Crime Units
RIA	Information System Authority (Riigi Infosüseemi Amet)
RDI	Research, development and innovation
RSCI	Responsible, Supporting, Consulted and Informed
RFC	Request for Comments
R&D	Research and Development
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)
SI-CERT	Slovenian Computer Emergency Response Team
SIGOV-CERT	Slovenian Governmental Computer Emergency Response Team
SIS	Internal Intelligence Service (Serviço de Informações de Segurança)
SNAV	National Security Council
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
UCD	University College Dublin
UCD-CCI	Irish UCD Centre for Cybersecurity and Cybercrime Investigation
UACI	Unità d'analisi del crimine informatico
UIT	Technological Investigation Unit (Unidad de Investigación Tecnológica)
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
URSIV	Information Security Administration (Uprava Republike Slovenije za informacijsko varnost)
ZIT	Public Prosecutor's Offices of the Länder and Courts of the Länder (Die Staatsanwaltschaften der Länder und Landgerichte)

TP-09-21-478-EN-N

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
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-541-8
DOI: 10.2824/594421