

Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary

NOVEMBER 2018



About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and the public. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu

Contributors

Philip Anderson, François Beauvois, Efthymios Lalas, Catalin Patrascu, Andreas Sfakianakis, Silvia Signorato, Václav Stupka, Koen Van Impe

Editors

Silvia Portesi (ENISA), Alexandra Michota (ENISA)

Contact

For queries in relation to this paper, please use CSIRT-LE-cooperation@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

Acknowledgements

ENISA would like to thank all of the following people and organisations.

The subject-matter experts, selected from the list of network and information security (NIS) experts compiled following the ENISA call for expression of interest (CEI) (Ref. ENISA M-CEI-17-C01), who on an individual basis provided valuable input to the report.

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:

- CERT.be, Belgium
- Rogério Bravo, Criminal Police, Portugal
- Rogério Gil Raposo, National Cybersecurity Centre, CERT.PT, Portugal
- Raffaele Incardona, Public Prosecutor, District Prosecutor's Office, Venice, Italy.
- Aljoša Špeh, Head of Computer Crime Investigation Unit, Police Directorate Koper, Police Slovenia.
- Petr Klement, Supreme Public Prosecutor's Office, Czech Republic
- Andreas Iacovou, National CSIRT.CY, Cyprus
- François-Xavier Masson, French Police
- Court of Appeals-Hertogenbosch, the Netherlands
- Matthew Yeomans, CSIRT, Malta

- Michael Dwucet, Marc Brauer, Bundesamt für Sicherheit in der Informationstechnik/Federal Office for Information Security (BSI) — CERT-Bund, Germany
- IT-Dienstleistungszentrum, Berlin-CERT, Germany
- Oliver Klau (kriminaloberrat), Landeskriminalamt, Der Polizeipräsident in Berlin/ Police of Berlin , Germany
- Jörg Rauppach, Der Leitende Oberstaatsanwalt in Berlin/ Prosecutors office in Berlin, Germany
- Georgios Papaprodomou, Efthymios Lyssaris, Maria Grouztidou, Cybercrime Division, Hellenic police, Greece
- IT-CERT, Italy

All CSIRTs, law enforcement and judiciary respondents to the online survey conducted to collect data for this report as well as the European Union Agency for Law Enforcement Cooperation (Europol) European Cybercrime Centre (EC3) colleagues for their support in distributing the survey via their networks.

All the subject-matter experts/organisations who performed peer-reviews of the report, including Europol EC3.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2018
Reproduction is authorised provided the source is acknowledged.

ISBN: 978-92-9204-259-2, DOI: 10.2824/274312

Table of Contents

Executive summary	8
1. Introduction	10
1.1 Purpose	10
1.2 Background of the report	10
1.3 Report objectives and scope	11
1.3.1 Report objectives	11
1.3.2 Report scope	12
1.4 Target audience	12
2. Methodology	13
2.1 Information collection instruments used	13
2.1.1 Desk research	13
2.1.2 Interviews and written replies to the questionnaire	13
2.1.3 Online survey	15
2.2 Data used to develop the recommendations	16
2.3 Selection and classification of the stakeholders	16
2.4 Contribution by subject-matter experts	17
3. CSIRTs, LE and the judiciary: framework, information flow and tools	18
3.1 Some general remarks	18
3.1.1 Criminal procedures: non-adversarial versus adversarial	18
3.1.2 Criminal proceedings	18
3.1.3 Admissibility of electronic evidence in criminal courts	20
3.2 Applicable legal and policy framework	20
3.2.1 An Overview of the relevant legal and policy framework	20
3.2.2 Some recent developments	22
3.3 CSIRTs, LE and the judiciary: roles, structures and strengths	25

3.3.1	The role of CSIRTs, LE and the judiciary	25
3.3.2	The structure of CSIRTs, LE and the judiciary	28
3.3.3	Strengths of the three communities	32
3.4	The interaction and the information flow across CSIRTs, LE and the judiciary	33
3.4.1	Indirect v. direct interaction between CSIRTs and prosecutor and judge	34
3.4.2	CSIRTs and their duty (or not) to inform law enforcement or prosecutor and/or to report a crime and the coordination of actions	36
3.4.3	The kind of information exchanged and the related information flow	38
3.4.4	Frequency of the information exchange and of the usage of information provided by CSIRTs in criminal investigations and as evidence in criminal proceedings	40
3.4.5	A graphical representation of the information flow	42
3.5	The tools and the common taxonomy for CSIRTs and law enforcement	44
3.5.1	Tools	44
3.5.2	Common taxonomy for CSIRTs and law enforcement	46
4.	Challenges in cooperation and interaction	47
4.1	The challenges faced	47
4.2	Legal challenges	47
4.2.1	Data retention	47
4.2.2	Secrecy of criminal investigations and the ‘need to know’	48
4.2.3	Sharing of personal data, including IP addresses	49
4.2.4	Fundamental rights	50
4.2.5	Chain of custody and evidence admissibility	51
4.2.6	Diversity of legal frameworks between Member States and the timing of the investigative cooperation between Member States	51
4.3	Cultural challenges	52
4.4	Technical challenges	52
4.4.1	Validation of the digital forensic tools	52
4.4.2	Different technical maturity levels across different communities	53

4.4.3	Lack of common tools, tools for automated or semi-automated transfer of the data, and coordination tools	53
4.4.4	Taxonomy-related challenges	53
4.5	Organisational challenges	54
4.5.1	Need for reciprocal understanding of the structures, roles and strengths	54
4.5.2	Digital forensics expertise and the digital forensics training	55
5.	Conclusions and recommendations	60
5.1	Conclusions	60
5.1.1	CSIRTs interact much more with LE than with the prosecutors and they interact very rarely with the judiciary	60
5.1.2	CSIRTs support law enforcement (as well as prosecutor and judge) in a criminal investigation	60
5.1.3	There are legal provisions on CSIRTs and LE cooperation and their interaction with the judiciary	60
5.1.4	The understanding of whether CSIRTs have to report to/inform LE and/or prosecutor of suspicious criminal activities could be improved	60
5.1.5	There is need for a more extensive usage of information from CSIRTs in criminal investigations and as evidence in court	61
5.1.6	There is need to collect data in order to support cooperation in a data driven approach	61
5.1.7	Cultural limitations can be noted in the cooperation across the three communities and an interdisciplinary approach might help	61
5.2	Recommendations	61
5.2.1	Collect data on cooperation and interaction across CSIRT, LE and the judiciary	62
5.2.2	Build on shared experience at strategic cooperation level	62
5.2.3	Invest in CSIRT/LE/judiciary joint training and skills development	63
5.2.4	To reach a better mutual understanding of the other communities and develop memoranda of understanding to facilitate cooperation/interaction	63
5.2.5	Place liaison officers	64
5.2.6	Use (common) tools to facilitate cooperation and interaction	64
6.	Bibliography/references	66

Annex A: Abbreviations	76
Annex B: Definitions of the key concepts	78
Annex C: An overview of legal systems, areas of law, and legal traditions (common law and civil law)	82
Annex D: The WHOIS registry	84
Annex E: Questionnaire to support the subject matter expert Interviews	88
Annex F: Questions in the online survey	94
Annex G: Examples of topics for CSIRT/LE/judiciary joint training	104
Annex H: Example of segregation of duties (SoD) matrix	105

Executive summary

The purpose of this report is to further explore the cooperation between computer security incident response teams (CSIRTs) (in particular national and governmental CSIRTs) and law enforcement (LE) by adding the important dimension of their interaction with the judiciary (prosecutors and judges).

This report follows two reports that ENISA published in 2017: *Tools and methodologies to support cooperation between CSIRTs and law enforcement* (ENISA, 2017), which focused on technical aspects and *Improving cooperation between CSIRTs and law enforcement: Legal and organisational aspects* (ENISA, 2017a), which focused on the legal and organisational issues of cooperation; both are available on the ENISA website.

This report aims to support the cooperation between CSIRTs and LE, as well as their interaction with the judiciary in their fight against cybercrime, by providing information on the legal, organisational, technical and cultural aspects, identifying current shortcomings and making recommendations to further enhance cooperation. The geographical coverage is mainly the EU and European Free Trade Association (EFTA).

The data for this report was collected via desk research, interviews with subject-matter experts and an online survey. The data showed that CSIRTs, LE and the judiciary are characterised by significant differences in roles and structure. The kind of information to which CSIRTs and LE have access is different, this is one of the primary reasons why sharing information between them is paramount to respond to cybercrime. Across Member States different models/frameworks of interaction exist among the three communities (CSIRTs, LE and the judiciary). Overall CSIRTs interact more with LE rather than with the judiciary. CSIRTs offer support to LE to collect and analyse different types of evidence. CSIRTs are rarely called as witnesses in courts but the material they collect during the incident handling might be used to decide on (cyber) crime cases.

Although the cooperation and interaction across the CSIRT, LE and judiciary communities work well in principle, there are still some challenges to be faced. In particular, some legal aspects are seen as the biggest challenge with issues such the diversity of the legal frameworks, data retention, the sharing of personal data (including internet protocol (IP) addresses) and the confidentiality around criminal investigations as well as evidential admissibility of digital evidence.

Core recommendations to improve the aspects of the cooperation between CSIRTs and LE and their interaction with the judiciary are as follows.

- **ENISA, Europol EC3, the European agency for the enhancement of judicial cooperation (Eurojust) and the European Union Agency for Law Enforcement Training (CEPOL):** to facilitate joint training across the three communities (CSIRTs, LE and the judiciary) on aspects of their cooperation among the EU and EFTA addressing CSIRTs, LE and judiciary needs and engaging with designated CSIRTs in the MS and national police forces beyond the EU, as appropriate.
- **National/governmental CSIRTs, LE and possibly prosecutor services:** to work together towards a better mutual understanding of the strengths, needs and limitations of the three communities in relation to the sharing information, also by using segregation (or separation) of duties (SoD) matrices.
- **National/governmental CSIRTs, LE and possibly prosecutor services:** to appoint liaison officers to facilitate the cooperation and the interaction.

- **National/governmental CSIRTs, LE and possibly prosecutor services:** to investigate how the tools they use can be further improved to better receive the information provided by other communities and to better formulate their request for information addressed to the other communities.

1. Introduction

1.1 Purpose

As stated in the Council of the European Union Final report on the seventh round of mutual evaluations on 'The practical implementation and operation of the European policies on prevention and combating cybercrime' (Council of the European Union, 2017, p. 67), 'CSIRTs do not have the powers of an LEA (law-enforcement agency) vis-à-vis private subjects, but regarding attacks of a criminal nature (not all cyber incidents are criminal acts), have an important role in supporting the investigations, as they can help to provide information and to secure electronic evidence (e-evidence). It is therefore very important for this purpose that CSIRTs have a good cooperation with the LE, as obtaining information and evidence effectively is essential for the investigation of cyber-attacks, considering that data are very dynamic and can be lost easily'.

Collecting knowledge on current cooperation between CSIRTs and LE communities is a key step to enhance it. While the 2017 ENISA reports on CSIRT and LE cooperation (ENISA, 2017) (ENISA, 2017a) aimed to better understand in particular the legal/organisational and technical aspects of the cooperation, the purpose of this report is to further explore this cooperation by adding the important dimension of their interaction with the judiciary (prosecutors and judges).

1.2 Background of the report

In 2017, ENISA published two complementary reports addressing the cooperation between CSIRT and LE to fight against cybercrime, one on legal and organisational aspects, the other on technical aspects.

The 2017 ENISA report on *Improving cooperation between CSIRTs and law enforcement: Legal and organisational aspects* (ENISA, 2017a) confirmed that CSIRTs and LE often exchange information during the incident handling/investigations both formally and informally and that trust is the key success factor for the cooperation. It showed that there are challenges related to the variety of legal systems and legal provisions in the different Member States; adding further complexity is the diversity of communication channels between the various Member States that represents an issue for effective crime fighting.

The 2017 ENISA report *Tools and methodologies to support cooperation between CSIRTs and law enforcement* (ENISA, 2017) also confirmed that CSIRTs and LE exchange information often during incident handling/investigations both formally and informally and that trust is also the key success factor for the cooperation. It highlighted that despite CSIRTs and LE having different objectives and methods for collecting and processing information, there is, between the two communities, an increased reciprocal understanding of needs. Furthermore, according to the data collected for that report, CSIRTs are more inclined to use open-source tools (e.g. the malware information-sharing platform (MISP)) and the information sharing between CSIRTs and LE is more ad hoc than systematic.

As highlighted in the 6th ENISA/EC3 workshop for national and governmental CSIRTs and their LE counterparts (The Hague, 16-17 October 2017) (ENISA, 6th ENISA/EC3 Workshop, n.a.), the theme of interaction across CSIRTs, LE and judiciary (prosecutors and judges) is extremely important. In the context of the fight against (cyber) crime, indeed, it is not sufficient that evidence is collected, but it is also necessary that it is admissible in a criminal trial. Compliance with technical and legal requirements is

needed for the admissibility of evidence, notably adherence to the criminal procedure requirements is of paramount importance.

The *ENISA programming document 2018-2020* includes 'Objective 4.2. CSIRT and other NIS community building'. Under this objective, 'Output O.4.2.2 — Support the fight against cybercrime and collaboration between CSIRTs and LEA' has the goal to 'to build upon the progress ENISA has made in supporting different operational communities (e.g. CSIRTs, LE, European [Financial Institutes – Information Sharing and Analysis Centre] FI-ISAC) to enhance mutually satisfactory ways to collaborate and support exchange of good practices among different stakeholders in operational communities in Europe' (ENISA, 2017b, p. 43).

This report is a continuation of previous ENISA work and it contributes to the implementation of the *ENISA programming document 2018-2020*, Output O.4.2.2, in particular to what is planned for as 'Current cooperation between CSIRT and LEA community and on possible ways to further enhance their cooperation'.

1.3 Report objectives and scope

1.3.1 Report objectives

The 2017 ENISA reports on CSIRT and LE cooperation as well as previous ENISA work in the area focused only on these two communities: CSIRT and LE. The objectives of these past ENISA reports were to analyse how these two communities cooperate and share information both from the legal/organisational and the technical point of view. They identify challenges to the cooperation (such as limitations in the availability of specialised personnel) and propose ways to overcome them (such as to place liaison officers at both ends, to build and maintain a centralised repository of tools and methodologies and to invest further in joint training).

They gather further knowledge on the cooperation between CSIRTs and LE by also looking at the dimension of how their interaction with the judiciary helps to reach a better and more complete understanding of the dynamics, synergies and challenges that characterise their cooperation in the fight against cybercrime.

The main objectives of this report are as follows.

- Gather further knowledge and discuss the current ⁽¹⁾ cooperation between CSIRTs and LE by adding the dimension of their interaction with prosecutors and judges as far as it concerns their fight against cybercrime.
- Provide information on the relevant legal and policy framework shaping this cooperation and this interaction.
- Provide information on the information flow across the three communities (CSIRTs and LE and the judiciary).
- Provide information on the tools and methods used for the cooperation between CSIRTs and LE and their interaction with the judiciary.

⁽¹⁾ Data collection cut-off date for this report: 28 August 2018.

- Identify current challenges to the cooperation between CSIRTs and LE and their interaction with the judiciary.
- Formulate and propose recommendations to improve the cooperation between CSIRTs and LE and their interaction with the judiciary.

1.3.2 Report scope

The report focuses on aspects of cooperation between CSIRTs (national/governmental CSIRTs) and LE, and their cooperation with the judiciary (prosecutors and judges).

The geographical coverage is limited to the EU (European Union, 2017) and EFTA (EFTA, n.d.)⁽²⁾. (See also (ENISA, 2015b)). This does not mean however that all these countries are covered in the report and that no reference to other countries outside the EU and EFTA is made in the report. Possible specific differences among the EU and EFTA, or between the EU and the United States, or the EU and Asia, also fall outside the scope of this report.

The report does not target a specific sector; considerations made can apply to cooperation between CSIRTs and LEs and the interaction with the judiciary to fight against cybercrime (which includes crimes where a computer is an object and crimes where a computer is a tool of crime) in all sectors (from finance to energy, from transport to health).

Although some considerations might be made incidentally in this report on the general cooperation between LE and judiciary, this is not the focus of the report, which looks at such aspect only as far as they are relevant for reaching a better understanding of the cooperation and interaction between the CSIRTs, LE and judiciary community to respond to cybercrime.

The fight against terrorism, cyberwarfare, cyber espionage by nation states, as well as the enforcement of rights in civil and administrative courts, are outside the scope of this report, although some of the considerations developed might be extended to them.

This report does not aim to present an exhaustive set of instantiations of cooperation between CSIRTs and LEs and of their interaction with the judiciary, rather it seeks to facilitate the drawing of meaningful conclusions for the purpose of enhancing such cooperation and interaction.

1.4 Target audience

The intended target audience are CSIRTs (mainly national and governmental CSIRTs but not limited to them) LE, prosecutors, judges, as well as individuals and organisations with an interest in NIS.

Additionally, policy and law makers may benefit from select aspects of analysis as well as the recommendations of this report, as they prepare policies and legislation for enhancing the cooperation between CSIRTs and LEs and their interaction with the judiciary.

⁽²⁾ In this report 'n.d.' stands for 'no date' and it is used in the references when no date could be found for the cited source.

2. Methodology

The methodology chosen for this report and the way this methodology is presented in this chapter are largely inspired by Chapter 2 of the 2017 ENISA reports on *Improving cooperation between CSIRTs and law enforcement: Legal and organisational aspects* (ENISA, 2017a) and on *Tools and methodologies to support cooperation between CSIRTs and law enforcement* (ENISA, 2017).

In keeping with these two 2017 ENISA reports, data for this report was collected by desk research, interviews with subject-matter experts and an online survey. A qualitative methodological approach has mainly been used due to the rather new field addressed; however, some quantitative data were also collected: an online survey was conducted to validate and complement the findings from the desk research and the interviews.

2.1 Information collection instruments used

2.1.1 Desk research

A first desk research was conducted based on publicly available information sources, including ENISA publications. The findings from this desk research were particularly useful for the scoping of the report and for drafting the questionnaire to support the interviews.

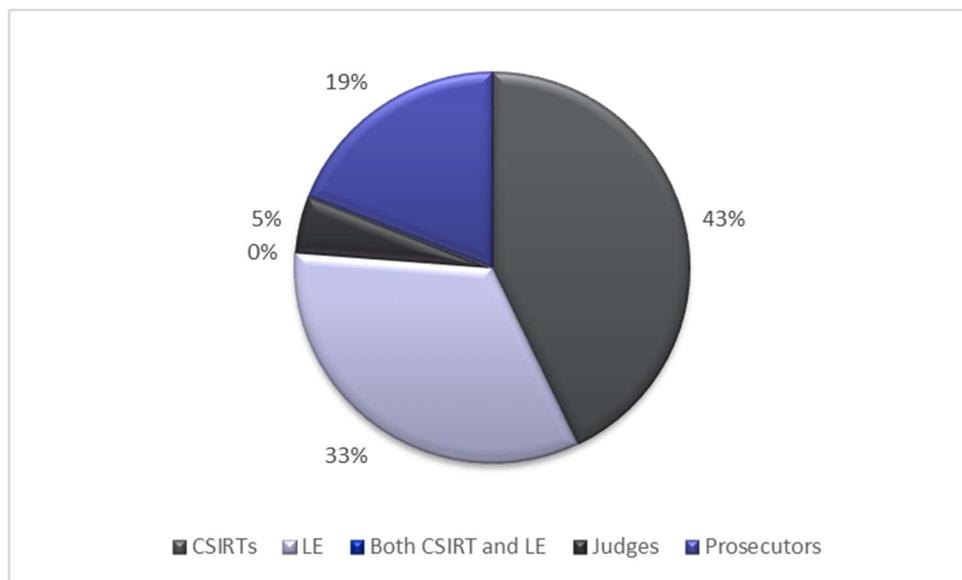
Supplementary desk research was conducted to address certain specific topics that the project team deemed appropriate to examine in more depth following the analysis of the data collected via the interviews. These included topics such as the recent discussion on access to the WHOIS database (DB) by LE.

Concerning the legal research, legal material (including some case-law) for instance fundamental principles of criminal procedure, comparative criminal law and procedure, and European law, was consulted.

2.1.2 Interviews and written replies to the questionnaire

A total of 21 subject-matter experts from 11 Member States replied to the questionnaire either via structured interviews or with written replies. Of the respondents, nine were experts from the CSIRTs community (mainly but not exclusively from national/governmental CSIRTs), seven from the LE community (mainly national police but also one from a local police force), and five from the judiciary community. This is in addition to the respondents of the online survey.

Figure 1 — Overview of communities of respondents to the interviews conducted for this report



A questionnaire (see Annex E — Samples of questionnaires to support the interviews) was prepared to support the interviews. Most questions were open. For all questions, including yes/no questions, interviewees could add comments and additional information.

The interviews included some questions common to CSIRTs, LE and the judiciary, followed by a specific set of questions for each community.

A pilot phone interview was conducted in June 2018. In addition, the questions were tested with an additional respondent to verify its suitability to be answered in writing. In addition to data for the report, the two pilot interviews served as a means to collect feedback on how the interview was received and avoided, for instance, unclear or inappropriate questions that might have decreased the willingness of the respondents to provide answers. The pilot interviews were also useful to verify the time to allocate to the interview.

The interviews were carried out from June to mid-July 2018. They were conducted either face-to-face or via phone and they lasted around 1 hour each. Interviewees received the questions in advance and in most cases, they had the opportunity to review the notes taken by the interviewers (project team) with their replies and validate them.

Of the 21 respondents, five asked to reply to the questions in writing as this was more convenient for them.

Some interviewees, or representatives of the same organisation of interviewees, also completed the online survey.

While the questionnaire developed to collect data for the 2017 ENISA reports focused only on CSIRT and LE cooperation, the questionnaire developed to collect data for this 2018 report addresses also their interaction with the judiciary and aims to collect more in-depth information on some topics, such as joint training.

The interview questions started with a set of common questions for all participants to answer, followed by three sets of specific questions for CSIRTs, LE or judiciary to answer respectively. In comparison to the interviews conducted for the 2017 ENISA reports on CSIRTs and LE cooperation, the interviews for this report covered inter alia the additional dimension of the interaction with the judiciary.

2.1.3 Online survey

An online survey was conducted to collect additional data to validate and further substantiate some findings. It was composed of 16 questions (see Annex F — Questions in the online survey), all with closed answers and some with the possibility to add additional comments and provide more details related to the answers.

The survey was developed using EUSurvey⁽³⁾, a survey tool which is 'supported by the European Commission's ISA programme, which promotes interoperability solutions for European public administrations' (European Commission, n.d.(b)).

The invitation to complete the survey was disseminated as follows.

- A closed ENISA mailing list of European national and governmental CSIRTs, which includes around 60 teams.
- Via Europol (Europol, n.d.) to the European Union cybercrime task force (EUCTF), which is 'composed of the heads of the designated national cybercrime units throughout the EU Member States and Europol. The EUCTF⁽⁴⁾ is an interagency group formed to allow the heads of cybercrime units, Europol, [the International Criminal Police Commission] Interpol, the European Commission, Eurojust, Norway, Switzerland and Iceland to discuss the strategic and operational issues related to cybercrime investigations and prosecutions within the EU and beyond' (Council of the European Union, 2017b, p. 13).
- Via Eurojust (Eurojust, n.d.) to the judicial authorities of the European judicial cybercrime network, which is composed by 'at least one national representative of the judicial authorities with appropriate expertise to participate in the network' and was set up to 'provide a centre of specialised expertise supporting judicial authorities, i.e. prosecutors and judges dealing with cybercrime, cyber-enabled crime and investigations in cyberspace'⁽⁵⁾ (Council of the European Union, 2016, p. 2).

The survey was launched in July 2018 and was open for around 2 weeks. The data collected via the online survey was used to validate the data collected through the desk research and the interviews and used to produce some statistical graphs.

⁽³⁾ <https://ec.europa.eu/eusurvey/home/welcome>

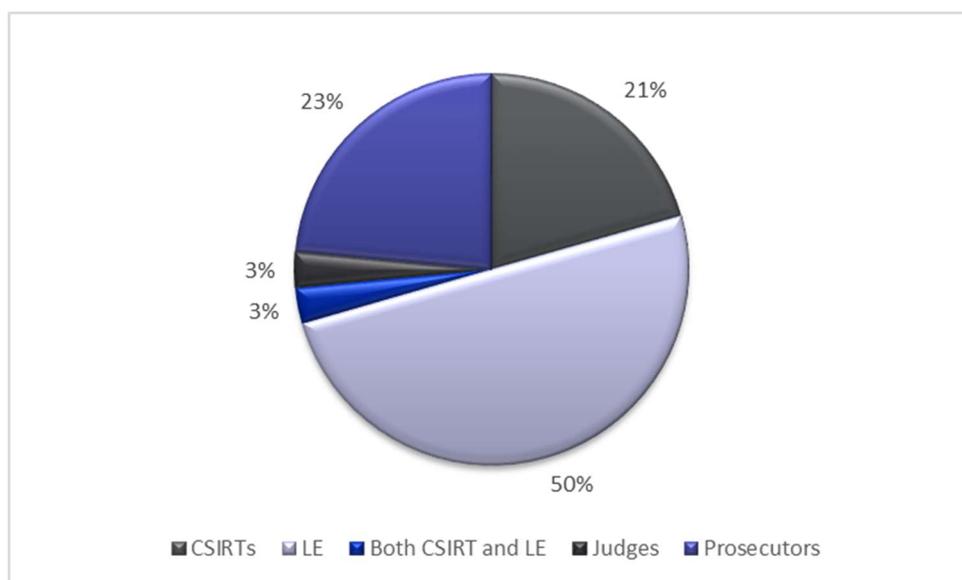
⁽⁴⁾ In execution of the JHA Council conclusions of 27-28 November 2008 and of the 26 April 2010, Europol together with the European Commission and the EU Member States have set up the European Union cybercrime task force (EUCTF) composed of the Heads of the designated national cybercrime units throughout the EU Member States and Europol. The EUCTF is an interagency group formed to allow the Heads of Cybercrime Units, Europol, the European Commission and Eurojust to discuss the strategic and operational issues related to cybercrime investigations and prosecutions within the EU and beyond.

⁽⁵⁾ Terms of Reference of EUCTF.

A total of 36 replies were received. Of these, 34 were from EU Member States (European Union, 2017) and EFTA countries (EFTA, n.d.), one from a non-EU/non-EFTA country and one from another organisation. It must be noted that the two replies from non-EU/EFTA countries were somewhat in line with the other replies received and have been used to formulate general considerations; however, the graphs in this report were developed based only on the 34 replies from EU and EFTA respondents, to ensure full consistency with the geographical scope of the report.

Of the 34 EU and EFTA respondents, seven respondents were from the CSIRT community, 17 from the LE community, one belonged to both of these communities, and nine were from the judiciary (eight prosecutors and one judge). An overview of the composition of the EU and EFTA respondents, based on the community they belong to, is presented hereinafter in Figure 2.

Figure 2 — Overview of communities of respondents to the online survey conducted for this report



Most respondents replied to all questions, despite most questions not being mandatory. Some respondents used the comment boxes to provide extra information.

2.2 Data used to develop the recommendations

The recommendations in this report (see Chapter 5) have been developed based on research findings of this report.

2.3 Selection and classification of the stakeholders

The project team discussed and agreed on criteria to use to ensure contribution of a wide range of stakeholders. The following criteria (which were not prioritised but considered as equal) were used for the selections of interviewees:

- CSIRTs/LE/judiciary community
- geographical location

- size of country (population)
- level of maturity in CSIRT-LE cooperation
- level of CSIRT maturity ⁽⁶⁾
- size of the CSIRT
- common law/civil law legal tradition.

2.4 Contribution by subject-matter experts

ENISA selected eight external subject-matter experts from the list of NIS experts compiled following the ENISA CEI (Ref. ENISA M-CEI-17-T01) (ENISA, n.d.(b)).

Six of them contributed to this report by supporting the data collection and the drafting while two were reviewers. The two CEI experts contributing as reviewers reviewed this report in several rounds including the first draft in April 2018, an intermediate draft in June 2018, the semi-final and the final draft in August 2018. They reviewed it in addition to ENISA reviewers and other external reviewers.

All eight experts contributed *ad personam*.

These experts contributed inter alia with their expertise in NIS aspects of cybercrime, including but not limited to CSIRT and law cooperation, operational cooperation, information sharing to handle incidents and to fight against cybercrime.

⁽⁶⁾ On CSIRT maturity, see (ENISA, n.d.(a)).

3. CSIRTs, LE and the judiciary: framework, information flow and tools

This chapter gives an overview of select legal provisions which have an influence on the rules governing the criminal procedures, including the admissibility of digital evidence. This chapter also discusses in detail the roles, structures and strengths of CSIRTs, LE and the judiciary and explores the current interaction and the information flow and the tools used.

3.1 Some general remarks

Below some preliminary remarks are made related to the context surrounding the cooperation between CSIRTs and LE and their interaction and information flow with the judiciary.

3.1.1 Criminal procedures: non-adversarial versus adversarial

'The Member State judicial systems are very diverse, reflecting differences in national judicial traditions (European Justice, n.d.(a)) and the legal traditions have an influence on the various areas of law. Concerning criminal procedural law, a distinction should be made between the non-adversarial system (also called, inquisitorial system), typical of civil law tradition, and the adversarial system (also called adversary system), typical of common law countries, (Delmas Marty & Spencer, 2004).

In an adversarial system (or adversary system) a criminal trial is conceived as a conflict or dispute. Each of the parties supports a contrary position. In these systems the oral evidence is of fundamental importance and the method of taking such evidence is based on the so-called cross examination. Although there are exceptions, in such a system the judge does not tend to play an active role in the collection of evidence. The judge must in fact guarantee respect for fairness and equality and be neutral with respect to the parties. The decisions of the judge set precedents.

In a non-adversarial system, the criminal trial is not conceived as a conflict or dispute but is instead conceived as something like an inquiry. In such a system, the judge sometimes has a more active role in the collection of evidence and can also interview the witnesses.

These differences between non-adversarial system and adversarial systems may influence the shaping of the relationships between CSIRTs and LE and the judiciary. Furthermore, the value of e-evidence can also change between the systems.

3.1.2 Criminal proceedings

Since this report deals with the cooperation between CSIRTs and LE and their interaction with the judiciary, the focus is on criminal proceedings.

As defined above, by criminal proceedings we refer to proceedings aiming to ascertain whether a crime has been committed and if so, by whom.

Principles and rules governing criminal proceedings are different from those governing civil, administrative, disciplinary or other proceedings.

The criminal procedure in each country is governed by the relevant legal provisions, in most cases by the criminal procedure code or similar. While criminal procedure differs dramatically by jurisdiction, in most cases we can identify common principles and features.

To ascertain whether a crime has been committed and if so, by whom, it is necessary to carry out a criminal investigation. This is followed, once there are the conditions for it (e.g. sufficient elements to believe that the suspect committed the crime), by a criminal charge and a formal criminal trial, which can be either non-adversarial or adversarial in form (based on the legal system, as discussed above). At the trial, the judge (or the jury) finds the defendant either guilty or not guilty based on the evidence presented by the prosecutor and the defendant. In a criminal trial the prosecution bears the burden of proof, which means that the prosecutor must prove beyond reasonable doubt that the defendant committed the crime.

While most criminal cases are decided before national (or regional, or local) courts, under certain conditions it is possible that the process is held by a supranational court, such as one of the following.

- The European Court of Human Rights (European Court of Human Rights, n.d.), which rules on individual or state applications alleging violations of the rights set out in the European Convention on Human Rights. It has its seat in Strasbourg, France. For an overview of case-law of the European Court of Human Rights in the area of human rights and criminal procedures see (McBride, 2018).
- The Court of Justice of the European Union (Court of Justice of the European Union, n.d.), which ensures compliance with EU law and rules on the interpretation and application of the treaties establishing the European Union. It has its seat in Luxembourg.
- The International Court of Justice (International Court of Justice, n.d.), which is a body of the United Nations based in The Hague, The Netherlands.

The outcome of most criminal law cases depends upon the admissibility and strength of evidence presented by the prosecution or the defence. The evidence can take many different forms including physical evidence, testimonies, documents or e-evidence. While the admissibility of evidence is discussed in the following section, on the strength of the evidence we can say that the rules and practices for determining it differ from one jurisdiction to another, but in general, the standard of proof is high in criminal proceedings and therefore high-quality evidence is expected. Therefore, it is desirable (particularly in the case of electronic evidence) to ensure close cooperation between public prosecutors and experts to ensure that evidence is collected and handled with professional care.

As mentioned in Section 1.5 — Definitions of key concepts, we can, in general, identify two main categories of cybercrime.

- Cybercrimes in the strict sense, are crimes where the computer is the object and they are normally also committed by means of information technology (IT) tools. This is the case of illegal access to information system.
- Cybercrimes in a broad sense, which are crimes that are committed by using an IT tool but could also be committed without the use of IT tools, like in cases when data is instrumentalised, e.g. homicide of a patient by manipulating data related to that patient's health (i.e. the medical treatment administered according to the manipulated patient details results in the patient's death).

Except for cases dealt by a supranational court, normally (cyber) crime cases are decided before national (or regional, or local) courts.

3.1.3 Admissibility of electronic evidence in criminal courts

As highlighted in Council of the European Union *Final report on the seventh round of mutual evaluations on 'The practical implementation and operation of the European polices on prevention and combating cybercrime'*, the 'nature of e-evidence may create issues regarding admissibility that do not arise with other types of evidence. For this reason, in some Member States there are specific requirements regarding the collection of e-evidence to be admissible in courts. However, the evaluation has shown that in most Member States, procedural law is mainly technology-neutral, which means that general rules and principles on gathering of evidence are applied and that the procedural system does not contain any specific formal rules on admissibility and assessment of e-evidence' (Council of the European Union, 2017, p. 11). On the topic of e-evidence in court see for instance the AEEC project (Admissibility of electronic evidence in court (AEEC) project, 2006), a pioneer EU project in the field (see also (Insa, Fredesvinda , 2007), and the Evidence project (Evidence project).

It is important that the collection of e-evidence complies with all of the relevant principles, such as data integrity, audit trail, specialist support, appropriate training and legality (ENISA & Anderson, 2014a, p. 5).

E-evidence is fragile by nature and often volatile. Digital data can be easily lost or altered. If e-evidence is collected in an unsuitable manner, there is a risk that the content of that e-evidence does not correspond to the original content. There is therefore the risk that e-evidence cannot be used to help establish (or refute) that a crime has been committed. To avoid this risk, some best practices have been developed internationally. It is important that all personnel dealing with e-evidence know these best practices. Examples of best practices include the *ISO Guidelines for identification, collection, acquisition, and preservation of digital evidence* (International Organisation for Standardisation (ISO), 2012), the *NIST Guide to integrating forensic techniques into incident response (SP-800-86)* (National Institute of Standards and Technology (NIST), 2006) (in particular, NIST Chapter 3), *Electronic evidence — A basic guide for first responders* (ENISA & Anderson, 2014a), *Data acquisition guidelines for investigation purposes* (CERT-EU, 2012), the *Guidelines on digital forensic procedures for OLAF staff* (EU: European Anti-Fraud Office (OLAF), 2016a)), and the United Kingdom *ACPO Good practice guide for digital evidence* (The Association of Chief Police Officers of England, Wales and Northern Ireland (ACPO), 2012).

3.2 Applicable legal and policy framework

This section gives an overview of the relevant legal and policy framework that shapes the cooperation and interaction between CSIRTs, LE and their interaction with the judiciary. The section goes on to discuss recent developments that may impact or influence this cooperation and interaction such as the recent introduction of the General Data Protection Regulation (GDPR) (European Parliament and Council of the European Union, 2016b).

3.2.1 An Overview of the relevant legal and policy framework

The legal and policy context play an important role in governing and shaping the cooperation between CSIRTs and LEs and their interaction with the judiciary in the context of fighting against cybercrime. The main legislative and policy components of this framework are listed below. More information on the legal

and policy framework is available in the 2017 ENISA report *Improving cooperation between CSIRTs and law enforcement: Legal and organisational aspects* (ENISA, 2017a).

- The national legal and policy framework governs and shapes the cooperation between CSIRTs and LEs and their interaction with the judiciary. Transposition of the international and European law is an important component of the national criminal law and criminal procedure law. There might be however some specificities in legislative provisions depending on the country.
- At the international level, the Council of Europe convention on cybercrime (Council of Europe, 2001), often referred to as the 'Budapest Convention', is the first international treaty and remains the most relevant international treaty on cybercrime and electronic evidence. It is the 'only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between state parties to this treaty' (Council of Europe, n.d.)
- At EU level several legal and policy instruments are particularly relevant when discussing the cooperation between CSIRTs and LEs, *inter alia* the following.
 - Directive on attack against information systems (European Parliament and Council of the European Union, 2013a).
 - NIS Directive (European Parliament and Council of the European Union, 2016e).
 - *Cybersecurity strategy of the European Union (CSS)*(European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013).
 - Joint Communication on resilience, deterrence and defence: Building strong cybersecurity for the EU (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2017).
 - Commission recommendation on coordinated response to large scale cybersecurity incidents and Crises ('Blueprint') (European Commission, 2017a).
 - Commission communication on strengthening Europe's cyber resilience system (European Commission, 2016).
 - European Investigation Order (European Parliament and Council of the European Union, 2014).
 - EU data protection legislation, including the GDPR (European Parliament and Council of the European Union, 2016b), Directive on privacy and electronic communications (European Parliament and Council of the European Union, 2002), law enforcement data protection directive (LEA DP Directive) (Council of the European Union, 2008) (GDPR is addressed in this report in more detail in Section 3.2.2.1.)
 - Proposal for a Regulation on European production and preservation orders for electronic evidence (European Commission, 2018) (Addressed in more detail in Section 3.2.2.2.)
 - Proposal for a directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (European Commission, 2018a) (Addressed in more detail in Section 3.2.2.2.)
 - ENISA regulation (European Parliament and Council of the European Union, 2013b).
 - In addition, there are some EU instruments that play a role in support of the cybersecurity collaboration at international scale, such Instrument contributing to Stability and Peace (IcSP) (European Commission, n.d.(e)), European Neighbourhood Instrument (ENI) (European Union External Action Service, 2017) and Instrument for Pre-Accession Assistance (IPA) (European Commission, n.d.(f)).

Some of the most significant recent developments in the legal and policy framework shaping the CSIRT and LE cooperation and the interaction with the judiciary concern these two areas.

- The GDPR (European Parliament and Council of the European Union, 2016b) and data protection law enforcement directive (European Parliament and Council of the European Union, 2016).
- The proposals for a regulation and for a directive to improve cross-border access to e-evidence (European Commission, 2018) (European Commission, 2018a).

3.2.2 Some recent developments

3.2.2.1 General Data Protection Regulation (GDPR) and the data protection law enforcement directive

The GDPR (Regulation (EU) 2016/679) (European Parliament and Council of the European Union, 2016b) strengthens the protection of natural persons with regard to the processing of personal data and on the free movement of such data. It came into force on 24 May 2016 and applied from 25 May 2018. Some Member States have already adopted this legislation, others are working on its preparation, but this does not affect the binding nature of the regulation itself.

The Data Protection Law Enforcement Directive (Directive (EU) 2016/680) 'protects citizens' fundamental right to data protection whenever personal data are used by criminal-law-enforcement authorities. It will ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism' (European Parliament and Council of the European Union, 2016). It entered into force on 5 May 2016 and EU countries had to transpose it into their national law by 6 May 2018. Currently (status: 26 October 2018, see (EUR-lex, n.d.)), only 16 Member States (Belgium, Czech Republic, Germany, Ireland, France, Croatia, Italy, Lithuania, Luxembourg, Hungary, Malta, Austria, Portugal, Slovakia, Sweden and the United Kingdom) reported adoption of transposition measures in relation to this Directive.

The GDPR and the data protection law enforcement directive have different scopes.

- Article 1.1 of the GDPR provides that 'this regulation lays down rules relating to the protection of natural persons regarding the processing of personal data and rules relating to the free movement of personal data' (?);
- Article 1 of the data protection law enforcement directive 'lays down the rules relating to the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.

Due to the respective field of application of the GDPR and the data protection law enforcement directive, it can be said that in principle, both the GDPR and data protection law enforcement directive may apply to the CSIRTs when they deal with (including storing) personal data. However, it depends on the case.

(?) The first judgment on Regulation (EU) 2016/679 was issued on 29 May 2018. This is a German ruling, specifically, of the Court Order of the Regional Court of Bonn, 10 O 171/18, on the principle of data minimisation (ICANN v. EPAG Domainservices GmbH, 2018). Non-official translation to English (ICANN v. EPAG Domainservices GmbH, 2018b).

Under Article 6.1 a) of the GDPR, the processing of personal data, including IP addresses, is permitted for a specific, necessary and proportionate purpose (purpose of legitimate interest pursued by the CSIRTs, as specified on Article 6.1 f) if the data subject (the person concerned, the person whose personal data are processed) gives consent. In the event of an IT incident, there is no consent from the data subject (e.g. IP address holder) who caused the incident. However, according to the GDPR (see Article 13.3) and to Recital 49 it can be considered that the personal information, under certain circumstances, can be processed by the CSIRT even without consent. Recital 49 indeed provides that ‘The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), CSIRTs, by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping “denial of service” [DoS] attacks and damage to computer and electronic communication systems.’

If a CSIRT processes personal information, including IP address, on the basis of a specific mandate or delegation from competent authorities (e.g. by a police officer or by the prosecutor) for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the GDPR does not apply, the data protection law enforcement directive will apply to CSIRT instead.

As explained in Recital 11 of the data protection law enforcement directive ‘competent authorities [for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities] may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this directive’ (European Parliament and Council of the European Union, 2016). Therefore, if the CSIRT is bound by contract/legal act to collect and process personal data solely for the purposes mentioned in the directive, GDPR does not apply. The application of the GDPR on the other hand remains unaffected for the processing of personal data by the CSIRTs outside the scope of this directive.

The data protection law enforcement directive applies to LEA if the directive has been implemented in the Member State (a Directive, unlike a Regulation, is not directly applicable). This directive does not require the consent of the data subject, depending on the particular purposes for which the data are processed.

According to Article 2 par. 2 (d), the GDPR does not apply to the processing of personal data ‘by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to

public security'. Although the GDPR does not apply in these cases, the data protection law enforcement directive applies instead⁸.

Article 45 par. 2 of the data protection law enforcement directive stipulates the conditions of control by the supervisory authority and it states that 'Each Member State shall provide for each supervisory authority not to be competent for the supervision of processing operations of courts when acting in their judicial capacity'.

3.2.2.2 Proposals for a regulation and a directive to improve cross-border access to electronic evidence

As stated in the European Communication of April 2018 in the *Fourteenth progress report towards an effective and genuine security Union*, 'Electronic evidence has become relevant in a large majority of criminal investigations and increasingly often, judicial authorities need to make a request in another jurisdiction to obtain necessary evidence from service providers. Making it easier and quicker to obtain this evidence across borders is therefore of crucial importance for investigating and prosecuting crime, including terrorism or cybercrime' (European Commission, 2018b, p. 1).

Currently the cross-border requests for e-evidence are processed through the mutual legal assistance (MLA) instruments, through the European Investigation Order or based on voluntary cooperation. However, the current framework does 'Not fit for today's volume of requests' and there is a 'Lack of connection with the receiving state' (European Commission, 2018c).

Therefore, the European Commission proposed a new legislative package with measures to improve cross-border gathering of electronic evidence, in particular the following.

- The proposal for a regulation on European production and preservation orders for e-evidence in criminal matters (European Commission, 2018).
- The proposal for a directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (European Commission, 2018a).

These proposals should enable LE to order any service provider offering services in the EU to produce or preserve electronic evidence, regardless of the location of data or the service provider. European production and preservation orders should be based on mutual recognition⁽⁹⁾, which means that it should be directly binding and enforceable to both the service provider and relevant enforcing authority. These orders should therefore allow for an effective and fast response of the LE to reported incidents and

⁸ See art. 1 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

⁽⁹⁾ Mutual recognition in criminal proceedings means that a specific judicial decision from one Member State should be directly enforceable in any other Member State without further formalities or validation. This mechanism should be, in comparison with traditional mutual legal assistance, far more effective and efficient.

cybercrimes and effective collection of volatile e-evidence. CSIRTs might help the LE with the correct targeting of the orders and may also benefit from the data collected by the LE using the orders. On the other hand, (private) CSIRTs might also be in the position of the service providers and therefore be required to comply with the order.

3.3 CSIRTs, LE and the judiciary: roles, structures and strengths

This section provides an overview of roles, structures and strengths of the three communities (CSIRTs, LE and judiciary).

3.3.1 The role of CSIRTs, LE and the judiciary

This section provides an explanation of the roles of CSIRTs, LEs and the judiciary (prosecutor and judges).

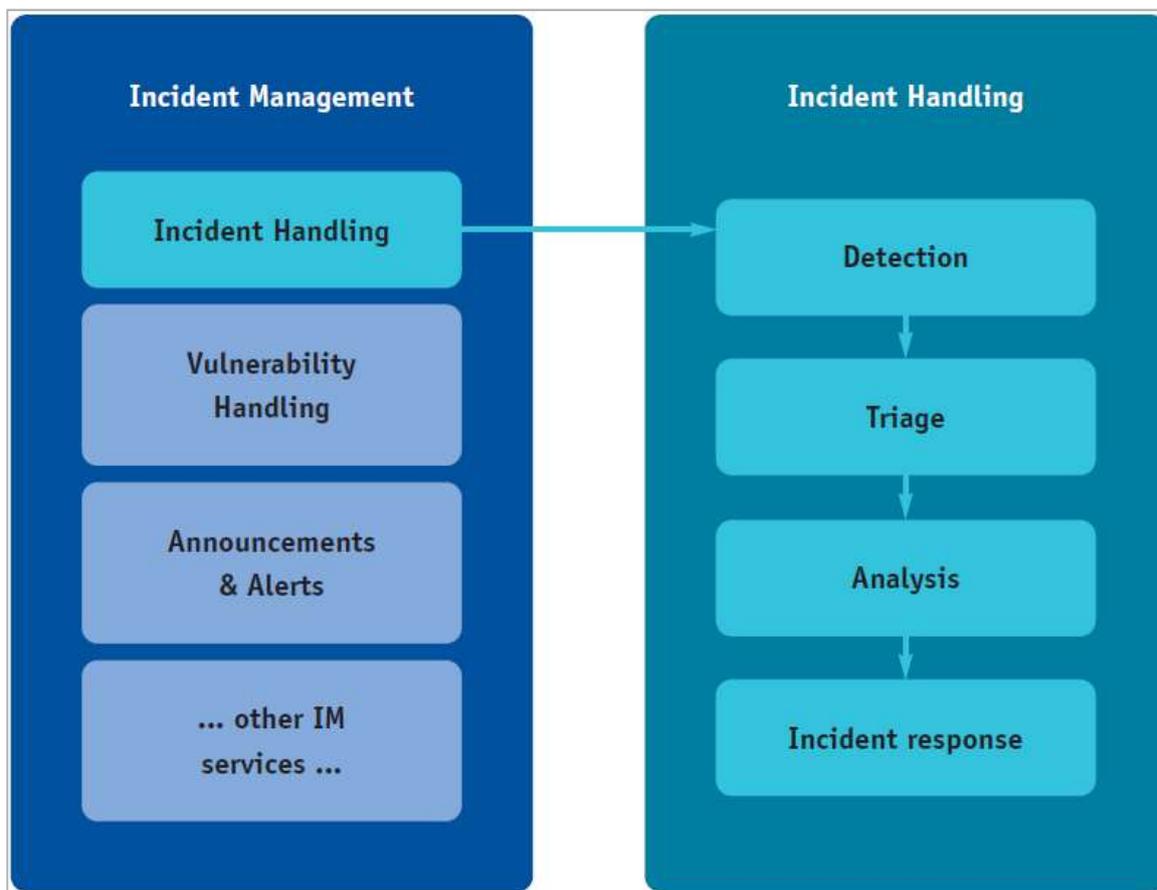
3.3.1.1 The role of the CSIRTs

The main role of the CSIRT is to protect their constituency by preventing and containing IT incidents, primarily from a technical point of view.

Annex I of the NIS Directive (European Parliament and Council of the European Union, 2016e), in addition to the requirements, lists the tasks of the CSIRTs, which includes at least: '(i) monitoring incidents at a national level; (ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents; (iii) responding to incidents; (iv) providing dynamic risk and incident analysis and situational awareness; (v) participating in the CSIRTs network.'

CSIRTs deal with incident management (IM), including incident handling. The figure below provides an overview of IM and incident handling stages.

Figure 3 — Incident management and incident handling stages (Source: (ENISA, 2010, p. 10)



It must be noted that ‘CSIRTs do not have the powers of [law enforcement] LE vis-à-vis private subjects, but as regards attacks of a criminal nature (not all the cyber incidents are criminal acts), have an important role in supporting the investigations, as they can help to provide information and to secure e-evidence’ (Council of the European Union, 2017, p. 67). CSIRTs play an important role and ‘have to work closely with law enforcement [LE] and other authorities’ (ENISA, 2015c, p. 9). Additionally, CSIRT have an ongoing need to collaborate and communicate within their constituency and across other communities they interact with such as LE and the judiciary (ENISA, 2018, p. 16).

During the incident management and handling process, CSIRTs acquire, store and process data and they need to be aware that the data they process and retain can be crucial for the investigation and the prosecution of a crime in a criminal trial, it is important that their role, in responding to cybercrime too, is recognised.

As mentioned in Recital 62 of the NIS directive (European Parliament and Council of the European Union, 2016e) indeed ‘Incidents may be the result of criminal activities the prevention, investigation and prosecution of which is supported by coordination and cooperation between operators of essential services [see Annex II of the NIS directive], digital service providers, competent authorities and law-enforcement authorities [LEAs]. Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage operators of essential services and digital service providers to report incidents of a suspected serious criminal nature to the relevant law-enforcement authorities. Where appropriate, it is desirable that coordination between competent

authorities and law-enforcement authorities of different Member States be facilitated by the European cybercrime centre (EC3) and ENISA’.

3.3.1.2 The role of the LE

The role of the LE in carrying out investigations is aimed at collecting information and evidence on whether a crime has been committed (or is going to be committed) and by whom. LE needs to collect evidence in compliance with the law and according to the powers conferred on them. In some occasions, LE has the possibility to collect the evidence directly, but in many cases the evidence is provided by others involved. It is of paramount importance to remark that if the evidence collected has been tampered with or partially deleted by the first responders, the future value of that evidence to support a criminal case during the indictment¹⁰ will be significantly or even totally affected.

3.3.1.3 The role of the judiciary

The role of the judiciary is variable depending on the specificities of the legal system considered; however, it is possible to identify three main functions of the judiciary.

- The judiciary (namely prosecutors) supervises investigations (normally conducted by the LE).
- The judiciary acts as body for the protection of fundamental rights.
- The judiciary (namely judges) decides whether a crime has been committed and by whom.

Some further details are provided below on the role of the prosecutors and judges. It must be noted that differences exist between legal systems and the particularities of each legal system cannot be covered in this report.

3.3.1.4 The role of the prosecutors

‘The public prosecutors’ office or prosecution service, which is regarded as part of the judiciary in most Member States [and for this report], plays an essential role in criminal proceedings. The responsibilities and status of public prosecutors vary considerably among Member States’ (European Commission (run by), n.d.(b)).

The prosecutor normally coordinates and supervises criminal investigations and formulates the charge (when there are sufficient elements for it).

3.3.1.5 The role of the judges

The judge plays a central role in the criminal proceedings. Judges issue orders to perform procedural measures and to collect evidence, decide on the admissibility and relevance of the evidence, determine the facts, interpret the law and decide the case by sentencing the criminal defendants or by dismissing the case. Most important of all, judges are impartial decision-makers in the pursuit of justice.

The judge is in charge to guarantee that the whole investigation and trial is in compliance with civil liberties and the rights of persons charged with a criminal offence. Article 6 par. 2 of European Convention

¹⁰ An indictment is a formal charge of a serious crime.

on Human Rights (Council of Europe, 1950) affirms the right to a fair trial, including that ‘Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law’. Also, the civil liberties and the rights of the other parties participating in a trial must be complied with (for example, witnesses).

3.3.2 The structure of CSIRTs, LE and the judiciary

This section provides an outline of the structures of CSIRTs, LE and judiciary.

3.3.2.1 The structure of the CSIRTs

A CSIRT is a team of IT security experts whose main business is to respond to computer security incidents, providing the necessary tools and services to handle them and support their constituents to mitigate the incidents. Also, most CSIRTs provide preventative and educational services for their constituency, issuing warnings on vulnerabilities, and also providing awareness to users about threats and scams taking advantage of these flaws.

Based on their duties and area of responsibility (constituency), there could be national, governmental, sectoral and private CSIRTs. The NIS Directive (European Parliament and Council of the European Union, 2016e) does not make any reference to this categorisation of CSIRTs, and only states that Member States are to designate one or more CSIRTs to cover certain industry sectors. Usually national and governmental CSIRTs are designated by the Member States as CSIRTs under the NIS Directive.

National and governmental CSIRTs play a key role in coordinating Incident Management with the relevant stakeholders at national level. In addition, they bear responsibility for cooperation with the national and governmental teams in other countries, and also as part of the CSIRTs network established by the NIS directive.

3.3.2.2 The structure of the LE

The LE structure has been designed to comply with both their stated missions and their legal framework of intervention. Although the structure differs among Member States, generally LE is hierarchically organised to identify each level’s responsibility and accountability. Normally each level is dedicated to a certain level of decision-making and should be accountable for any action taken. LE usually fulfils the following missions: general policing, prevention, investigating, public order and security purposes.

Depending on the countries’ institutional landscape, the history and the legal systems, LE have different structures and may be organised in a more centralised way. At national level, again depending on the Member State, LE might be organised as a two-layer system: central entities that host the most specialised teams (organised crime, terrorism, intelligence, support units) and regional services which provide a service closer to the population. Central units normally deal with the nationwide and transnational crime, while regional units tend to lead investigations in their jurisdiction only.

At international level, international entities provide coordination support among LE. Europol is the LE coordinating the European Member State police forces. It provides them with intelligence, analysis capacities (analysts and tools) as well as coordination support for joint operations. Europol is competent to support and strengthen action taken by MS authorities in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States only. Each MS has

competent authorities which are the single point of contact for any operational and strategic communication between them. When an MS LE needs cooperation from another MS LEA, it needs to have a clear and identified point of contact to deal with, without necessarily having to be informed on the operational model of each police force.

The Europol Liaison Bureaux (ELB) ⁽¹¹⁾ and the joint cybercrime action taskforce (J-CAT) ⁽¹²⁾ serve as liaison officers focused on strengthening operational cooperation in fighting cybercrime. ELB support the law-enforcement activities of the Member States against cybercrime by facilitating the exchange of information between Europol and its liaison officers; ELB are also a Point of Contact (PoC) as are Europol National Units (ENUs) to provide information and advice in the analysis of information concerning their seconding state. (Hillebrand, 2012). J-CAT is a country-led innovative framework that includes both EU and non-EU countries that operates from Europol's headquarters and it is supported by Europol's European cybercrime centre (EC3). The objective of J-CAT is to drive intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the joint identification, prioritisation, preparation and initiation of cross-border investigations and operations by its partners.

Interpol is the global police organisation. With 190 members, it is the second largest international organisation after the United Nations. The organisation works with a network of Interpol national central bureaus (NCBs) which are also single PoCs in each country (Interpol, n.d.a), like the Europol ENUs. Both the NCBs and ENUs are LE-only entities — the information sharing is not authorised to non-LE third parties.

The Interpol spectrum covers all EU Member States as well as countries outside the EU. While Europol and Interpol are two separate organisations they cooperate on a day-to-day basis ⁽¹³⁾.

3.3.2.3 The structure of the judiciary

'While the judicial systems of the Member States differ significantly in detail, there is a set of common principles which apply to all of them, as well as to the EU as such. One of these common principles is that the courts must be impartial and independent of the government and the legislating institution (i.e. the institution(s) passing the law). This principle of independence of the judiciary is one of the values on which the EU is founded: the rule of law and respect for freedom, equality and fundamental rights. It is expressly mentioned in Article 47 of the Charter of Fundamental Rights of the EU, and in Article 6 of the European Convention on Human Rights' (European Commission (run by), n.d.d).

As for the structure of the CSIRTs and the LE, the actual structure of the prosecution office and of the courts vary from country to country. However, there are certain similarities as described below.

3.3.2.4 The structure of the prosecution service

Normally the prosecution service is organised in a hierarchical way: each prosecutor reports to the respective superior prosecutor and there is a prosecutor-general who heads the entire prosecutor's office.

⁽¹¹⁾ <https://www.europol.europa.eu/partners-agreements/member-states>

⁽¹²⁾ <https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce>

⁽¹³⁾ In the case of cross-border crime that involves countries outside Europe, or countries with which Europol does not have operational agreements.

Depending on the country, the prosecution office might have a more centralised structure or a more decentralised one.

Generally, the structure of the prosecution service mirrors that of the court system or it is even part of it (e.g. in countries where prosecutors and judges are part of the same structure while performing different roles).

3.3.2.5 The structure of the courts

The national court systems are normally divided into branches (e.g. ordinary civil and criminal, administrative, military, etc.). The ordinary criminal court systems are generally organised into first-, second- (e.g. courts of appeal) and third-instance courts (e.g. supreme courts), and their centralised/decentralised structure depends on the governmental or constitutional structure of the country.

Normally the ministry of justice is responsible for matters related to court organisation, including budget. In some countries a supreme council of the judiciary is established as a central body responsible for guaranteeing the independence of the judiciary.

Eurojust has been set up with the aim of supporting the MS competent national authorities (including prosecutors and judges) when they deal with serious cross-border and organised crime. Eurojust is 'composed of national prosecutors, magistrates, or police officers of equivalent competence, detached from each Member State according to their own legal systems' (Eurojust, n.d.). The European Council, in its Conclusion 46, agreed that a unit (Eurojust) should be set up, composed of national prosecutors, magistrates, or police officers of equivalent competence, detached from each Member State according to their own legal systems (Eurojust, 2018).

3.3.2.6 The Role of CSIRTs, LE and the judiciary along with the workflow of responding to cybercrime

According to the data collected, the role of each community (CSIRTs, LE and judiciary) along the workflow of responding to cybercrime can be described as follows.

- **Discovery of the crime:** LE can receive a crime report (e.g. from the victim) or discover a suspicious activity by itself. The CSIRT can discover a suspicious activity during incident handling and, depending on the legal system may have/has an obligation to inform LE of the activity. In some Member States, at least under certain circumstances, CSIRT (the focus of this report is national and/or governmental CSIRTs) in certain circumstances national or governmental CSIRTs must inform the prosecutor of any activity that might be considered criminal.
- **Criminal investigation:** normally LE conducts the criminal investigation while the prosecutor defines the strategy of the case, sets the evidence threshold and supervises it. The judiciary ensures that the investigation is conducted in compliance with civil liberties and guarantees⁽¹⁴⁾ and defines the limits of protection of the rights of the persons investigated.. Depending on the severity of the crime and the complexity of the case, the investigation means used (undercover police investigation, use of

⁽¹⁴⁾ On common minimum rules concerning certain aspects of the presumption of innocence in criminal proceedings and the right to be present at the trial in criminal proceedings see (European Parliament and Council of the European Union, 2016a). For an overview of case-law of the European Court of Human Rights in the area of human rights and criminal procedures see (McBride, 2018).

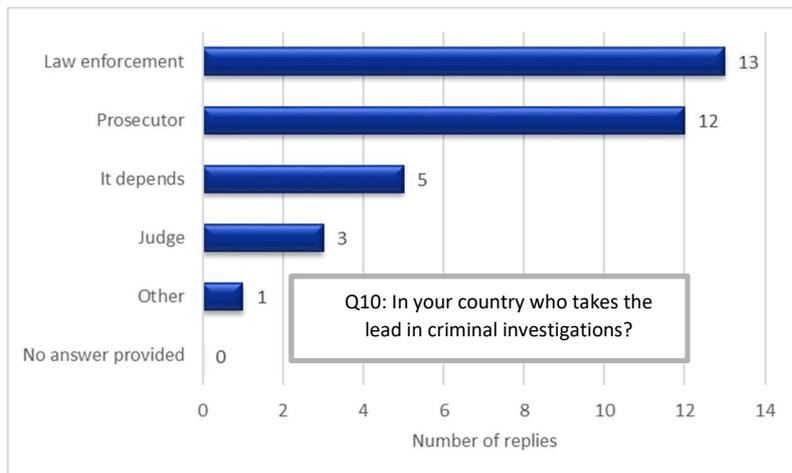
wiretaping technology, etc.) vary. CSIRT may play a role in the investigation by providing technical expertise and supporting the evidence collection (and preservation) by sharing information they have, or they have access to. As stated in the 2017 ENISA reports on CSIRT and LE cooperation (ENISA, 2017a) (ENISA, 2017) and confirmed during the interviews conducted for this report, CSIRTs and LE indeed often exchange information (both formally and informally) related to cybercrime cases, for instance to avoid interference in their actions. CSIRTs can support the investigations by providing LE with useful information for the investigations. When a more formal involvement of CSIRTs is required during the criminal investigations, the prosecutor usually needs to be consulted and give consent for the involvement of CSIRT in digital evidence acquiring, handling and analysis. This is because CSIRTs are not operating under the strict LE rules.

- **Prosecution either press charges or suspend/archive the case:** a criminal proceeding normally starts after the formal criminal charge (i.e. the formal accusation), usually made either by the prosecutor or by the police; it ends with the conviction or acquittal of the defendant. If the evidence collected support a charge then the competent authority (normally the prosecutor) formulates the charge and the suspect (normally from this point onwards called 'the defendant') is brought to court. If the amount and quality of the evidence collected during the criminal investigation is not sufficient to proceed or if the evidence collected shows that the facts do not have the elements to constitute a crime, in several states the prosecutor can discard the case. This however does not mean that the CSIRT must discard the eradication and the recovery phase (ENISA, 2016d, p. 10); an important phase of the incident response and that still needs to be performed from the incident handling process (SANS, 2011, p. 8).
- **Trial:** although (according to the data collected) this happens in general very rarely, a member of the CSIRT may be called to play a role in the process before a criminal court aiming to decide whether a person (after the formal charge, 'the defendant') has committed a crime. At least in some Member States a CSIRT expert can be called to testify as an (expert) witness in computer crime cases. The CSIRT experts testify based on the general rules of testimony normally set out in the criminal procedural codes. However, according to the data collected via interviews and the online survey, the cases where CSIRT experts are called as witnesses in criminal proceeding are not frequent at all. Some interviewees stated that in some cases, detailed reports from CSIRTs are also used in criminal proceedings to support the decision on the conviction or the acquittal of the defendant. Furthermore, CSIRTs can also provide other forms of evidence (for instance, a cloned image of a hard disk) to be used in criminal proceedings. CSIRTs have a long history of cooperation across the EU and they coordinate by means of a CSIRT secretariat function provided for in the network and information security directive (NISD).

All of the examples given above of course vary depending on the legal systems and on the specificities of the crime, including its severity.

Based on the data collected via the online survey and the literature research, it is clear that LE and/or prosecutors take the lead in criminal investigations.

Figure 4 — Replies to question 10 of the online survey conducted for this report



3.3.3 Strengths of the three communities

The main strengths of the CSIRT and LE communities identified by the data collected via the online survey (see Figures 5 and 6) include the following.

- For the CSIRTs: the use of agile processes, the technical skills and the technical tools used, as well as the well-established cooperation they have within and outside the CSIRT community (e.g. security companies and internet service providers (ISPs)).
- For the LE: the ability to draft detailed reports to be used in criminal proceedings, the knowledge of the chain of custody and the requirements for admissibility of evidence in court as well as the detective skills and well-defined roles which are easy to understand by all parties.

Figure 5 — Replies to question 15 of the online survey conducted for this report

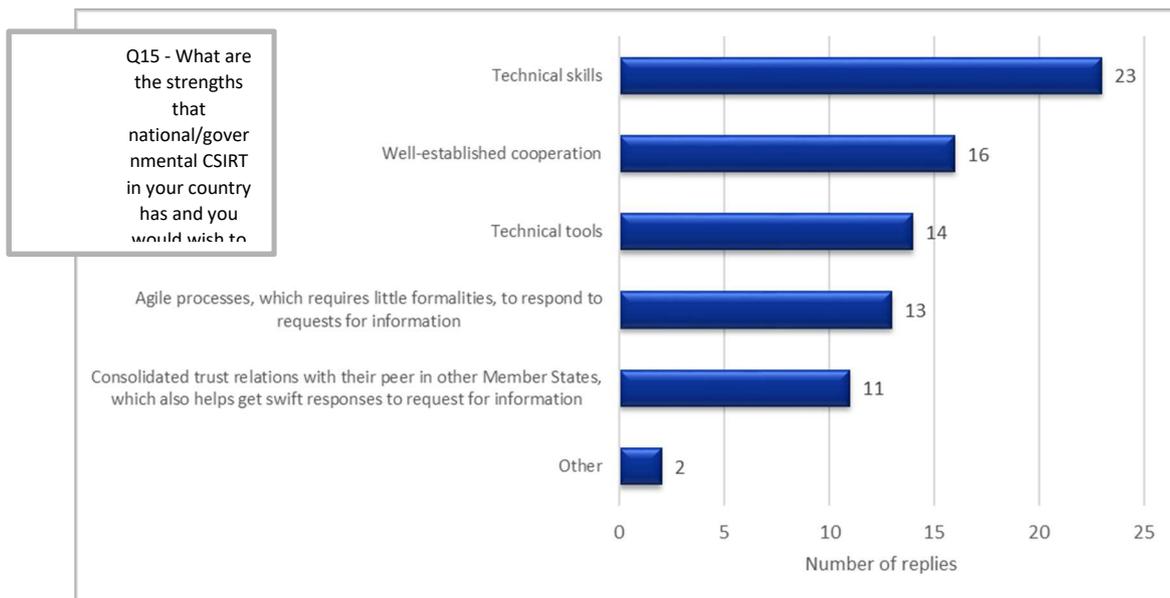
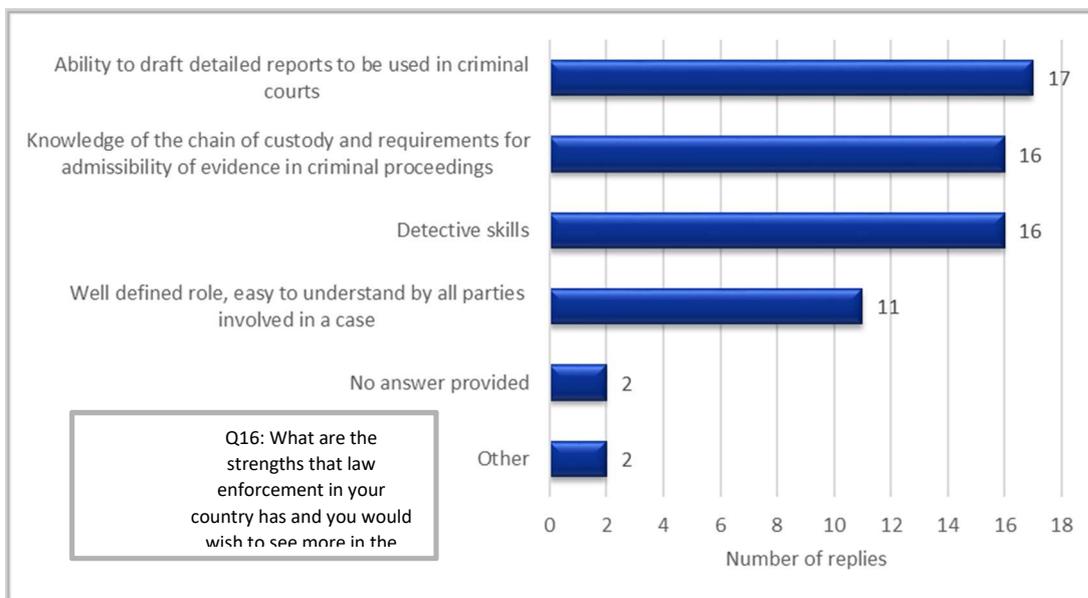


Figure 6 — Replies to question 16 of the online survey conducted for this report



No specific data were collected via the online survey on the strengths of the judiciary. However, from some statements made by the subject-matter experts interviewed it can be derived that prosecutors and judges (because of their role, experience and background) have a deep knowledge of matters related to admissibility of evidence and the delicate balance between the need for collection and preservation of e-evidence to prosecute crime and the protection of the fundamental rights.

3.4 The interaction and the information flow across CSIRTs, LE and the judiciary

This section addresses the interaction and information flow across CSIRTs, LEs and the judiciary, in particular focusing on LE’s direct and indirect interactions during investigations, the duties of CSIRTs followed by an in-depth discussion on the types of information that is exchanged.

Cooperation between CSIRTs, LE and the judiciary can be mutually beneficial. This is also illustrated by examples from practice. One of these examples can be the cooperation between a national/governmental CSIRT or another CSIRT (e.g. a university CSIRT) and the police in the case of attempted hacker attacks on a computer system, as illustrated in the example in the box.

Example of cooperation between CSIRTs, LEs and the judiciary

A CSIRT detects an incident likely to be a crime (e.g. an attack against an information system) and informs the police/files a complaint with the police, which in turn ask for the details about the incident and possible evidence.

Thanks to the close cooperation and the police instructions, the CSIRT is able to collect relevant traffic and localisation data in a way that allows it to be used as evidence in court. Further investigation reveals that the incident was of a larger scale than initially estimated and that further data are needed from other service providers. Therefore, using the police procedural tools and the expertise of the CSIRT staff, additional data are requested from the operator of the network, through which the communication traces of the attacker are identified, and other victim organisations are identified.

The data obtained reveal that the attacker's communication in several cases was led through servers in a different jurisdiction. Thanks to the involvement of the CSIRT and the CSIRT community, additional necessary operational data from a CSIRT in a different country are obtained and then made available to the police. Obtaining these data following the standard measures of international police and judicial cooperation in criminal cases would have taken much longer. At the stage of analysing, processing and applying the evidence in court, the police can also use advanced forensic tools and CSIRT personnel's expertise.

Following this positive experience of cooperation, both the police and the CSIRT are able to identify problematic areas of cooperation that they can then streamline. For example, within the CSIRT, internal processes for informing the police/filing complaints with the police and for collecting evidence or passing it on to LE are established. On the part of the police, means for securing the electronic transfer of digital evidence are implemented, as well as procedural measures for cooperation with security teams, including measures that allow secure two-way sharing of sensitive information. On the part of the court, the possibility of using a CSIRT employee as an expert witness, who is able to explain to the court the technical details of the case and the specifics of the individual pieces of evidence, is verified.

3.4.1 Indirect v. direct interaction between CSIRTs and prosecutor and judge

The default approach for an investigation is that LE undertakes the investigative aspects of an incident and the prosecutor supervises the investigation. The leads to follow, the targets to work on and the legal framework are decided by the prosecutor. While it is normally done through cooperation, where there is any disagreement the final say is with the prosecutor and, in some case, with the judge. In several EU Member States, when a crime is ongoing, or the incident has just occurred (e.g. within 24 hours), LE can undertake immediate actions such as searches, arrests and warrants without the prosecutor's prior agreement (although a validation of the measures taken is then needed) and only for as long as a prosecutor has not been assigned to or not taken the lead in the investigation yet.

As an investigation unfolds, LE and prosecutors continually make decisions to adapt to the circumstances of the events. In this situation, the CSIRTs can be formally asked to cooperate by providing their technical expertise or data that they may have e.g. in their own systems or via their channels.

CSIRTs normally interact with LE much more rarely do they engage directly with the prosecutor. Several interviewees described the normal information flow as 'linear', in other words CSIRT > LE > prosecutor (> judge). That means that normally the CSIRT informs LE and then LE informs the prosecutor.

However, under certain circumstances (namely for emergency cases) the CSIRT has a direct channel (email, phone) to the prosecutor e.g. when LE is not available, the CSIRT can report a crime directly to the prosecutor. In addition, the prosecutor can directly request the CSIRT for instance to explain to the prosecutor a specific technical point which will inform the next stages of the investigation. In this situation, the prosecutor can directly engage with the CSIRT, but the LE might still act as a facilitator.

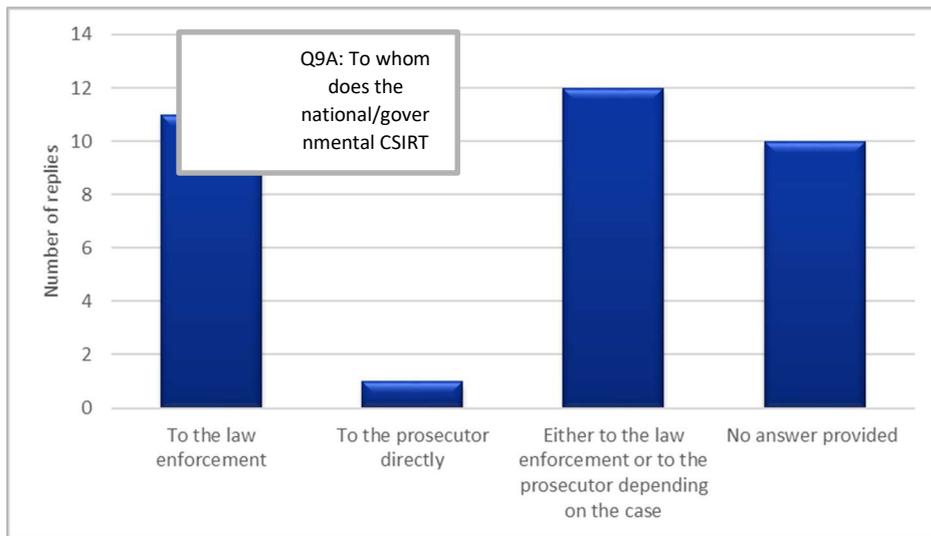
Some interviewees stated that there are also formal and informal ways of communication and that sometimes official requests for information (e.g. from CSIRT to LE or from LE to CSIRTs) are preceded by some informal discussion between CSIRT and LE personnel working on the incident/case.

CSIRTs (like any witness) can be requested to provide testimony during a trial. Either the prosecutor or the defence can summon CSIRT personnel who provided evidence. In this case, the CSIRT personnel are normally in the same situation as the private expert when giving testimony. As expert witnesses, CSIRTs personnel have to outline their skills and knowledge and explain to the court how the evidence was handled. The defence might aim to challenge not the evidence as such but how that evidence was collected and handled (e.g. searched for, collected and preserved). It must be noted that while LE personnel are generally prepared to testify in Court, CSIRT personnel may be reluctant or ill-prepared to serve as expert witnesses in Court as they might be less familiar with trial sessions.

To summarise, CSIRTs normally interact with the judiciary via LE and do not have direct interaction with prosecutors: they have even less frequent direct interaction with judges. There are however cases where CSIRT and prosecutors and judges have direct contact, for instance when the CSIRT is asked to provide technical input directly to the prosecutor on a case or where the CSIRT is asked to testify in court. Nonetheless, the contact is normally facilitated by the LE, especially in the case of interaction between the CSIRT and the prosecutor.

According to the data collected both via the interviews and the online survey, where the CSIRTs have a duty to report cybercrime (whether CSIRTs have this duty is discussed below in the report), normally the CSIRT report to LE although there are cases (depending on the legal systems) where they report it directly to the prosecutor. The results from the online survey on this matter are represented in Figure 7.

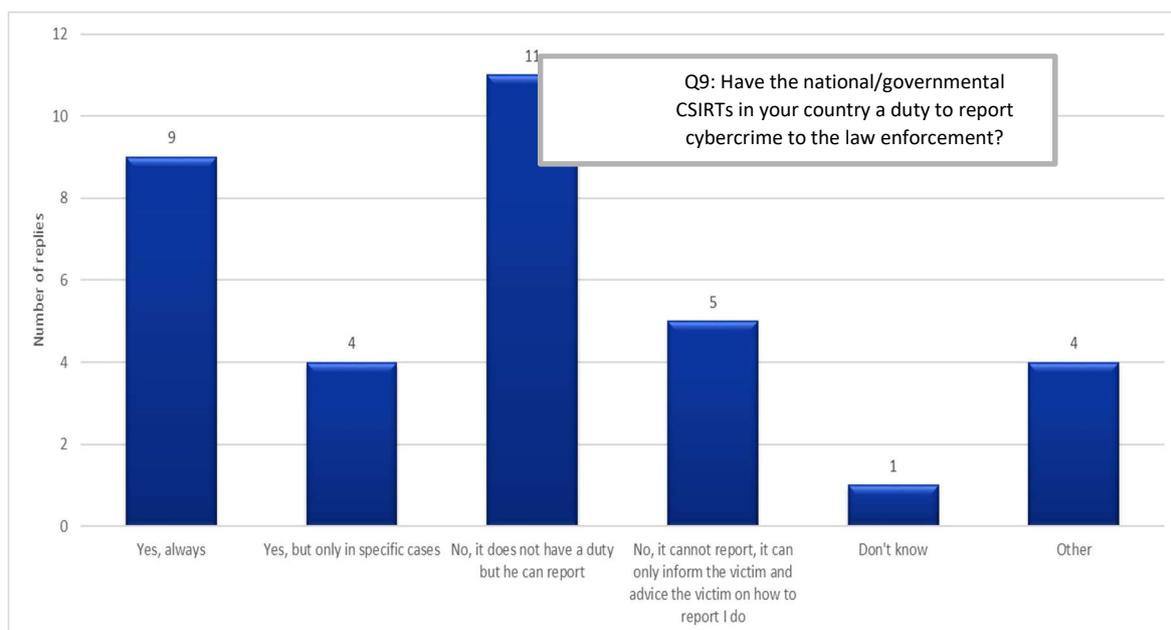
Figure 7 — Replies to question 9A of the online survey conducted for this report



3.4.2 CSIRTs and their duty (or not) to inform law enforcement or prosecutor and/or to report a crime and the coordination of actions

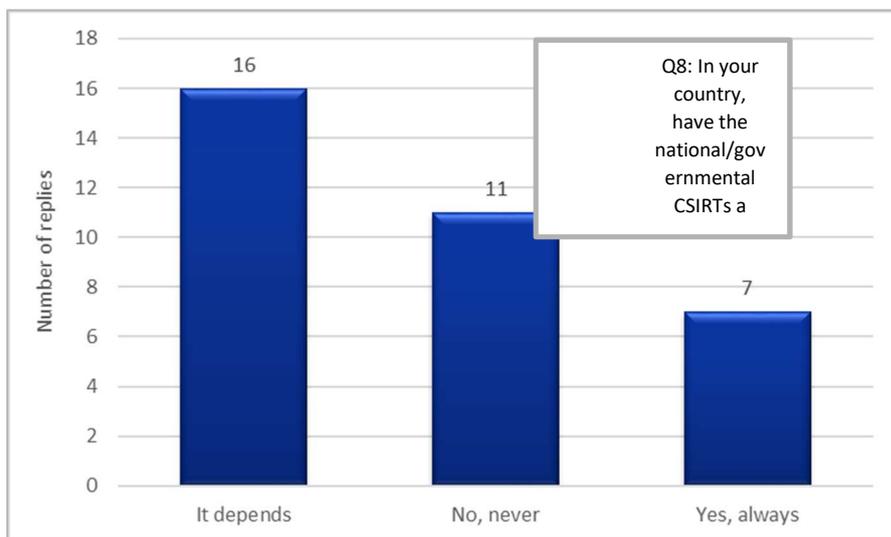
From data collected via interviews it emerged that whether a national/governmental CSIRT has a duty to inform or report to the LE or to the prosecutor varies considerably from country to country. However, even considering this differentiating factor, it seems that there is a lack of common understanding on when CSIRTs have a duty to report an alleged criminal act: the data collected appears indeed rather heterogeneous. It may also be the case that CSIRTs require continuous support and legal guidance to be better able to determine when an incident can be considered a crime.

Figure 8 — Replies to question 9 of the online survey conducted for this report



Concerning the duty of the CSIRTs to inform the victims, as shown in Figure 9, according to most respondents to the online survey, CSIRTs have this duty only under certain circumstances (not much more additional data were gathered on such circumstances).

Figure 9 — Replies to question 8 of the online survey conducted for this report



However, whether or not CSIRTs have a duty to inform LE (or the prosecutor) and/or the victim, one of the most important aspects to consider is the coordination process between CSIRTs, LE and the prosecutor.

As mentioned, CSIRTs are more focused on preventing and reacting to cyber incidents, but some CSIRT actions may affect criminal investigations (in most countries conducted by the police and coordinated/supervised by the prosecution service). An example is the case when a CSIRT might notify a web domain owner or the host about a command and control server and request shut down. But at the same time that command and control server might be under investigation by an LE. That is why the coordination and escalation process between different entities must be in place and clear to all parties (CSIRTs, LE and the judiciary).

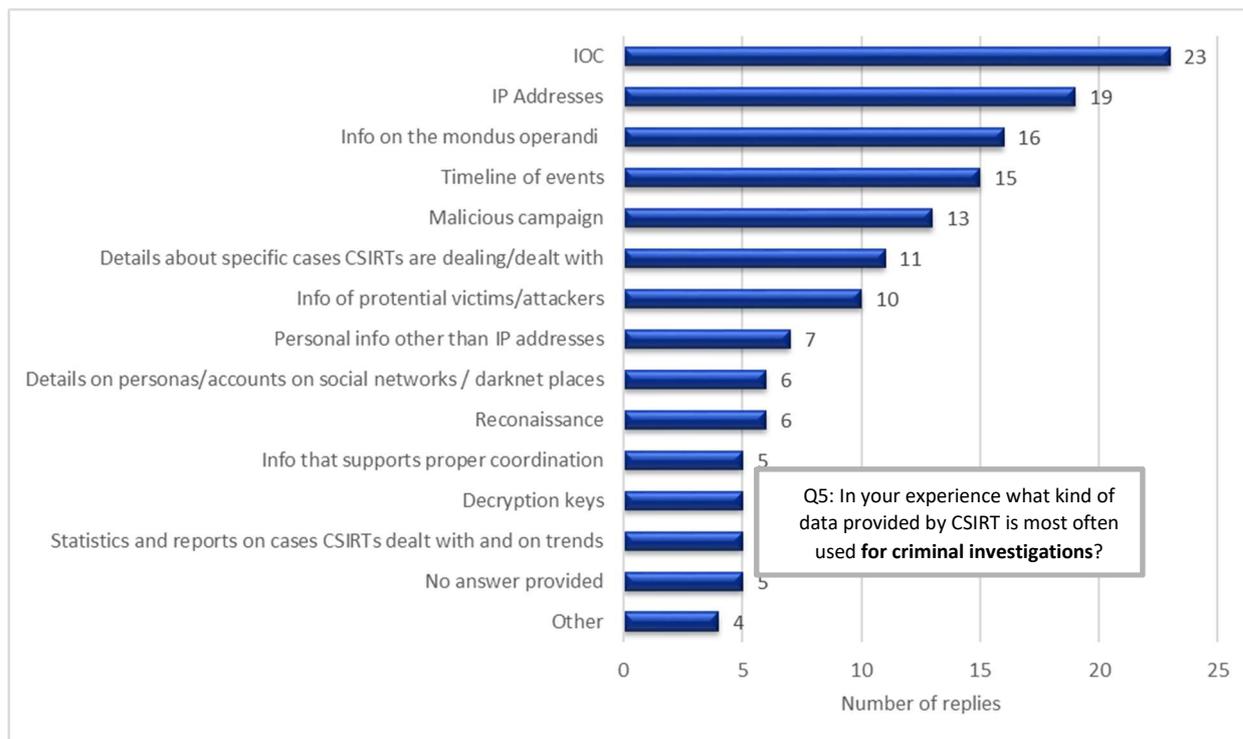
Proper coordination in the cyber field does require proper mechanisms and tools, including the usage of a dedicated platform where different types of data can be properly marked (e.g. a specific domain is sinkholed ⁽¹⁵⁾ and cannot be the subject of a takedown). However, it must be noted that CSIRTs and LE are already using their own platforms for information storing, processing and exchange (e.g. the ‘MeliCERTes facility [in the CSIRT community that] aims to facilitate swift and effective operational cooperation for the CSIRT network’ (European Commission, 2017b). A new platform might lead to the duplication of efforts.

⁽¹⁵⁾ ‘DNS sinkholing is a mechanism aimed at protecting users by intercepting DNS request attempting to connect to known malicious or unwanted domains and returning a false, or rather controlled IP address. The controlled IP address points to a sinkhole server defined by the DNS sinkhole administrator.’ (<https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/dns-sinkhole>).

3.4.3 The kind of information exchanged and the related information flow

According to the results from the online survey shown in Figure 10 as well as those from the subject-matter expert interviews, the CSIRT-provided data most often used for criminal investigations are indicators of compromise (IOCs), IP addresses, information on *modus operandi* and timeline.

Figure 10 — Replies to question 5 of the online survey conducted for this report



Also, according to several subject-matter experts interviewed, the CSIRTs normally share with the police and (whether directly or via the police) with the prosecutor any type of information that is related to the incident and that might be relevant for the investigation. This information includes IP addresses, web domains, email details (addresses, headers, content) and IOCs.

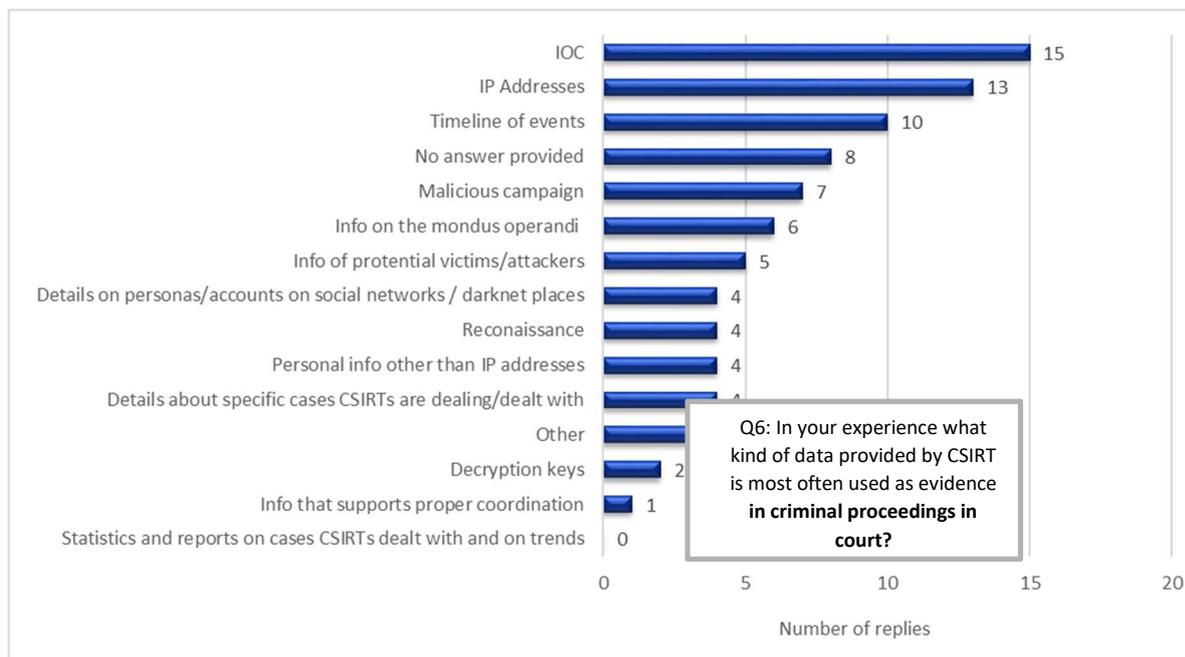
LE shares mainly IP addresses with CSIRTs, while sharing all information needed to decide on criminal prosecution with the prosecutors and judges. The judges share with judges all (digital) evidence useful to prosecute the suspect. Digital evidence sharing between judges belonging to different Member States can be either direct or indirect. This depends on what is provided for in bilateral or multilateral agreements between the states, if they exist, and on the cooperation in criminal matters that can be used in the specific case.

Almost any kind of data might be relevant and thus can be exchanged between CSIRTs and LEAs. They are still using the comma separated value (csv) format which can be converted into any human- or machine-processable format of events.

Similar replies were given in the online survey to the question on what kind of CSIRT-provided data are most often used as evidence in criminal proceedings in court. However, the number of 'no answer

provided' received in response to this question was higher; this might be since the respondents (especially from the CSIRT community) have less visibility on the actual use of the information they provide in court.

Figure 11 — Replies to question 6 of the online survey conducted for this report



3.4.4 Frequency of the information exchange and of the usage of information provided by CSIRTs in criminal investigations and as evidence in criminal proceedings

Several interviewees noted that the information sharing between CSIRTs and LE may be very frequent (on a daily basis or more than once a day), but it depends on the incident and on the severity of the incident. Some other interviewees stated that the information sharing is much less frequent, e.g. once per month.

In principle information sharing takes place immediately where there is an emergency and around once a week for minor incidents (as some interviewees highlighted, it not possible to send information immediately for minor incidents and therefore a list of minor incidents is sent to LE or to the prosecution office (depending on the country) e.g. once per week).

CSIRTs share information with LE also for intelligence purposes and there are regular bulletins (e.g. once per month) sent.

Some interviewees noted that when there is an emergency (and LE is not available), the national/governmental CSIRT has a direct channel to the prosecutor (e.g. phone). This provision, of course, does not undermine the 24/7 PoC service available in each MS.

On the usage of information provided by CSIRTs, it must be noted that according to the answers received via the online survey, most respondents replied that it is used occasionally for criminal investigation while rarely as evidence in criminal proceeding. See Figure 12.

Figure 12 — Replies to question 1 of the online survey conducted for this report

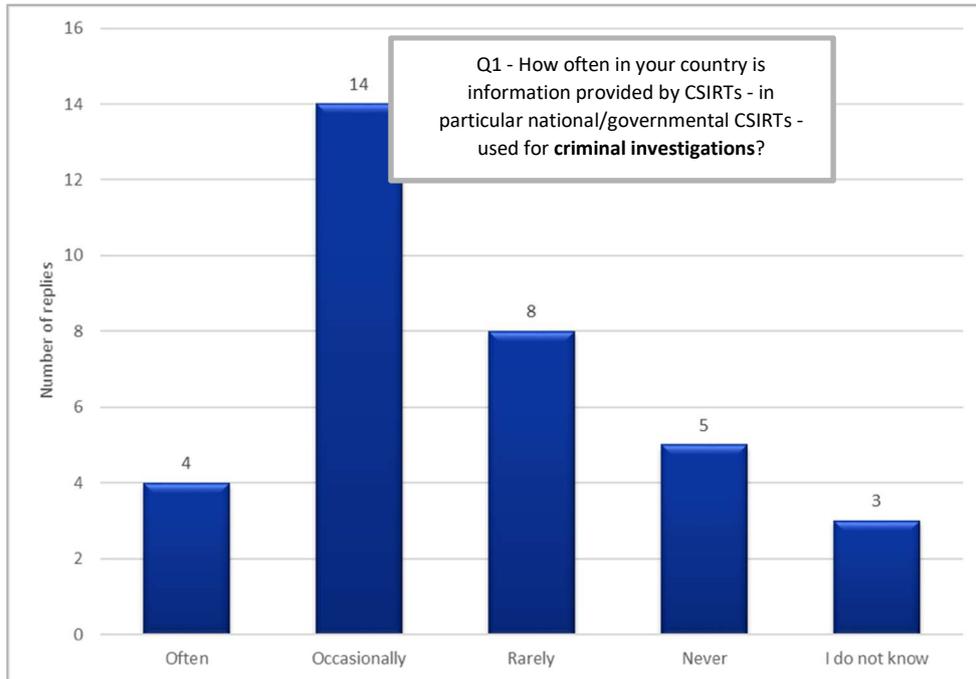
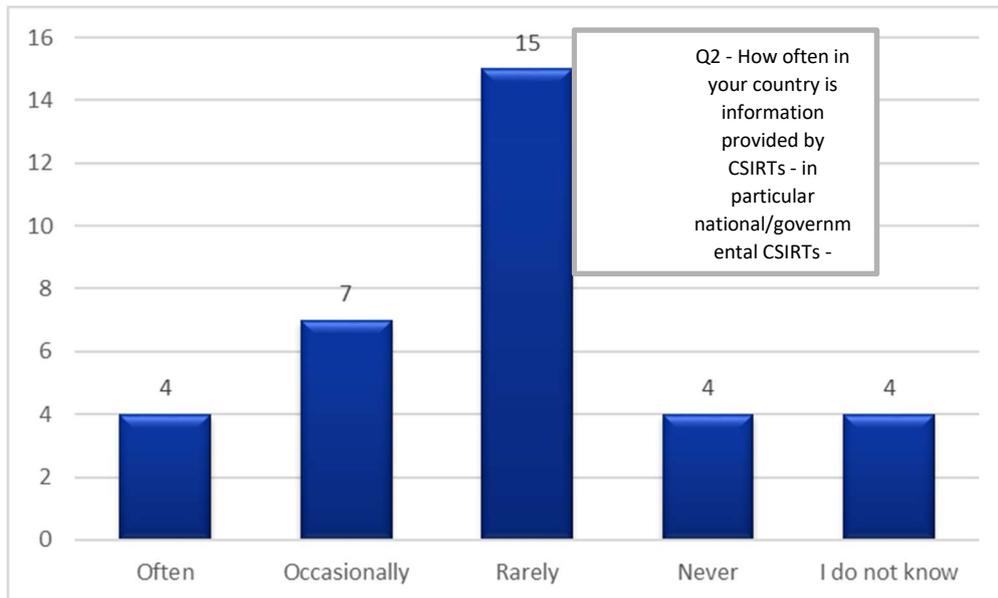


Figure 13 — Replies to question 2 of the online survey conducted for this report



Further, Figures 14 and 15 show that, according to the replies received from the online survey, CSIRTs are hardly ever called either to write detailed expert reports to use in criminal proceedings or to be witnesses in criminal courts.

Figure 14 — Replies to question 3 of the online survey conducted for this report

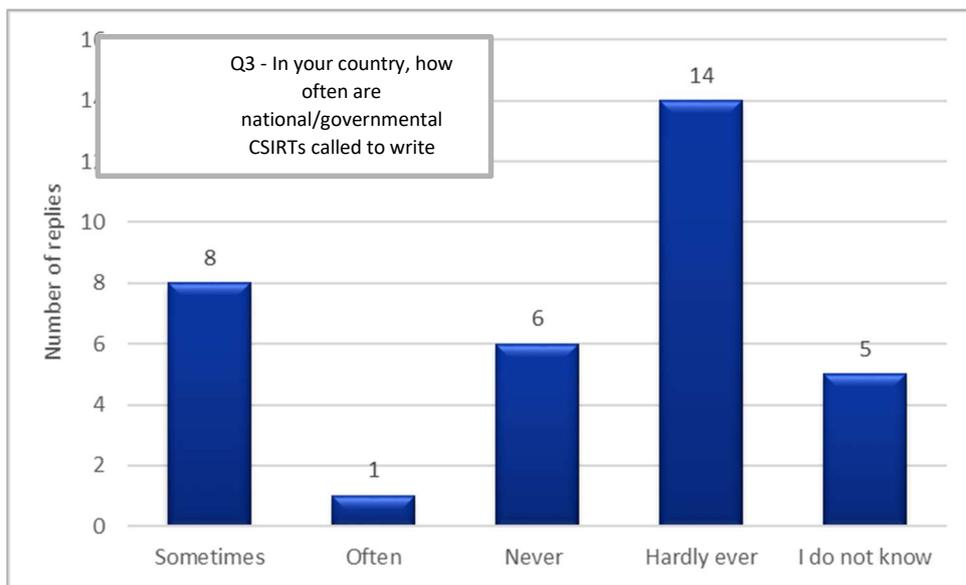
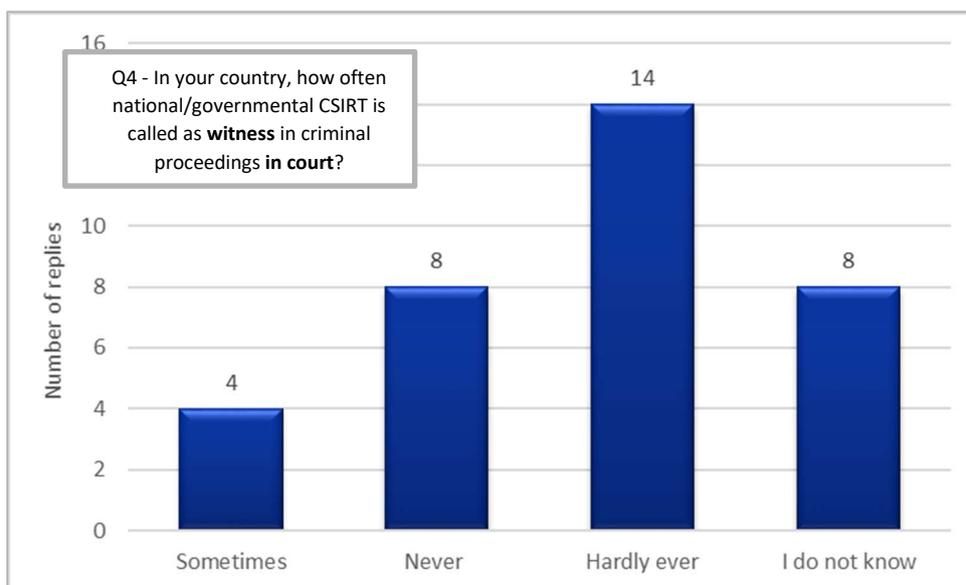


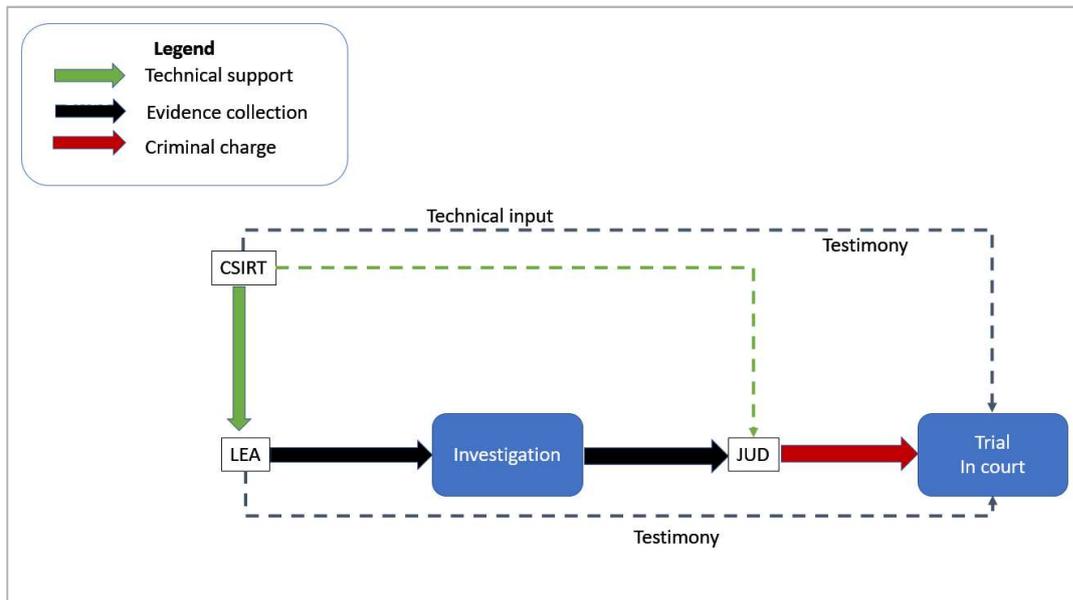
Figure 15 — Replies to question 4 of the online survey conducted for this report



3.4.5 A graphical representation of the information flow

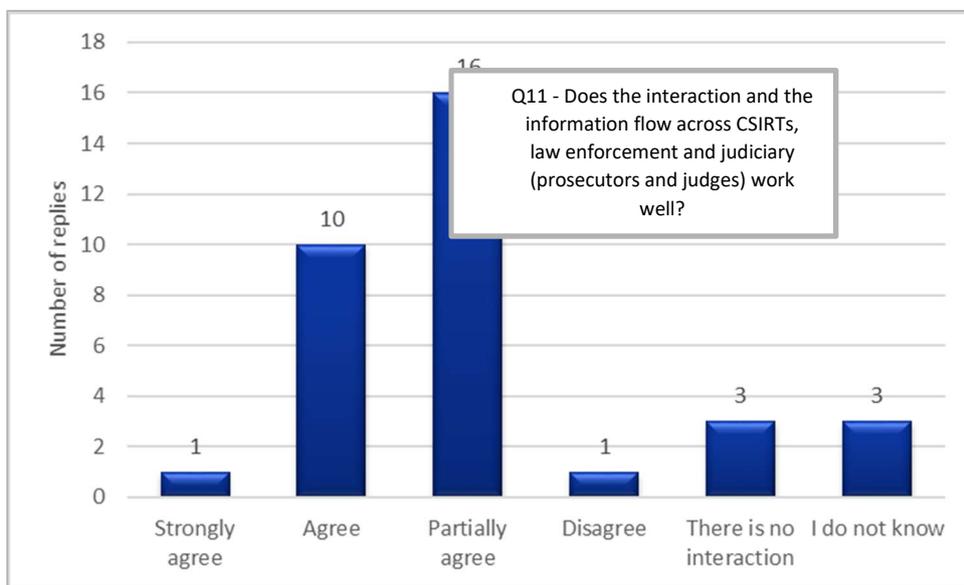
Although the information flow across CSIRTs, LE and judiciary varies from legal system to legal system it also depends on the specific case being dealt with (e.g. the severity of the case and whether it's considered an emergency might have an impact on the information flow), a graphical representation of this flow of information is presented in Figure 16 based on an abstraction and generalisation of the data collected for this report (especially the responses from the subject-matter expert interviews and the online survey). The broken lines in it represent information provided, as opposed to the arrows which represent actions taken. This graphical representation (with all the usual limitations due to abstraction and generalisation) aims to describe what the information flow might look like and shows the complexity of such information flow.

Figure 16 — Graphical representation of the flow of information across CSIRTs, LE and the judiciary



Responses to Question 11 on the online survey (see Figure 18), ‘agree’ or ‘partially agree’ on the interaction and the information flow across CSIRTs, LE and the judiciary working well. This gives a clear indication that when information is exchanged then the process does work but perhaps there is room for improvement.

Figure 17 — Replies to question 11 of the online survey conducted for this report



Some interviewees noted that the information flow is largely one-way (from CSIRTs to LEs/prosecutor) and this is mainly due to the prosecution and LE not being allowed to share information/evidence collected within the criminal proceedings (see Section 4.1.2 on the secrecy of criminal investigations in the report). The information flow from LE/prosecutor to CSIRTs takes place only to prevent further damage or in emergency situations. Other respondents highlighted that police can only officially share with the CSIRT a

specific portion of the information as a precautionary measure, i.e. all information not classified as 'secrecy'; clearly the public prosecutor that directs the investigation can order the sharing of additional pieces of information.

Other interviewees noted that the distribution of authority and formalities sometimes make the cooperation/interaction less smooth, but that this might also be so due to the need to comply with certain legal requirements.

What has also emerged from data collected is that cooperation and interaction depends on interpersonal relations: if the interpersonal relations are good, the cooperation/interaction works well. This finding further confirmed one of the findings of the 2017 ENISA reports on CSIRTs and law-enforcement cooperation (ENISA, 2017) (ENISA, 2017a), i.e. that trust is paramount for the cooperation among the three communities.

3.5 The tools and the common taxonomy for CSIRTs and law enforcement

This section provides a detailed overview of the tools and taxonomies used for data sharing.

3.5.1 Tools

This section gives an overview of the tools for normal communication and information sharing within the CSIRTs and within the LE community for cooperation between the two communities.

As mentioned above, the CSIRTs interact with the prosecutors generally via LE; they interact rarely with judges (only seldom they are called as expert witnesses in court). For this reason, the tools used by the prosecutors and judges for their internal communication and information sharing or for communication with the CSIRTs are not addressed in this report.

3.5.1.1 Overview of tools used within the CSIRTs community and within the law-enforcement community

Secure email is a common tool in the cybersecurity community and is used by LE to communicate and share information with other police forces and with independent or private-sector experts, as well as with CSIRT personnel. LE tends to use the pretty good privacy (PGP) cryptography system more and more, this allows LE to protect the data in exchanges with other police forces (also in international exchanges) in an easy manner. MS competent authorities (e.g. LE) also use other secured email systems to exchange non-structured data very quickly, e.g. the secure information exchange network application (SIENA), the Europol platform for experts (EPE) for non-operational exchange of information for Europol or the Interpol PoC for Interpol.

For more structured data the only family of tools comprises police files: the wanted or signalled person or objects stored in the national and EU databases. This tool seems to fit better to certain types of data, such as IOCs or other pure cybercrime data. The analysis projects, (previously called focal points ⁽¹⁶⁾) also are important tools: each piece of data is analysed stored in Europol databases to then be shared in order to identify common cases among several countries.

⁽¹⁶⁾ <https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects>

The malware information-sharing platform (MISP) platform is a widely used and well-established tool within the CSIRT community. The MISP's main use and its strong point is its sharing capability: a user of the platform can very easily share routine structured data with other entities through push and pull. MISP is increasingly becoming a standard among the CSIRT community in the EU and EFTA. A new trend in LE is to implement MISP (Computer Incident Response Center (CIRCL) Luxembourg, 2018). The MISP tool is also fit for storing IOCs and for sharing them in an automated and structured way. It is a good first place for LE to discover threat intelligence: the MISP instances automatically share the feeds at each update.

Within the LE community, in addition to MISP, the use of other new tools is increasing for cybercrime-oriented information sharing. Europol malwares analysis system (EMAS) for instance allows LE to share malware samples: each malware submitted is analysed. The IOC obtained are then crossmatched in Europol databases. The EPE is a portal full of information and tools. Among them can be found technical developments for IT forensic investigations, best practices or WHOIS legal considerations. It is one of the communication tools of Europol's EC3 with the LE community alongside EPE that allows private parties, LEA and others to exchange information. It uses secured connections and closed networks. Working with outside partners creates new habits and new systems such as interconnecting networks that were isolated before.

LE use investigation graph tools which crawl into any kind of dataset to make connections and provide a graphical representation of them. Some of the tools can be fed with any type of data, such as blockchain⁽¹⁷⁾, Structured Query Language (SQL) database (DB), in-house files and so on.

More generally, LE are entering into the threat-intelligence area with tools able to manage and crosscheck large datasets for further identification of perpetrators. It is usually based on the Elasticsearch framework⁽¹⁸⁾ with a lot of in-house programming to fit LE needs: graph visualisation, indexing of seized hacker forums, etc.

3.5.1.2 Overview of tools used for information sharing between the CSIRT and LE communities

Basic standard tooling such as secure email and telephone are used for communication and information sharing between CSIRTs and LE. As also highlighted in 2017 ENISA report on *Tools and methodologies to support cooperation between CSIRTs and law enforcement* (ENISA, 2017, p. 28), in 'several Member States there is an already established and secure (and sometimes segregated) government network that can be used for secure communication. These types of network could be used as a communication path for exchanging information'.

Since the use of MISP is already widespread in the CSIRT community and there is an ongoing increase in the use of MISP by LE, it seems to be or likely to be one of the most suitable tools for the exchange of information between CSIRTs and LE. 'It is important to note that a separate community (or even better a

⁽¹⁷⁾ Blockchain is a public ledger consisting of all transactions taken place across a peer-to-peer network. It is a data structure consisting of linked blocks of data, e.g. confirmed financial transactions with each block pointing/referring to the previous one forming a chain in linear and chronological order. This decentralised technology enables the participants of a peer-to-peer network to make transactions without the need of a trusted central authority and at the same time relying on cryptography to ensure the integrity of transactions. (<https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/blockchain>).

⁽¹⁸⁾ <https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html>

separate MISP instance) can be used for information exchange between CSIRT and LEA. This way, there is no risk for potentially disclosing sensitive information with parties that should not [have it]' (ENISA, 2017, p. 30).

Whenever needed, also face-to-face meetings, even in particularly secure locations if required, take place between CSIRTs and law enforcement.

3.5.2 Common taxonomy for CSIRTs and law enforcement

Although CSIRTs and LE might have their own taxonomy to deal with incidents/cybercrime, a common taxonomy for CSIRTs and LE enforcement has been developed to facilitate their cooperation. The 'common taxonomy for LE and CSIRTs, which was set up to simplify CSIRT and LEA cooperation. This taxonomy resulted from collaboration initiatives such as the annual ENISA/EC3 workshop which involved CSIRTs, LEAs, ENISA, and EC3' (ENISA, 2018). The common taxonomy for CSIRTs and LE has as an objective 'to support the CSIRTs and the public prosecutors in their dealing with LEAs in cases of criminal investigations, by providing a common taxonomy for the classification of incidents, named common taxonomy for law enforcement and the national network of CSIRTs' (Europol: European Cybercrime Centre and ENISA, 2017). This common taxonomy has been already implemented and imported in MISP (GitHub, n.d. a).

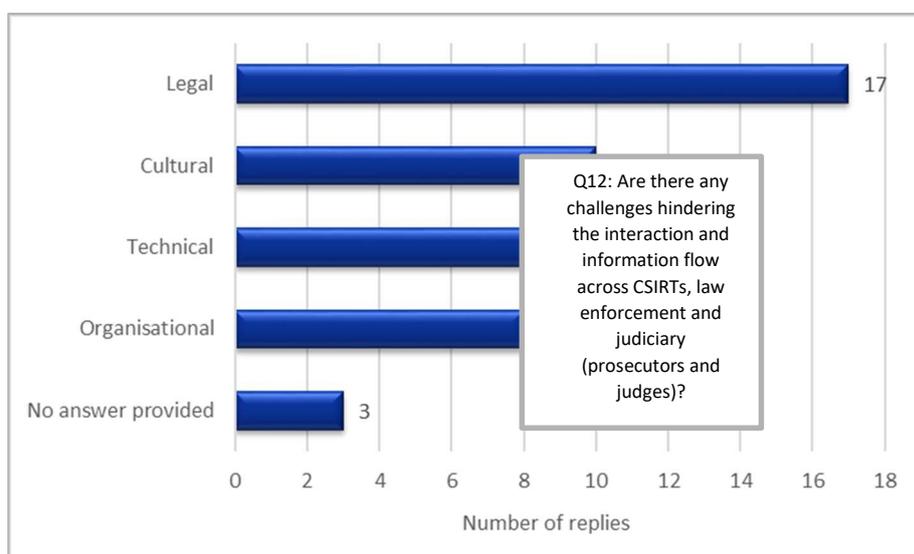
4. Challenges in cooperation and interaction

This chapter outlines the legal, cultural, technical and organisational challenges faced in the cooperation between CSIRTs and LEs and their interaction with the judiciary.

4.1 The challenges faced

According to the data collected for this report, there are challenges related to the cooperation between CSIRTs and LE (which is line also to the findings from 2017 ENISA reports (ENISA, 2017) (ENISA, 2017a), and their interaction with the judiciary. In particular, these challenges seem to be first legal, then cultural, technical and organisational. See Figure 18 which illustrates these findings.

Figure 18 — Replies to question 12 of the online survey conducted for this report



4.2 Legal challenges

This section presents some legal challenges faced in the cooperation between CSIRTs and LE and their interaction with the judiciary as identified from the data collected for this report.

4.2.1 Data retention

An important challenge is the need to find a balance between two opposing requirements. The first requirement is the investigative need to preserve the greatest amount of traffic data ⁽¹⁹⁾ for as long as possible. However, such data retention inevitably interferes with some fundamental rights, in particular

⁽¹⁹⁾ Article 1, letter d) of the Convention on Cybercrime (Council of Europe, 2001) states that ‘Traffic data’ ‘means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service’. These data, e.g. the IP address, can be very important in criminal investigations. For this reason, the legislation of many Member States requires that ‘traffic data’ be kept for a certain time for the purpose of the investigation, the detection and the prosecution of crime. This storage activity of ‘traffic data’ is called ‘data retention’.

the right to privacy and the right to erasure (or the right to be forgotten). Consequently, there is a second requirement, related to the principle that a level of government must not take any action that exceeds that necessary to carry out its assigned tasks ('proportionality'): the fundamental rights can be violated for investigative purposes without exceeding the limits of what is strictly necessary.

Finding a balance between these two needs is not easy. The no-longer-in-force Directive 2006/24/EC⁽²⁰⁾ (European Parliament and Council of the European Union, 2006) provided some rules on this topic. However, the judgment of the grand chamber in *Joined Case C-293/12 and C-594/12 Digital Rights Ireland Ltd v minister for communications, marine and natural resources and others and Kärntner Landesregierung and others* (Court of Justice of the European Union, 2014), of 8 April 2014 took the view that 'Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary' (see par. 65). Accordingly, the judgment of the grand chamber declared Directive 2006/24/EC invalid because of a violation of the principle of proportionality. For an overview of amendments to national data retention laws in 2016 after the *Digital Rights Ireland* judgment see (FRA). On case-law related to the concept of personal data, jurisprudence on IP addresses and data retention relevant for CSIRT and LE cooperation, see also the ENISA report *Improving cooperation between CSIRTs and law enforcement: Legal and organisational aspects* (ENISA, 2017a, pp. 30-31).

4.2.2 Secrecy of criminal investigations and the 'need to know'

Data exchange between CSIRTs and law enforcement represents a challenge in two ways: from CSIRT to LE and from LE to CSIRT.

For the information flow from LE to CSIRT, if the information originated from an investigation, the secret of the investigation applies, and law enforcement are not in a position to share the information they have with the CSIRTs. However, it must be noted that the prosecutor can exceptionally authorise a police officer to share and 'release' that person of this obligation to secrecy. In such cases, information sharing is then allowed, usually for impelling remediation motives or if it concerns information that is not sensitive for the investigation.

As emerged from the interviews, one of the most challenging aspects is the balance between the need to maintain the secrecy and the 'need to know': both CSIRTs and LE might work on the same incident/case and if there is no coordination they might interfere in a detrimental way in each other's work. In addition, for instance, if LE cannot share some information during the investigations, then it is difficult for the CSIRT to understand LE needs.

As far as it concerns the information flow from CSIRT to LE, it is important to consider how the LE can receive and use data from outside sources. Usually, data transferred by CSIRTs are for intelligence purposes. Should any of the data be used to identify and arrest a person, a stringent set of rules must be followed (see Section 4.1.6 — Chain of custody). Data collected to be used for judicial purposes must

⁽²⁰⁾ Directive concerned the retention of data generated or processed in connection with providing publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

follow evidence rules. The problem arises in this context when CSIRT information handling and transmission channels might not be well fitted to this situation.

4.2.3 Sharing of personal data, including IP addresses

One of the current challenges is to maintain and, where possible and needed, to increase the data sharing between CSIRTs and LEAs while remaining in line with the personal data legal framework provisions. Based on applicable legislation and the common interpretation, in principle IP addresses are considered personal data. Not only IP addresses but any online identifier that may be connected to natural persons (e.g. domain names, URLs, or email addresses) is personal data. In addition, sometimes the threat/incident data or intelligence may contain not only metadata but also content data.

It is therefore important to see to what extent IP addresses and other personal information related to the incident are allowed to be shared between CSIRTs and LEAs. On LEAs, it is clearly marked in Article 2 d) of the GDPR that there is no limitation, and in Recital 49, allows CSIRTs to process that information.

The Data Protection Law Enforcement Directive (Directive (EU) 2016/680) (European Parliament and Council of the European Union, 2016) is an important point of reference on the subject. It clarifies that when the processing of personal data by competent authorities is carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, consent by the owner of these personal data is not required. However, there might be other cases where the sharing of personal data between CSIRTs and LE takes place and the related data process (including the sharing) must have a different legal ground, which could be, for instance, the protection of public interest or the consent of the data owner.

4.2.3.1 An Introduction to the WHOIS registry/service

The Internet Corporation for Assigned Names and Numbers (ICANN) is 'a not-for-profit, public-benefit organisation' that operates 'the internet's domain name system [DNS], coordinates allocation and assignment of the internet's unique identifiers, such as internet protocol [IP] addresses, accredits generic top-level domain (gTLD) name registrars, and helps facilitate the voices of volunteers worldwide who are dedicated to keeping the internet secure, stable and interoperable' (ICANN, 2018a, p. 2).

WHOIS ⁽²¹⁾ is 'the system that asks the question, who is responsible for a domain name or an IP address?' (ICANN, 2018b) The WHOIS data may include 'name, address, email, phone number, and administrative

⁽²¹⁾ What is the domain WHOIS?

- Publicly available database of registration information on registrants of a domain name.
- Maintained by ICANN and its contracted registries and registrars.

What information?

- Domain names details:
- Domain name, IP address, Name server, creation/expiry date, domain status.

and technical contacts'. WHOIS is a query and response protocol with data stored in a decentralised way; in other words, 'the WHOIS service is not a single, centrally-operated database': the data are managed by independent entities known as 'registrars' and 'registries'. (ICANN, 2018c).

The registrar is 'An organisation that verifies availability and reserves domain names on behalf of a registrant. Domain names ending with .aero, .biz, .com, .coop, .info, .museum, .name, .net, .org, and .pro can be registered through many different companies (known as 'registrars') that compete with one another. A listing of these companies appears in the accredited registrar directory' (ICANN, 2018a). 'Any entity that wants to become a registrar must earn ICANN accreditation' (ICANN, 2018b).

The registry is an entity that 'keeps the master database and also generates the 'zone file' which allows computers to route Internet traffic to and from top-level domains anywhere in the world. Internet users do not interact directly with the registry operator; users can register names in top-level domains (TLDs) including .biz, .com, .info, .net, .name, .org by using an ICANN-accredited registrar' (ICANN, 2018a, p. 23)

4.2.4 Fundamental rights

CSIRTs and LE handle various types of data. 'All categories of data may be personal data', e.g. content data but also subscriber data; however, 'they have a different level of interference with fundamental rights' (European Commission, 2018c). Based on the data dealt with, appropriate conditions and safeguards apply to their collection and preservation and it is necessary to find a balance between the needs for collection and preservation of e-evidence and the protection of the fundamental rights of the suspect; this to guarantee the rights of third parties (including the victim) and also the rights of the suspect during the criminal investigations and the right of the accused to a fair trial.

It must be also noted that both LE and judiciary should request from CSIRTs only the information that is strictly necessary. This is also imposed by Article 52 of the Charter of Fundamental Rights of the European Union (European Parliament, Council and Commission, 2000), which provides that 'Any limitation on the exercise of the rights and freedoms recognised by this charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the [European] Union or the need to protect the rights and freedoms of others'. For an overview of case-law of the European Court of Human Rights in the area of human rights and criminal procedures see (McBride, 2018).

-
- Information on Registrar
 - Registrar's URL, registrar's abuse email, phone number.
 - Information on registrants (domain name holder)
 - Registrant email, postal address, fax and telephone number.
 - Administration contact and technical details

4.2.5 Chain of custody and evidence admissibility

Compliance with the chain of custody plays a fundamental role in the criminal trial, since it is not only the type of data that has been collected that is important, but also the fact that the data are stored with continuity according to certain technical rules (in addition to the guidelines mentioned in Section 3.1.4 — Admissibility of electronic evidence in criminal courts, see *Identification and handling of electronic evidence handbook, Document for teachers*, (ENISA, 2013b); *Digital forensics. Toolset, document for students* (ENISA, 2013a); *Mobile threats incident handling: Handbook, Document for teachers* (ENISA, 2014); *Methodologies for the identification of critical information infrastructure assets and services. Guidelines for charting electronic data communication networks* (ENISA, 2015d); *Forensic analysis. Webserver analysis handbook, Document for teachers* (ENISA, 2018); and *Exploring cloud incidents* (ENISA, 2016c)).

‘The chain of custody through appropriate policy frameworks can be used in order to assess the quality of the collected data. [...] Chain of custody investigations may also help in establishing the hierarchical structure that prevailed at the time that the acts under investigations were committed’ (Mitrakas & Zaich, 2009, p. 164 and 173). The chain of custody aims to guarantee that the data has not be tampered with between its creation and its usage in court. The main objective is to prove the data are directly connected to the suspect, so that the court can judge based on reliable evidence, this means evidence is collected in a manner that protects civil liberties. To avoid issues, evidence must be safeguarded at all times from the moment of the collection to the trial.

The chain of custody is relevant for the purpose of the admissibility of evidence, although how this admissibility is regulated and dealt with may vary from Member State to Member State and depend on the different kinds of data. For instance, in some Member States compliance with the chain of custody in the case of flow metadata is only important for the evaluation of evidence, however in the case of content data to be used for forensic examination compliance with the chain of custody is relevant for the admissibility of evidence (Home Office, 2014). It should be noted that, in the latter case, there is usually no specific rule of inadmissibility for the violation of the chain of custody. The inadmissibility of the evidence derives from the fact that the violation of the chain of custody can be traced back to one of the general causes of inadmissibility of the evidence provided by the rules of a state.

4.2.6 Diversity of legal frameworks between Member States and the timing of the investigative cooperation between Member States

In cross-border cases, the investigative cooperation between the different Member States is characterised by some challenges due to the variety of legal system and legal provisions. In addition, the instruments made available for such cooperation might not yet be sufficient to respond in a timely way to a request for a prompt collection of the e-evidence that, as mentioned, is volatile and by nature easy to manipulate and destroy. There is also the European Investigation Order (Directive 2014/41/EU), which can be issued by any Member State: the receiving Member State is required to execute the order. It can also be used for the collection of electronic evidence. There is also a proposal for the regulation on European production and preservation orders for electronic evidence in criminal matters, which would allow any Member State judiciary to request e-evidence directly from service providers (electronic communication providers, providers of information society services and IP and domain registries).

4.3 Cultural challenges

From the online survey and from the interviews conducted for this report it emerged that cultural challenges also impact the cooperation between CSIRTs and LE and their interaction with the judiciary. Some interviewees affirmed for instance that the main difficulty is to make some judiciary personnel understand the technical language of the CSIRT and to make the CSIRT understand the legal importance of some technical aspects. It seems that the three communities have different approaches to problems and *modus operandi* and they speak different 'languages': CSIRTs have a technical approach to problems, while judiciaries have a legal approach. The LEAs have to relate with these two different mentalities and languages and 'mediate'. Other interviewees highlighted that the cultural challenges related to how an organisation deals with other organisations; for instance, statements such as 'my job is more important than yours', 'you have to share because I am the authority' do not help the cooperation, while having a liaison officer (even better with a physical desk available in the other organisation) helps a great deal.

Also, the level and focus of training vary and the opportunities for CSIRT-LE-judiciary joint training are limited. Nevertheless, training provides insights to other disciplines that might be required in interdisciplinary environments, such as when there are interactions across technical and legal domains. Building on the development of this capability can be seen as a suitable approach (ENISA, 2018, p. 26).

An ENISA report on *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity* is currently under preparation and expected to be published on the ENISA website by end of 2018 or beginning of 2019.

4.4 Technical challenges

Some technical challenges faced in the cooperation between CSIRTs and LE and their interaction with the judiciary are discussed below.

4.4.1 Validation of the digital forensic tools

Digital forensics encompasses tools and techniques aiming to recover any element of data on a device, whether it has been deleted or not. Digital forensics was introduced in police investigation with the advent of the digitalisation of enterprises in financial cases to recover deleted evidence such as accounting documents and data. It is a specialised field that not all IT personnel might be familiar with (IT staff are not always familiar with the requirements on acquiring the evidence). Digital forensics is mainly linked with the system and network fields at a very basic level: the inner structure of a hard-drive or the artefacts left by network operation in the core of the operating system or live physical memory.

The tools and methodologies that digital forensic experts use need to be validated. The forensic tools fall under national standards in order to produce evidence that is likely to be admissible in court, such a standard was developed by NIST and was the first to be designed, using a testing protocol for hardware and software (NIST, 2018). The philosophy behind the validation of a tool belongs to the scientific experimentation field. To be validated, a tool must provide results that are repeatable and reproducible. 'Repeatable' means using the same method(s), on the same item(s), using the same equipment, by the same operator, within a short interval of time, *must* lead to the same results. 'Reproducible' means that using the same method, on the same items, in a different laboratory, by a different operator, utilising different equipment, *must* lead to the same results. An indicative example is the Cyber Observable

eXpression (CybOX™) ⁽²²⁾ that has helped with standardising, storing and sharing digital forensic information; CybOX™ represents objects and relationships that are common in forensic investigations.

No international standard is currently in place and each country has discretion as to what is admissible in court and what is not. What is at stake for the Member States is to have evidence admissibility in computer forensics, therefore a validation system for forensic methods and tools that are adapted to the each legal framework is needed.

4.4.2 Different technical maturity levels across different communities

As of today, the level of technical maturity differs from country to country and across the judiciary. For resource reasons, some LEAs might still lack the automation level that would allow for information to be processed and exchanged more efficiently. LE and the judiciary are gradually engaging in digitalising their processes and bringing them to a higher level of technical expertise.

4.4.3 Lack of common tools, tools for automated or semi-automated transfer of the data, and coordination tools

Arguably the most important challenge is the cybersecurity aspect: LE IT networks tend to be isolated ones. This is due to the critical nature of the information stored in the LE system. To avoid taking too many risks, LE IT management tend to choose to have very limited channels with the outside network. LE use isolated networks that simply prevent them sharing information with the outside world due to technical restrictions (proxy, lack of open IPs). This however makes information exchange, from a technical point of view, very difficult.

While the need for information sharing between the CSIRT and LE communities has started to be addressed by tools such as MISP, there is no one tool in place, other than email, to help the coordination between the two when dealing with a case (LEAs) or an incident (CSIRTs). For example, a structured data and automation inducing tool could be used by LE to mark specific resources (IP addresses, web domains, etc.) as being under investigation and therefore CSIRTs would know to avoid interference with those resources in the incident-resolution phase.

4.4.4 Taxonomy-related challenges

It must be noted that 'creating' a taxonomy is not a simple task. When dealing with topics such as security incidents, there can be different ways in which to classify them, and it is not always easy or possible to determine which is the best or the most correct classification. Organisations defining taxonomies are usually driven by different needs, and since different CSIRTs have different expectations, teams often end up developing their own incident classifications for internal use. In fact, the common taxonomy for LE and CSIRTs is itself an adaptation of the Portuguese National Cybersecurity Centre's CERT.PT (CERT.PT, 2018) taxonomy, which is itself an adaptation of the European CSIRT Network eCSIRT.net movie taxonomy (Stikvoort, 2012). One main advantage of the common taxonomy for LE and CSIRTs for its use in the context of cybercrime is that it has been extended to include the mapping of the incident classifications with a legal framework. Similarly, there have been a number of taxonomies that are in essence a branch or

⁽²²⁾ Cyber Observable eXpression (CybOX): <https://cybox.mitre.org/>

modification of another (GitHub, n.d. a) (ENISA, 2018). With the goal of reaching a consensus on a reference security incident classification taxonomy, 'ENISA and the European computer security incident response team (CSIRT) community have jointly set up a task force' (GitHub, n.d.). Taxonomies are generally seen by national CSIRTs, LE and competent authorities as the most suitable way to deal with cybercrime classification matters; this view has also been supported by an ENISA study ⁽²³⁾.

LE and prosecutors need to associate the incidents with the provisions and typology of crimes in their legal framework. It is essential for them to assess whether a fact (e.g. a cyber incident) can be qualified as a crime. The judicial system normally does not use any taxonomy: at this stage, the event will have to fit into the criminal code provisions. Choices will be made on a legal basis and investigation strategy. It is essential for CSIRT personnel to be trained to identify cyber incidents that qualify as a crime and have the ability and be duly authorised to report to the judiciary and/or LE in view of a potential investigation. A common taxonomy can become purposeful in this regard as it is relatively easy to understand by CSIRTs (because they can just look at the incident from a technical standpoint) while allowing LE and the prosecutors and judges to make the appropriate associations with the provisions in the criminal code.

Some CSIRTs have developed a taxonomy which connects categories of incidents to the offences in the criminal code and that help and support the interaction across the three communities. Indeed, such taxonomies propose a way of handling each incident, specify the evidence that may be relevant and therefore should be preserved by the CSIRT and provide additional information about procedural measures that can be used by LE and judiciary to request and obtain relevant evidence. Also the common taxonomy for law enforcement ⁽²¹⁾ is linked with the main international and European legislations: 'any incident categorised in this taxonomy can be matched to the relevant and appropriate legislative framework and subsequently mapped to relevant national legislation' (Europol: European Cybercrime Centre and ENISA, 2017, p. 5).

A common taxonomy has added a lot in efficiency and to the extent that it also covers internal processes of CSIRTs, LEAs and the judiciary, all parties could better familiarise themselves with the language used by the other collaborating communities. This is likely to increase the rate of adoption across all communities.

4.5 Organisational challenges

Some organisational challenges faced in the cooperation between CSIRTs and LE and their interaction with the judiciary are presented here as identified according to the data collected for this report

4.5.1 Need for reciprocal understanding of the structures, roles and strengths

CSIRTs, LE and judiciary have different structures and roles. If CSIRTs have a light hierarchical system based on operational matters, LE and judiciary organisations in comparison are much more hierarchical.

Although with some simplification we can say that; the CSIRT role is to mitigate an incident and get the system back on track, the LE role is to find who committed the crime and collect the evidence, the

⁽²³⁾ Common taxonomy for law enforcement and the national network of CSIRTs: <https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts>

prosecutor role is to coordinate the investigations and bring the suspect to court if there are the conditions for it, the judge role is to decide on whether the accused has committed the crime and the sanction based on the evidence provided.

Different structures and different roles might create some friction between those involved: LE might want to wait and collect as much evidence as possible when the CSIRT might want to clean the system as quickly as possible and get it back up and running. CSIRTs might want quick responses, while LE and the judiciary need to be in a position to take certain formal steps to provide a response and comply with certain legal requirements whose fulfilment might take some time.

What could also help enhance the cooperation and the interaction is a reciprocal understanding of strengths. There is therefore a need for a reciprocal understanding across the CSIRT, LE and the judiciary communities. This is a necessary element for a better cooperating and interaction.

4.5.2 Digital forensics expertise and the digital forensics training

‘The exponential growth of digital traces, as well as the expansion of cybercrime, and digitisation of investigative methods represent significant changes to society and lead to a broadening horizon of digital investigation (Casey E. , 2017)’ (Henseler & van Loenhout, 2018, p. 78).

The digital forensics activities require expertise in: ‘data collection, data examination and data analysis. Data collection involves the correct preservation and copying of digital data sources. Data examination relates to the investigation of copies of digital data sources to find files, fragments etc. without interpreting the resultant findings in the context of the case. Data analysis involves the analysis, reconstruction, interpretation and qualification of the evidence which is obtained from the digital data sources’ (Henseler & van Loenhout, 2018). There are, of course, police officer specialists in digital forensic investigations who are trained⁽²⁴⁾ and well-prepared to conduct digital investigations. However, since there are multiple areas that need to be covered in digital investigations it is unlikely that all of those areas are known to a single expert or to a team of experts: Windows forensics, Linux/Unix forensics, OS X forensics, mobile forensics, virtualisation/containerisation etc. While police forces cooperate and exchange expertise, in some cases there is a need to request some expert external support. CSIRTs are sometime therefore called to provide this technical expertise on some specific cases.

Although the use of concepts of (factual) witnesses, expert witnesses and forensic experts in different legal cultures vary. For the purpose of this study, we can understand a factual witness as an individual who knows specific facts about the case that could be important for the purpose of the criminal investigation. So, a factual witness could be a CSIRT member who knows what happened in the CSIRT constituency. An expert witness, on the other hand, is a specialist on a particular body of knowledge, who can provide valuable expert information to LE and the judiciary. So, the expert witness could be, for example, a member of a CSIRT who knows nothing about the case at hand, but can explain to the investigator, prosecutor or the court what specific digital evidence proves or does not prove. From the perspective of the procedural criminal law, the status of the factual witness and the expert witness is generally no different. The difference is in the nature and quality of the testimony provided.

⁽²⁴⁾ Police officer training might mix internal and external/private courses. Depending on the country and the recruitment policy, these courses can begin from scratch to train neophytes or be opened only to selected officers who already have a solid background in the subject.

Any specialist in a particular body of knowledge may become an expert who fulfils the established criteria and, depending on the country, gets enrolled in the official register of forensic experts in given scientific fields. The nature of these criteria varies considerably across countries. In some jurisdictions, only the court decides whether or not the expert meets the criteria, in others the expert must be accredited or must hold a licence granted by an independent body, elsewhere the expert must be a member of a professional organisation. In any case, only forensic experts can provide expert opinions which serve as specific evidence in court. Expert opinions and their processing also have a much more formal character compared with expert witness testimonies, and the responsibility of the forensic expert for the quality of their opinion is higher and usually specifically legally regulated.

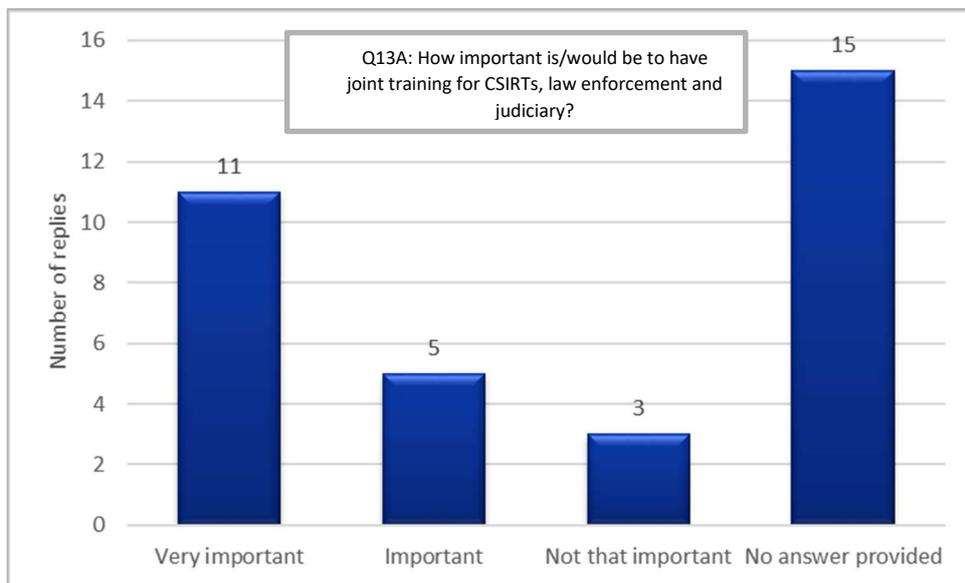
Experts need to be chosen based on their skills and experience. Depending on the legal system, different levels of verification of the expert's skills maybe needed. In some systems CSIRTs might need to be accredited and included in a specific register of digital forensics experts or a register of court experts to be in the position to provide support during criminal investigations and criminal proceedings (judges and/or the prosecutor may also appoint one or more digital forensics expert to evaluate some aspects of digital evidence). In addition, sometimes it seems that there is some confusion regarding the skills and the role of digital forensics: an engineer or a computer scientist is not always an expert in digital forensics.

The difference in education (mainly technical education for CSIRTs, mainly technical/legal education for LE and predominantly legal education for the judiciary) might represent a challenge in their communication and way of approaching the same matter. However, what might be seen as a challenge should also be seen as an enabling factor and an element of enrichment especially in the context of the expertise exchange and joint training.

In addition, the recent rise in cybercrime has shown the limits of the forensic training: cybercrime requires knowledge in almost all IT fields: systems, networks, programming, live memory, and electronics (the Internet of Things (IoT)). Digital forensics training for CSIRTs personal, LE and the judiciary needs to address these new challenges, but sometimes the resources available for training are not sufficient to respond to needs which are in constant development.

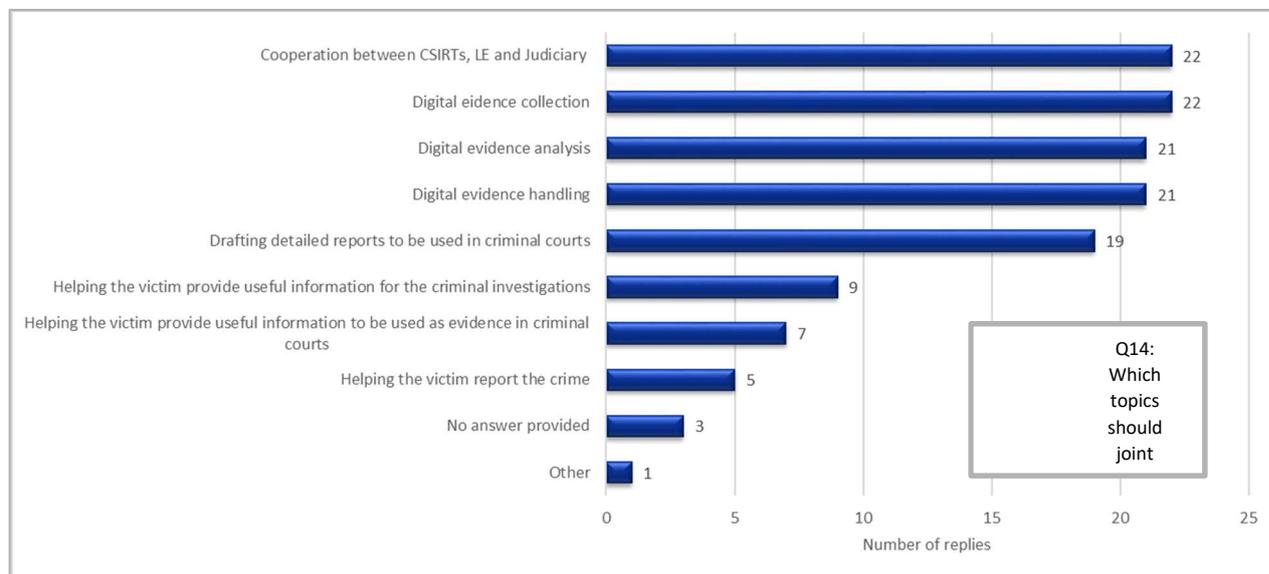
As emerged from the online survey, it seems that to have joint training for CSIRTs, LE and the judiciary is considered as important or very important.

Figure 19 — Replies to question 13A of the online survey conducted for this report



According to the data collected, the joint training should address *inter alia* cooperation between CSIRT, LE and the judiciary, digital collection, evidence analysis, digital evidence handling and the drafting of detailed reports to be used in criminal courts.

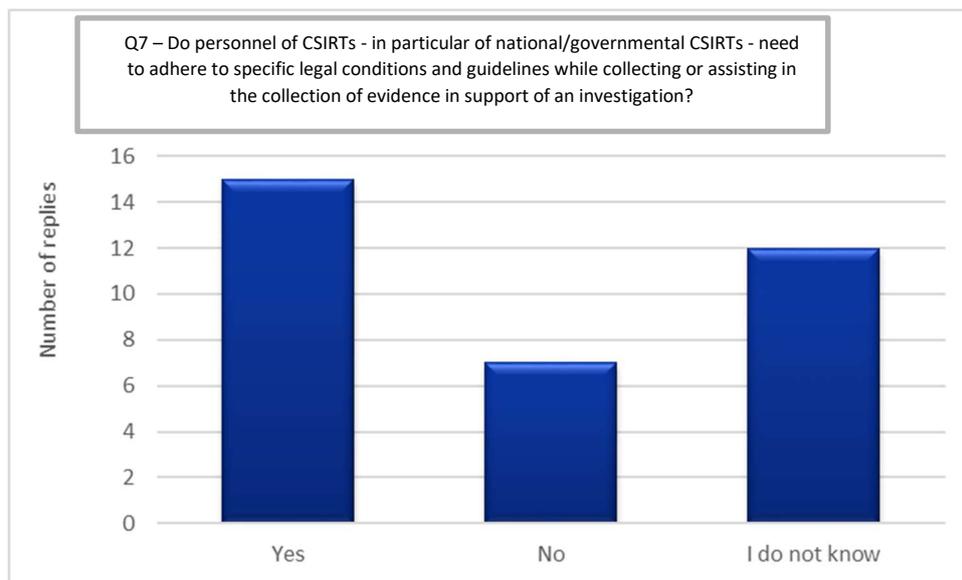
Figure 20 — Replies to question 14 of the online survey conducted for this report



It is important that the CSIRTs are adequately trained to also handle the kinds of information that are usually not useful for responding to an incident, but that could become e-evidence in a criminal trial.

The digital forensics experts, including CSIRTs when they are called to support criminal investigations (and evidence evaluation in criminal proceedings), must normally fulfil specific legal conditions and guidelines while collecting or assisting in the collection of evidence (see below).

Figure 21 - Replies to question 7 of the online survey conducted for this report



In some countries there are codes of practice from the forensic regulators that stipulate that all providers of digital forensics services to the criminal justice system must be accredited according to certain standards (on registration requirements for forensic experts see also: (Henseler & van Loenhout, 2018, p. 80). In some countries, the validation process however appears to be rather complicated. For instance, forensic experts may be required by law to demonstrate professional qualifications, but it might happen that there is no official body to set or examine these qualifications. The president of each court therefore decides what the necessary qualifications are for forensic experts, and so the quality of experts in each court may vary. Also, due to strict requirements on qualifications, in some countries, it might be complicated or even impossible for members of CSIRTs to become forensic experts. In these cases, the only way would be to call the member of the CSIRT as a witness instead of as a forensic expert.

The duties, powers and function of the forensic expert are often different from those of the witness. The differences vary from one Member State to another. For example, there may be cases of incapacity and incompatibility or even conditions of abstention or disqualification of witness when the requirements are different from those provided for the forensics expert.

Investigators must carry out investigations in full compliance with various legal guarantees. Some of them are also important in the context of CSIRT involvement. In particular, they are: the presumption of innocence (Council of Europe, n.d., p. 9), the impartiality in the conduct of investigations (on this topic, see for instance (OLAF Supervisory Committee, 2010), the reasonable duration for investigations, and the confidentiality of investigations.

From the online survey and from the interviews conducted for this report it emerged that cultural challenges also impact the cooperation between CSIRTs and LE and their interaction with the judiciary. Some interviewees affirmed for instance that the main difficulty is to make judiciary understand the technical language of the CSIRT and to make the CSIRT understand the legal importance of some technical

aspects. It seems that the three communities have different approaches to problems and modus operandi and they speak different 'languages'. Without resorting into generalisations, it could be simply stated that CSIRTs have a prevalent technical approach to problems, while the judiciary obviously have a strict legal approach. The LE have to relate with these two approaches and even languages used.

Also, the level and focus of training vary and the opportunities for CSIRT-LE-judiciary joint training are limited ⁽²⁵⁾.

⁽²⁵⁾ *Cybersecurity culture guidelines: Enhancing CSIRT/LEA community* (provisional title) is currently under preparation and expected to be published on the ENISA website by end of 2018 or beginning of 2019.

5. Conclusions and recommendations

5.1 Conclusions

Using the analysis of the results collected from the desk research, the interviews with subject-matter experts, and the online survey, the conclusions summarised below were drawn.

5.1.1 CSIRTs interact much more with LE than with the prosecutors and they interact very rarely with the judiciary

Usually, CSIRTs interact with LE that, in turn, interact with prosecutors. The CSIRT rarely interacts directly with prosecutors. Even more rarely the CSIRT interacts directly with judges. As a result, LE often act as a link between CSIRTs and judiciary. CSIRTs and LE mainly have technical training while the judiciary has legal training. LE also plays a fundamental role of link between subjects who have different training and use different languages.

5.1.2 CSIRTs support law enforcement (as well as prosecutor and judge) in a criminal investigation

The CSIRT technical background can provide a valuable support to criminal investigations, CSIRTs often have the tools and experience of incidents that allow them to quickly deal with these incidents more efficiently. In addition, CSIRTs can have data (e.g. IP addresses, web domains) that may be very important for the investigations. Therefore, the CSIRT support activity for LE and/or prosecutors can be fundamental to identify who committed or is going to commit a crime. Moreover, depending on the national legal system, the CSIRT personnel can sometimes play the role of forensic expert or witness during a criminal trial.

5.1.3 There are legal provisions on CSIRTs and LE cooperation and their interaction with the judiciary

The diversity of legal systems is likely to shape the cooperation between CSIRTs and LE as well as their interaction with the judiciary. However, the implementation of European Directives and the application of European regulations are helping to reduce these differences between states. Regardless of the differences between legal systems, the data collected via the interviews show that mutual trust is still a key factor for effective cooperation between CSIRTs and LE and for effective interaction with the judiciary.

5.1.4 The understanding of whether CSIRTs have to report to/inform LE and/or prosecutor of suspicious criminal activities could be improved

Depending on the Member State, the CSIRTs may be obliged or not obliged to report an event. In any case, CSIRTs usually report crimes to LE and only rarely to prosecutors. From the data collected it emerged that overall the understanding of whether CSIRTs have to report to/inform LE and/or prosecutor of suspicious criminal activities could be improved. However, it seems that the practical experience and good relations between CSIRTs and LE help CSIRTs comply with their legal obligations.

5.1.5 There is need for a more extensive usage of information from CSIRTs in criminal investigations and as evidence in court

As emerged from the desk research and from the interviews, CSIRTs can play an important role in fighting cybercrime; however, (at least as emerged from the results of the online survey) the frequency of usage of information from CSIRT for criminal investigations and proceeding is low. It seems therefore that the usage of the information that CSIRTs have and that might be key for responding to (cyber) crime could be extended at least in frequency.

5.1.6 There is need to collect data in order to support cooperation in a data driven approach

As emerged during the desk research, the data available at the moment in area of CSIRT, LE and judiciary cooperation are still quite limited. No evidence was found during the data collection for instance of the existence of a central repository of data associated with investigations that involve all three communities.

It is important to collect more data in order to support the cooperation and the decision-making processes at supranational and national level, but also at the level of the CSIRT, LE and judiciary teams involved in the cooperation. On evidence-based policymaking see (Commission on evidence-based policymaking, 2017).

Having central repositories of data associated with investigations that involve all three communities, if based on suitable metrics, could break new ground in the understanding of the interactions and priorities and possibly make the investigation and prosecution more effective.

5.1.7 Cultural limitations can be noted in the cooperation across the three communities and an interdisciplinary approach might help

Cultural differences across the three communities exist. If these cultural differences are factored in, the information flow is hindered, and the cooperation becomes more difficult. While a data driven approach is quite desirable, understanding the human and cultural aspects is important as well in order to gain appropriate insight (ENISA, 2016, p. 18).

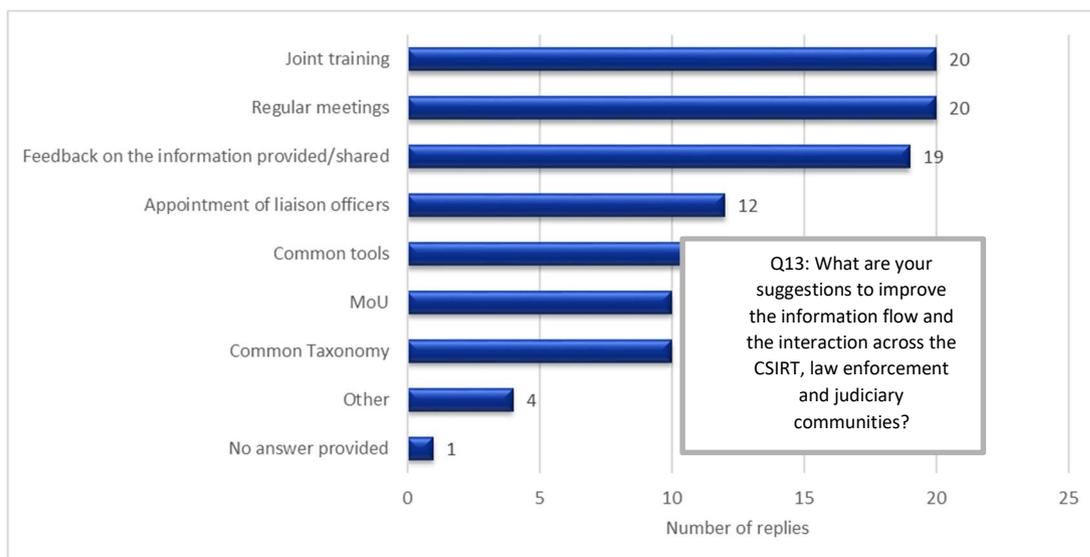
Sometimes the differences in culture are due to the fact that most of the members of the three communities (CSIRTs, LE and the judiciary) have different backgrounds. For this reason, an interdisciplinary approach that values all relevant fields of knowledge (namely legal and technical) is key to enhance cooperation this can also be addressed through training and experience building.

Sharing experiences and looking at the information flow from all three community perspectives helps understand potential, needs and priorities across the three communities.

5.2 Recommendations

According to the data collected via the online survey, joint training, regular meetings and feedback on the information provided/shared are suggested to be the best ways to improve the information flow and interaction across the three communities. See Figure 22.

Figure 22 — Replies to question 13 of the online survey conducted for this report



Some recommendations have been formulated based on the data collected for this report (see below).

5.2.1 Collect data on cooperation and interaction across CSIRT, LE and the judiciary

The data available on the cooperation and interaction across CSIRT, LE and judiciary communities are quite limited. Such data are key to enhancing the cooperation and interaction and to support related decision-making processes.

While the Member States, and in particular national/governmental CSIRTs, LE and judiciary, would collect the data at national level, ENISA, EC3 and Eurojust could support this data collection by suggesting data collection methodologies and methods, providing samples of questions and some common definitions of key concepts, proposing metrics, indexes and data report templates. Data collected at national level could be then aggregated by ENISA at EU/EFTA level.

Recommendations

- **National/governmental CSIRTs, LE and the judiciary:** to collect data on cooperation across the three communities.
- **ENISA, EC3 and Eurojust:** to support the data collection.
- **ENISA:** to aggregate at EU/EFTA level the data collected at national level.

5.2.2 Build on shared experience at strategic cooperation level

To have at national and EU/EFTA level, even possibly beyond, a common plan for the cooperation may help enhance the cooperation. Sharing experience at strategic cooperation can be a first step towards this.

Recommendations

- **National/governmental CSIRTs, national LE and the judiciary:** to share at national as well as at EU/EFTA level their experience at strategic cooperation.
- **ENISA, Europol EC3 and possibly Eurojust:** to facilitate, within the EU/EFTA and beyond, the sharing of experience at strategic cooperation across the three communities.

5.2.3 Invest in CSIRT/LE/judiciary joint training and skills development

Joint training across CSIRTs, LE and the judiciary would help share existing practices but would also allow the development of collaborative approaches for the future.

Good training plays a central role in improving the cooperation, including communication of CSIRTs, LE and the judiciary; joint training should therefore be facilitated.

There should be common understanding of legal and technical matters, including of the challenges faced by one or more than one of the three communities. An example of topics is provided in Annex D — Examples of topics for csirt/le/judiciary joint training.

There should be joint exercises based on real-life scenarios and hands-on sessions, where CSIRTs, LE and the judiciary can practice jointly fighting cybercrime in order to better know each other's objectives and needs, especially what type of information each of them needs to do their job. The joint training might be also an opportunity to further understand the potential that CSIRTs have (e.g. information, contacts, expertise) for the criminal investigations.

Organising training at a regional level (e.g. for countries with similar legal systems or with other commonalities) as well as engagement, for the joint training, with leading CSIRTs and national police forces beyond the EU could be considered.

It is important to develop the awareness that such training is necessary. Therefore, CSIRTs, LE and the judiciary should provide training to their personnel and joint training should not be perceived as occasional, but instead scheduled at regular intervals. In addition, it is important to ensure the quality of training through the involvement of highly qualified individuals and the use of suitable material (some freely accessible material is for instance available on the ENISA site (ENISA, n.d.c)).

Recommendations

- **National/governmental CSIRTs and national LE training centres:** to organise CSIRT-LE-judiciary joint training.
- **ENISA, Europol EC3, Eurojust and CEPOL:** to facilitate joint training at EU and EFTA national level for CSIRTs, LE and the judiciary and engage with leading CSIRTs and national police forces beyond the EU, as appropriate.
- **CSIRTs, LE and the judiciary:** to provide the training requirements to the facilitators of the joint training.

5.2.4 To reach a better mutual understanding of the other communities and develop memoranda of understanding to facilitate cooperation/interaction

Mutual understanding of roles, strengths but also of needs and limitations is key for the cooperation and interaction across the CSIRT, LE and judiciary communities.

Communication and regular meetings between the three communities help reach this mutual understanding. Also feedback on the information provided and shared or on how the requests for information have been formulated would help to further enhance the mutual understanding.

In order to support the three communities to reach a better understanding of each other duties assigned by the roles each community plays, a SoD matrix (see an example in Annex E — Example of segregation of

duties matrix) could be drafted at national level. The aim of this matrix is to highlight conflicting or overlapping duties performed by one community or more. As shown in the SoD template in Annex E, the CSIRTs, LE, judges and prosecutors have to identify the key responsibilities for their communities and then link them with the skills required to fulfil these duties. SoD matrices are usually used to ensure compliance with laws and regulations.

In some Member States there are memoranda between LE and CSIRTs and, in some cases, also between the three communities (CSIRT, LE and the judiciary). Based on these memoranda of understanding, for instance LE and the judiciary are immediately notified by CSIRTs of IT incidents (especially more severe ones) and can immediately coordinate their actions with the CSIRTs. This coordination activity reduces the risk that CSIRTs may erase significant data just because they are unaware that such data may be critical for the solution of a criminal case.

Developing memoranda of understanding might also help manage expectations in the cooperation/interaction and clarify the strengths, need for information sharing of the different communities and limitations they might have in sharing the information.

Recommendations

- **National/governmental CSIRTs, LE and possibly prosecutor services:** to work together towards a better mutual understanding of strengths, needs and limitations of the three communities (CSIRTs, LE and the judiciary) in relation to the sharing information, also by using SoD matrices.
- **National/governmental CSIRTs, LE and possibly prosecutor services:** to develop memoranda of understanding to facilitate their cooperation/interaction.

5.2.5 Place liaison officers

To establish liaison officers (e.g. national/governmental CSIRT personnel to LE and to prosecutor and vice versa) would be beneficial not only for trust-building knowledge but also for reaching a better reciprocal understanding of the three communities and for facilitating the information flow.

Also providing that they liaise within the other organisation(s) from an allocated physical space (an office that the liaison officer can use if needed) could help not only from the practical side but also to clearly affirm and recognise this role.

Recommendation

- **National/governmental CSIRTs, LE and possibly prosecutor services:** to appoint liaison officers to facilitate the cooperation and the interaction.

5.2.6 Use (common) tools to facilitate cooperation and interaction

CSIRTs, LEs and the judiciary use different types of tools and this is natural given the differences in the roles of these communities. One suggestion would be that the CSIRTs and LE (which could then feed the information to the prosecutors when needed) have access to a common platform where they can share information about threats and those involved in threats, cybersecurity incidents, cyber-attacks and associated tactics, techniques and procedures (TTPs).

CSIRTs are rarely called as witnesses in criminal proceedings; however, when this does occur, court information systems to support cybercrime trials by means of presenting digital evidence may help CSIRTs better fulfil their role.

Recommendations

- **National/governmental CSIRTs, LE and possibly prosecutor services:** to investigate the possibility of having a common platform to share information about threats and those involved in threats, cybersecurity incidents, cyber-attacks and associated TTPs.
- **National/governmental CSIRTs, LE and possibly prosecutor services:** to investigate how the tools they use can be further improved to better receive the information provided by other communities and to better formulate their requests for information addressed to the other communities.

6. Bibliography/references

- Admissibility of electronic evidence in court (AEEC) project. (2006). *The admissibility of electronic evidence in court: Fight against high-tech crime*. Retrieved August 3, 2018, from https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf
- Association of Chief Police Officers of England, Wales and Northern Ireland (ACPO). (2012, March). *ACPO good practice guide for digital evidence*. Retrieved July 31, 2018, from <http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf>
- Berniz, U. (n.d.). *What is Scandinavian Law? Concept, Characteristics, Future*. Retrieved from <http://www.scandinavianlaw.se/pdf/50-1.pdf>
- Bureau of Justice Statistics. (2018, August 20). *Terms & definitions: Law enforcement*. Retrieved from <https://www.bjs.gov/index.cfm?ty=tdtp&tid=7>
- Cambridge Dictionary. (n.d.). *Prosecutor*. Retrieved July 27, 2018, from <https://dictionary.cambridge.org/dictionary/english/prosecutor>
- Cambridge University Press. (n.d.). *Cambridge Dictionary*. Retrieved July 28, 2017, from <http://dictionary.cambridge.org/dictionary/english/practice>
- Casey, E. (2004). *Digital evidence and computer crime*.
- Casey, E. (2017). The value of forensic preparedness and digital-identification expertise in smart society. *Digital Investigation*. Retrieved August 3, 2018, from <https://www.sciencedirect.com/science/article/pii/S1742287617302815>
- CERT.PT. (2018, August 2). Retrieved from <https://www.cncs.gov.pt/en/>
- CERT-EU. (2012). *Incident response — Data acquisition guidelines for investigation purposes*. Retrieved July 31, 2018, from http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_04_Guideline_DataAcquisition_v1_4_4.pdf
- Commission on evidence-based policymaking. (2017, September). *The promise of evidence-based policymaking*. Retrieved August 27, 2018, from <https://www.cep.gov/content/dam/cep/report/cep-final-report.pdf>
- Computer Incident Response Center Luxembourg. (2018, August 20). *Malware information sharing platform MISP — A Threat Sharing Platform*. Retrieved from circl.lu: <http://circl.lu/services/misp-malware-information-sharing-platform/>
- Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*. Retrieved July 29, 2018, from <https://www.echr.coe.int/pages/home.aspx?p=basictexts>
- Council of Europe. (2001, November 2001). *Convention on Cybercrime*. Retrieved July 28, 2017, from <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>

- Council of Europe. (n.d.). *Budapest Convention and related standards*. Retrieved 28 July, from <http://www.coe.int/en/web/cybercrime/the-budapest-convention>
- Council of Europe. (n.d.). Retrieved from European Convention on Human Rights: https://www.echr.coe.int/Documents/Convention_ENG.pdf
- Council of the European Union. (2008, November 27). *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*. Retrieved July 31, 2017, from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF>
- Council of the European Union. (2016, June 9). *Council conclusions on the European Judicial Cybercrime Network*. Retrieved July 5, 2018, from <https://www.consilium.europa.eu/media/24301/network-en.pdf>
- Council of the European Union. (2017, October 2). *Final report of the seventh round of mutual evaluations on 'The practical implementation and operation of the European policies on prevention and combating cybercrime'*. Retrieved from <http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf>
- Council of the European Union. (2017b, March 13). *Joint paper Eurojust/Europol sent to delegations on common challenges in combating cybercrime*. Retrieved September 5, 2017, from <http://data.consilium.europa.eu/doc/document/ST-7021-2017-INIT/en/pdf>
- Court of Justice of the European Union. (n.d.). *The Court of Justice of the European Union*. Retrieved July 4, 2018, from https://curia.europa.eu/jcms/jcms/j_6/en/
- Delmas Marty, M., & Spencer, J. R. (2004). *European criminal procedures*. Retrieved July 4 2018, from <http://catdir.loc.gov/catdir/samples/cam041/2002073784.pdf>
- EFTA. (n.d.). *The EFTA states*. Retrieved September 05, 2017, from <http://www.efta.int/about-efta/the-efta-states>
- ENISA. (2009, December). *Baseline capabilities for national/governmental CERTs (Part 1 Operational Aspects)*. Retrieved September 30, 2017, from <https://www.enisa.europa.eu/publications/baseline-capabilities-for-national-governmental-certs>
- ENISA. (2010). *Good practice guide for incident management*. Retrieved July 29, 2018, from <https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management>
- ENISA. (2010). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*. Retrieved July 31, 2017, from <https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing>
- ENISA. (2013a, September). *Digital forensics toolset*. Retrieved from www.enisa.europa.eu: <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/digital-forensics-toolset/view>
- ENISA. (2013b, September). *Identification and handling of electronic evidence handbook*. Retrieved from www.enisa.europa.eu: <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/identification-and-handling-of-electronic-evidence-handbook/view>

- ENISA. (2014). *www.enisa.europa.eu*. Retrieved from Mobile threats incident handling: <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/Mobileincidenthandlinghandbook.pdf/view>
- ENISA. (2015a). *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. Retrieved July 06, 2017, from <https://www.enisa.europa.eu/publications/cybersecurity-information-sharing>
- ENISA. (2015b). *ENISA — CERT Inventory*. Retrieved 07 06, 2017, from <https://www.enisa.europa.eu/publications/inventory-of-cert-activities-in-europe>
- ENISA. (2015c). *CSIRT Capabilities. How to assess maturity?* Retrieved July 28, 2017, from <https://www.enisa.europa.eu/publications/csirt-capabilities>
- ENISA. (2015d). *Methodologies for the identification of critical information infrastructure assets and services*. Retrieved from www.enisa.europa.eu: <https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis>
- ENISA. (2016a). *A good practice guide of using taxonomies in incident prevention and detection*. Retrieved July 07, 2017, from <https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection>
- ENISA. (2016b). *Report on Cyber Security Information Sharing in the Energy Sector*. Retrieved July 06, 2017, from <https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector>
- ENISA. (2016c). *Exploring Cloud Incidents*. Retrieved from www.enisa.europa.eu: <https://www.enisa.europa.eu/publications/exploring-cloud-incidents>
- ENISA. (2016d). *Incident Handling Management — Handbook, Document for Teachers*. Retrieved August 24, 2018, from https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/incident_handling_management-handbook
- 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, November). *ENISA Programming Document 2018-2020*. Retrieved July 4, 2018, from <https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020>
- ENISA. (2018). *Reference Incident Classification Taxonomy*. Retrieved August 2, 2018, from <https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy>
- ENISA. (2018, January 26). *Reference Incident Classification Taxonomy*. Retrieved from ENISA: <https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy>

- ENISA. (2018, August 19). *Training Resources*. Retrieved from www.enisa.europa.eu:
<https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material>
- ENISA. (n.a.). *6th ENISA/EC3 Workshop*. Retrieved July 4, 2018, from <https://www.enisa.europa.eu/events/6th-enisa-ec3-workshop/6th-enisa-ec3-workshop>
- ENISA. (n.d.a). *CSIRT Maturity*. Retrieved July 4, 2018, from <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity>
- ENISA. (n.d.b). *CEI — List of NIS Experts*. Retrieved July 4, 2018, from <https://www.enisa.europa.eu/procurement/cei-list-of-nis-experts>
- ENISA. (n.d.c). *Training Resources*. Retrieved August 3, 2018, from <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material>
- ENISA, & Anderson, P. (2014a). *Electronic evidence — a basic guide for first responders*. Retrieved July 29, 2018, from <https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders/>
- EUR-lex. (n.d.). *National transposition measures communicated by the Member States concerning: Directive (EU) 2016/680*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L0680>
- Eurojust. (n.d.). *Eurojust*. Retrieved July 29, 2018, from <http://www.eurojust.europa.eu/Pages/home.aspx>
- Europe Union. (2018, August 14). *EU member countries in brief*. Retrieved from [Europa.eu](http://europa.eu):
https://europa.eu/european-union/about-eu/countries/member-countries_en
- European Commission. (2018, April 17). *COM(2018) 211 final*. Retrieved from ICANN:
<https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-211-F1-EN-MAIN-PART-1.PDF>
- European Commission — European Anti-Fraud Office (OLAF). (2016a, February 15). *Guidelines on Digital Forensic Procedures for OLAF Staff*. Retrieved July 31, 2018, from https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf
- European Commission (run by). (n.a.c). *Glossary*. Retrieved July 28, 2017, from http://ec.europa.eu/civiljustice/network/network_en.htm
- European Commission (run by). (n.d.a). *Legal systems — EU and national*. Retrieved July 4, 2018, from https://beta.e-justice.europa.eu/523/EN/legal_systems__eu_and_national
- European Commission (run by). (n.d.b). *Judicial systems in Member States*. Retrieved July 29, 2018, from https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-en.do
- European Commission (run by). (n.d.d). *Judicial systems*. Retrieved from https://e-justice.europa.eu/content_judicial_systems-14-en.do
- European Commission. (2014a). *Cultural and visual*. Retrieved July 27, 2018, from https://europa.eu/european-union/file/825/download_en?token=p8YdsZ5b
- European Commission. (2016, July 5). *Communication from the Commission Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry COM/2016/0410*

final. Retrieved July 29, 2017, from <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:410:FIN>

European Commission. (2017a, September 13). *Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises*. Retrieved October 20, 2017, from <http://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-MAIN-PART-1.PDF>

European Commission. (2017b, September). *2016 CEF Telecom Call — Cyber Security*. Retrieved August 1, 2018, from https://ec.europa.eu/inea/sites/inea/files/fiche_cybersecurity-2016.1.pdf

European Commission. (2018, January 29). Retrieved from ICANN: <https://www.icann.org/en/system/files/correspondence/avramopoulos-et-al-to-marby-29jan18-en.pdf>

European Commission. (2018, April 4). *on European production and preservation orders for electronic evidence in criminal matters (COM/2018/225 final)*. Retrieved July 4, 2018, from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN>

European Commission. (2018, April 17). *Proposal for Regulation on European production and preservation orders for electronic evidence in criminal matter (COM(2018) 225 final)*. Retrieved July 4, 2018, from https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF

European Commission. (2018a, April 17). *Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (COM/2018/226 final)*. Retrieved July 4, 2018, from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN>

European Commission. (2018b, April 17). *Communication Fourteenth progress report towards an effective and genuine Security Union (COM(2018) 211 final)*. Retrieved July 17, 2018, from <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-211-F1-EN-MAIN-PART-1.PDF>

European Commission. (2018c). *Improving criminal justice in cyberspace*. Retrieved July 30, 2018, from <https://rm.coe.int/octopus-ws-1-ec-evidence/16808c54dd>

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. (2013, February 7). *Joint Communication to the European Parliament, the Council, The European Economic and social committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Retrieved July 29, 2017, from http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. (2017, September 13). *Joint Communication JOIN(2017) 450 to the European Parliament and Council 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'*. Retrieved September 24, 2017, from <https://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF>

European Commission. (n.d.). *European e-Justice Portal — Judicial systems*. Retrieved July 27, 2018, from https://e-justice.europa.eu/content_legal_notice-365-en.do

- European Commission. (n.d. b). *EU Survey*. Retrieved July 4, 2017, from <https://ec.europa.eu/eusurvey/home/welcome>
- European Commission. (n.d. e). *Instrument contributing to Stability and Peace, preventing conflict around the world*. Retrieved August 3, 2017, from http://ec.europa.eu/dgs/fpi/what-we-do/instrument_contributing_to_stability_and_peace_en.htm
- European Commission. (n.d. f). *Instrument for Pre-Accession Assistance (IPA)*. Retrieved August 3, 2017, from http://ec.europa.eu/regional_policy/en/funding/ipa/
- European Commission. (2018, February 7). *Technical input on proposed WHOIS models on behalf of the European Union*. Retrieved from ICANN: <https://www.icann.org/en/system/files/files/gdpr-comments-european-commission-union-icann-proposed-compliance-models-07feb18-en.pdf>
- European Court of Human Rights. (n.d.). <https://www.echr.coe.int/Pages/home.aspx?p=home>. Retrieved July 4, 2018, from <https://www.echr.coe.int/Pages/home.aspx?p=home>
- European Data Protection Board. (2018a, August 13). *Cross-border cooperation and consistency procedures — State of play*. Retrieved from European Data Protection Board: https://edpb.europa.eu/news/news_en
- European Data Protection Board. (2018b, July 5). Retrieved from edpd: https://edpb.europa.eu/sites/edpb/files/files/file1/icann_letter_en.pdf
- European Justice. (2018, August 20). *My rights during the investigation of the crime and before the case reaches the court*. Retrieved from European Justice: https://e-justice.europa.eu/content_rights_of_defendants_in_criminal_proceedings_-169-EE-maximizeMS-en.do?clang=en&idSubpage=2&member=1
- European Parliament and Council of the European Union. (2002, July 12). *Directive 2002/58/EC 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. Retrieved August 28, 2017, from <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058>
- European Parliament and Council of the European Union. (2006, March 15). *Directive 2006/24/EC, 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*. Retrieved August 28, 2017, from <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32006L0024>
- European Parliament and Council of the European Union. (2013a, August 12). *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*. Retrieved July 29, 2017, from <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>
- European Parliament and Council of the European Union. (2013b, May 21). *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004*. Retrieved July 29, 2017, from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF>

- European Parliament and Council of the European Union. (2014, April 3). *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters*. Retrieved August 3, 2017, from <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>
- European Parliament and Council of the European Union. (2016, April 2016). *Directive (EU) 2016/680 on protection of natural persons with regard to processing of personal data by competent authorities for purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, a*. Retrieved July 29, 2017, from <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1501330438653&uri=CELEX:32016L0680>
- European Parliament and Council of the European Union. (2016a, March 9). *Directive on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings (EU) 2016/343*. Retrieved July 30, 2018, from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0343>
- European Parliament and Council of the European Union. (2016b, April 27). *Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC (General data protection directive) (GDPR)*. Retrieved July 29, 2017, from <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1501330122517&uri=CELEX:32016R0679>
- European Parliament and Council of the European Union. (2016e, July 06). *Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Retrieved July 06, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
- European Parliament, Council and Commission. (2000). *Charter of Fundamental Rights of the European Union*. Retrieved August 2, 2018, from http://www.europarl.europa.eu/charter/pdf/text_en.pdf
- European Union. (2017, September 9). *The 28 member countries of the EU*. Retrieved from https://europa.eu/european-union/about-eu/countries_en
- European Union External Service. (2017, August 3). *European neighbourhood policy (ENP)*. Retrieved from https://eeas.europa.eu/topics/european-neighbourhood-policy-enp_en
- Europol: European Cybercrime Centre and ENISA. (2017, December). *Common taxonomy for law enforcement and CSIRTs*. Retrieved August 2, 2018, from <https://www.europol.europa.eu/publications-documents/common-taxonomy-for-national-network-of-csirts>
- Europol. (2017). *Internet Organised Crime Threat Assessment (IOCTA) 2017*. Retrieved 11 02, 2017, from <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>
- Europol. (n.d.). *Europol*. Retrieved July 29, 2018, from <https://www.europol.europa.eu/>
- EVIDENCE Project. (n.d.). *European Informatics Data Exchange Framework for Courts and Evidence (Evidence)*. Retrieved August 3, 2018, from <http://www.evidenceproject.eu/>

- FRA (European Union Agency for Fundamental Rights). (n.d.). *Data retention across the EU*. Retrieved from <http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention>
- Geberth, V. J. (1995). *The 'Signature' Aspect in Criminal Investigation*. Retrieved July 31, 2017, from <http://www.practicalhomicide.com/articles/signature.htm>
- GitHub. (n.d. a). *MISP/misp-taxonomies*. Retrieved October 10, 2017, from <https://github.com/MISP/misp-taxonomies/blob/master/europol-incident/machinetag.json>
- GitHub. (n.d.). *Reference security incident classification taxonomy task force ToR*. Retrieved July 30, 2018, from <https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/Documentation/ToR.md>
- Henseler, H., & van Loenhout, S. (2018, March). Educating judges, prosecutors and lawyers in the use of digital forensic experts. *Digital Investigation*. Retrieved August 3, 2018, from <https://www.sciencedirect.com/science/article/pii/S1742287618300422>
- Home Office. (2014, February 24). Retrieved from Evidence in criminal investigations: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/488508/Evidence_v3.0EXT_clean.pdf
- ICANN. (2018a, August 13). *Beginner's Guide to Participating in ICANN*. Retrieved from ICANN: <https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf>
- ICANN. (2018b, August 13). *About WHOIS*. Retrieved from ICANN WHOIS: <https://whois.icann.org/en/about-whois>
- ICANN. (2018c, August 13). *German Appellate Court Rules on ICANN Request to Preserve WHOIS Data*. Retrieved from ICANN: <https://www.icann.org/news/announcement-2-2018-08-03-en>
- ICANN. (2018d, August 13). *What is WHOIS data used for?* Retrieved from ICANN: <https://whois.icann.org/en/what-whois-data-used>
- ICANN. (2018e, August 13). *Whois Compliance with GDPR — Reference*. Retrieved from GAC ICANN: <https://gac.icann.org/activity/whois-compliance-with-gdpr-reference>
- ICANN. (2018f, June 18). *Draft WHOIS Accreditation and Access Model*. Retrieved from ICANN: <https://www.icann.org/en/system/files/files/draft-whois-accreditation-access-model-v1.6-18jun18-en.pdf>
- ICANN. (2018g). *Temporary Specification for gTLD Registration Data*. Retrieved 08 21, 2018, from <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>
- ICANN. (2018h, May 25). *ICANN Files Legal Action in Germany to Preserve WHOIS Data*. Retrieved August 21, 2018, from <https://www.icann.org/news/announcement-2018-05-25-en>
- ICANN. (2018i, July 19). *ICANN Request to Preserve WHOIS Data Referred to German Appeal Court*. Retrieved August 21, 2018, from <https://www.icann.org/news/announcement-2-2018-07-19-en>
- ICANN v. EPAG Domainservices GmbH, 10 O 171/18 (Landgericht [regional court] Bonn, Germany May 29, 2018). Retrieved August 21, 2018, from <https://www.icann.org/de/system/files/files/litigation-icann-v-epag-request-court-order-prelim-injunction-redacted-30may18-de.pdf>

- ICANN v. EPAG Domainservices GmbH, 10 O 171/18 (Regional Court of Bonn May 29, 2018b). Retrieved August 21, 2018, from <https://www.icann.org/en/system/files/files/litigation-icann-v-epag-request-court-order-prelim-injunction-redacted-30may18-en.pdf>
- Insa, Fredesvinda. (2007). The admissibility of electronic evidence in court (AEEC): Fighting against high-tech crime—Results of a European study. *Journal of Digital Forensic Practice*, 285–289,. Retrieved August 3, 2018, from <https://www.tandfonline.com/doi/abs/10.1080/15567280701418049>
- International Court of Justice. (n.d.). Retrieved July 4, 2018, from <http://www.icj-cij.org/en>
- International Organisation for Standardisation (ISO). (2012). *Guidelines for identification, collection, acquisition, and preservation of digital evidence (ISO/IEC 27037:2012)*. Retrieved July 30, 2018, from <http://www.iso27001security.com/html/27037.html>
- Interpol. (n.d.a). *Structure and governance — national central bureaus*. Retrieved August 3, 2018, from <https://www.interpol.int/About-INTERPOL/Structure-and-governance/National-Central-Bureaus>
- McBride, J. (2018). *Human rights and criminal procedure — The case-law of the European Court of Human Rights*. Council of Europe.
- Mitrakas, A., & Zaich, D. (2009). Digital Forensics and the Chain of Custody to Counter Cybercrime. In *In Socioeconomic and Legal Implications of Electronic Intrusion*. doi:DOI: 10.4018/978-1-60566-204-6.ch010
- National Institute of Standards and Technology (NIST). (2006, August). *Guide to integrating forensic techniques into incident response*. Retrieved July 31, 2018, from <https://csrc.nist.gov/publications/detail/sp/800-86/final>
- NIST. (2018, August 20). *Computer forensics tool testing program (CFTT)*. Retrieved from National Institute of Standards and Technology: <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt>
- OLAF Supervisory Committee. (2010). Retrieved from Opinion No 5/2010: http://europa.eu/supervisory-committee-olaf/sites/default/files/documents/publications/opinions/Opinion_No_5_2010.pdf
- Portesi, S. (2008). *Ph.D. Thesis on the challenges faced by police forces in searching and seizing in situ computer evidence during criminal investigations: with special reference to England and Wales*.
- SANS. (2011). *Incident handler's handbook*. Retrieved from SANS institute infosec reading room: <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>
- Stikvoort, D. (2012). *Incident Classification/Incident Taxonomy according to eCSIRT.net — adapted*. Retrieved August 2, 2018, from <https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf>
- The Courts of Norway. (2018, August 20). *Accused or charged*. Retrieved from The Courts of Norway: <https://www.domstol.no/en/The-criminal-court-proceedings/who-is-involved/Tiltalt-eller-siktet/>
- United Nations Office and Drugs and Crime. (2006). *Policing, Crime Investigation Criminal Justice Assessment Toolkit*. Retrieved July 27, 2018, from https://www.unodc.org/documents/justice-and-prison-reform/cjat_eng/3_Crime_Investigation.pdf



Annex A: Abbreviations

Abbreviation	Description
ACPO	Association of Chief Police Officers of England, Wales and Northern Ireland (United Kingdom)
AEEC	Admissibility of Electronic Evidence in Court project
CEF	Connecting Europe Facility
CEI	Call for Expression of Interest
CEPOL	European Union Agency for Law Enforcement Training
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team for the EU institutions
CIRCL	Computer Incident Response Center (Luxembourg)
CSIRT	Computer Security Incident Response Team
CSS	Cyber Security Strategy
CSV	Comma-Separated Value (format)
CyBOX TM	Cyber Observable eXpression (language)
DB	Database
DDoS	Distributed Denial-of-Service (attack)
DG	Directorate General
DNS	Domain Name System
DoS	Denial of Service (attack)
DPO	Data Protection Officer
EC3	European Cybercrime Centre (Europol)
EDPB	European Data Protection Board
EEA	European Economic Area
EFTA	European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland)
ELO	Europol Liaison Office
EMAS	Europol Malware Analysis System
ENI	European Neighbourhood Instrument
ENISA	European Union Agency for Network and Information Security
ENP	European Neighbourhood Policy
ENU	Europol National Unit
EPAG	EPAG Domain Services GmbH
EPE	Europol Platform for Experts
EU	European Union
EUCTF	European Union Cybercrime Task Force
Eurojust	European Agency for the Enhancement of Judicial Cooperation.
Europol	European Union Agency for Law Enforcement Cooperation
Evidence project	European Informatics Data Exchange Framework for Courts and Evidence project
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
gLTD	Generic Top-Level Domain
ICANN	Internet Corporation for Assigned Names and Numbers
IcSP	Instrument contributing to Stability and Peace
IOC	Indicators Of Compromise

IoT	Internet of Things
IP	Internet Protocol
IPA	Instrument for Pre-Accession Assistance
ISA	International Society of Automation
ISF	Internal Security Fund
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
IT	Information Technology
J-CAT	Joint Cybercrime Action Taskforce
JHA	Justice and Home Affairs Council configuration (Council of the European Union)
LB	Liaison Bureau (J-CAT)
LE	Law Enforcement
LEA	Law-Enforcement Agency
MISP	Malware Information-Sharing Platform
MLA	Mutual Legal Assistance
MS	Member State
n.d.	No date
NCB	National Central Bureau (Interpol)
NIS	Network Information Security
NISD	Network and Information Security Directive
NIST	National Institute of Standards and Technology (United States)
OLAF	European Commission European Anti-Fraud Office
PGP	Pretty Good Privacy
PoC	Point of Contact
SIENA	Secure Information Exchange Network Application
SoD	Segregation (or separation) of Duties
TIP	Threat Intelligence Platform

Annex B: Definitions of the key concepts

In the context of this report the following definitions, listed in alphabetical order, apply:

- **Challenge** refers to ‘a situation that poses difficulties, a situation where one or more than one obstacle is present and needs to be overcome/removed, and where determination is required’ (Portesi, 2008). Challenges can be legal, organisational, technical, cultural, etc.
- **Communication** in most cases refers to the information sharing between different parties, in particular CSIRTs, LEs and judiciary. Sometimes the term ‘communication’ is also used in its legal sense of ‘policy document with no mandatory authority’ (European Commission (run by), n.a.c), such as the Commission *Communication on Strengthening Europe’s Cyber Resilience System* (European Commission, 2016). In a few cases it refers to the transmitted information or — especially when in plural — to a system used to transmit the information. Communication is an essential component of the cooperation between CSIRTs and LEs.
- **Computer security incident response team (CSIRT) or computer emergency response team (CERT)** is ‘an organisation that studies computer and network security to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and [...] offer other information to help improve computer and network security’. At present, ‘both terms (CERT and CSIRT) are used in a synonymous manner, with CSIRT being the more precise term’ (ENISA, 2015b, p. 7) (ENISA, 2015a, p. 12) (ENISA, 2016b, p. 10).
- **Cooperation** and **collaboration** are synonymous in this report. They refer to the joint work — especially of CSIRTs and LEs — in their coordination of actions, their reciprocal help and their joining efforts to fight against cybercrime.
- **Criminal courts** are courts in which criminal cases are tried and determined in order to appropriately punish offenders.
- **Criminal investigation or crime investigation** refers to the process of collecting (and preserving) evidence to be used to ascertain a fact that might be considered as a criminal activity and determine who is responsible for it. Normally this process starts when the suspected criminal activity is reported to the LE (or to the prosecutor depending on the country), or when the LE or the prosecutor become otherwise aware that such fact has been or is going to be committed and/or closed. The definition of criminal investigation might somehow vary from country to country; a definition of crime investigation can be found in (United Nations Office and Drugs and Crime, 2006, p. 1).
- **Criminal proceedings** refer to proceedings aiming to ascertain if a crime has been committed and who committed it. The adjective ‘criminal’ is used to distinguish them from other kinds of proceedings, such as civil, administrative and disciplinary, which have different aims and are governed by different rules.
- **CSIRTs network** is the network established by the Article 12 of the NIS directive (European Parliament and Council of the European Union, 2016e) ‘to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation’. It is composed of EU Member States’ appointed CSIRTs and CERT-EU. The European Commission participates in the network as an observer. ENISA is tasked to actively support the CSIRTs cooperation, provide the secretariat and active support for incident coordination upon request.
- **Cybercrime** is an umbrella term. An unequivocal definition of cybercrime does not exist. In general, we refer by it to ‘Any offence where the *modus operandi* or signature [which refers to ‘the mental and

emotional motivations” (Geberth, 1995)] involves the use of a computer network in any way’ (Casey E., 2004, p. 667). Cybercrime includes both crimes where computer is an object (e.g. illegal access to an information system) or a tool (e.g. storage of illegal images on a computer device or usage of a computer to plan a murder) of crime. It must be noted that ‘While many aspects of cybercrime are firmly established, other areas of cybercrime have witnessed a striking upsurge in activity, including attacks on an unprecedented scale, as cybercrime continues to take new forms and new directions’ (Europol, 2017).

- **Cultural aspects** refer to the dimensions of the CSIRT-LE cooperation and their interaction with judiciary that relate to culture. ‘Culture shapes our identities, aspirations and how we relate to others and the world’. ‘The challenges are significant. Cultural diversity is an asset for the EU, but linguistic and cultural differences lead to (...) fragmentation’ (European Commission, 2014a, p. 3).
- **EFTA**: the European Free Trade Association (EFTA, n.d.) is the intergovernmental organisation of Iceland, Liechtenstein, Norway and Switzerland.
- **Electronic evidence** (or e-evidence) refers to ‘evidence stored in electronic form [...] consisting in stored subscriber data, access data, transactional data and content data’ (European Commission, 2018, p. 38).
- **EU Member States** are the states that are part of the European Union. At present (status: 26 October 2018), there are 28 Member States (EU-28). In alphabetical order, they are: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom (Europe Union, 2018).
- **Governmental CSIRTs** are teams whose constituency are the public administration networks. Currently ‘in the EU, governmental CSIRTs are typically used to protect the cyberspace of governmental institutions including critical infrastructure [- more precisely, following NIS Directive (European Parliament and Council of the European Union, 2016e) and its Annex 2, the Operator of Essential Services -] as well as to ensure cyber-crisis management” (ENISA, 2015c, p. 9). ‘Governmental CSIRTs [indeed] mainly manage crisis and provide response to cyber threats and incidents concerning the public sector, but in many cases also the critical infrastructures, and in limited cases also the private domain, which however is usually within the remits of other CSIRTs in the private sector. [...] In some Member States, governmental CSIRTs have coordinating and supervision functions for other relevant stakeholders, which proves to be a useful practice, especially in those Member States where the response mechanism to cyber- attacks is quite complex, and/or a significant number of different CSIRTs both in the public and the private sector co-exist in parallel’ (Council of the European Union, 2017, p. 66).
- **Information sharing** refers to ‘the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice’ (ENISA, 2010, p. 9).
- **Incident** is ‘any event having an actual adverse effect on the security of network and information systems’ (European Parliament and Council of the European Union, 2016e).
- **Incident handling** refers to ‘all procedures supporting the detection, analysis and containment of an incident and the response thereto’ (European Parliament and Council of the European Union, 2016e).
- **Interaction** refers ‘a mutual or reciprocal action or influence’ (Collins Dictionary).
- **Judges** refers to a person who is in charge of a court of law and who makes final decisions.
- **Judiciary** is the ‘entirety of courts and judicial authorities in a state or in another sovereign organisation such as the European Union (EU). The main task of the courts is to resolve legal disputes

and to ensure that the law is applied correctly and coherently' (European Commission, n.d.). Judiciary in this report refers both to prosecutors and judges (similar approach taken in (Council of the European Union, 2017)).

- **Law enforcement (LE), law-enforcement agencies (LEAs), police and police agencies** are terms used in this report are synonymous and used to refer to police and police agencies, also used as synonymous. For this report, 'law enforcement' does not encompass prosecution services and courts, which are referred to in this report as 'judiciary'. LE usually fulfil the following missions: general police, investigation, public order and security state missions (Bureau of Justice Statistics, 2018).
- **Legal aspects** refer to the dimensions of the CSIRT-LE cooperation and their interaction with judiciary that relate to the rules and policies shaping and governing it, including obligations, discretion, prohibition to share information in their effort to fight against cybercrime.
- **National CSIRT** is a CSIRT that 'acts as national point of contact (PoC) for information sharing (like incident reports, vulnerability information and other) with other national [...] CSIRTs in the EU Member States and worldwide. National [...] CSIRT can be considered as 'CERT of last resort', which is just another definition of a unique national PoC with a coordinating role. In a lot of cases a national [...] CSIRTs also acts as governmental [...] CSIRT. Definitions may vary across the EU Member States' (ENISA, 2009, p. 8). A 'crucial role in monitoring and responding to cyber incidents is played by the national CSIRTs that the majority of the Member States have already established' (Council of the European Union, 2017, p. 12). Requirements and tasks for CSIRTs are listed in Annex I of the NIS Directive (European Parliament and Council of the European Union, 2016e).
- **Network and information system** refers to '(a) an electronic communications network [...]; (b) any device or group of interconnected or related devices, one or more of which, under a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance" (European Parliament and Council of the European Union, 2016e).
- **Organisational aspects** refer to those dimensions of the CSIRT-LE cooperation and their interaction with judiciary that relate to steps taken, procedures followed, resources available, etc. in their cooperation to fight against cybercrime.
- **Practices** refers to 'something that is usually or regularly done, often as a habit, tradition, or custom' (Cambridge University Press, n.d.).
- **Prosecutors:** refers 'a legal official who accuses someone of committing a crime, especially in a [criminal] law court' (Cambridge Dictionary, n.d.). 'The public prosecutors' office or prosecution service [...] is regarded as part of the judiciary in many Member States' (European Commission (run by), n.d.(b)). Also, for this report prosecutors are considered as part of the judiciary.
- **Taxonomy** 'is defined as a classification of terms. Three characteristics define a taxonomy:
 - a form of classification scheme to group related things together and to define the relationship these things have to each other;
 - a semantic vocabulary to describe knowledge and information assets; and
 - a knowledge map to give users an immediately grasp of the overall structure of the knowledge domain covered by the taxonomy, which should be comprehensive, predictable and easy to navigate' (ENISA, 2016a , p. 7).

'There is currently no consensus on concepts and definitions related to taxonomies' (ENISA, 2016a , p. 5).

- **Technical aspects** refer to the dimensions of the CSIRT-LE cooperation and their interaction with judiciary that relate to the tools (e.g. applications, the platforms) and the methodologies used to share information in their effort to fight against cybercrime.

Annex C: An overview of legal systems, areas of law, and legal traditions (common law and civil law)

Each Member State has its own laws and rules that govern the various facets of social interaction. The set of all these laws and rules constitutes a legal system.

A legal system is divided into areas, such as: private law (which includes the civil law in the sense of the law related to civil wrongs as opposite of criminal law which relates to crimes), public law, international law, European law, criminal law (the law related to crimes), and criminal procedure. Every legal system has elements that characterise all areas of law within that system. Depending on the legal system, the same area of law (for example, criminal procedure) can be disciplined differently. On some specific matters, however, the Member States might have the same legislation, or a very similar one, either since they come from a similar legal tradition or because the matter is regulated at EU level.

The national legal systems can be divided into two main groups: the civil law systems⁽²⁶⁾ and the common law systems. Some countries have mixed legal systems of civil and common law. Most Member States of the European Union base their legal system on a codified civil law. Nordic legal tradition is generally considered as belonging to civil law tradition but with some own characteristics⁽²⁷⁾. Member States with common law system include United Kingdom, Ireland and Cyprus and a mixed legal system can be found in Malta. The European Union law is based on the treaties and mixes civil law with an attachment to the importance of case-law of the European Court of Justice. As seen in Figure 23, the map provides an overview of the different legal traditions in the EU and in EFTA.

The civil law systems derive from Roman law. These systems represent the legal systems of continental Europe and those that derive from them. Even though individual civil law systems may vary widely both in procedure and substantive law, there are common features, the main one being that its core principles are codified into a referable system, which serve as a primary source of law.

The common law systems derive from the juridical tradition developed in England (United Kingdom) in the Eleventh Century. Common law systems are English law, the United States law and those derived from them. The main feature of common law systems is that the body of law is derived mainly from judicial decisions of courts. The following main two differences should be mentioned between civil law and common law systems:

- These two groups of legal systems attribute a different role to judgments. Only in common law systems a case-law is considered not only as a source of law, but as a source of law of primary importance. In the common law system, judges therefore have an active role in developing rules. Instead, in a civil law system a case-law is not a source of law.

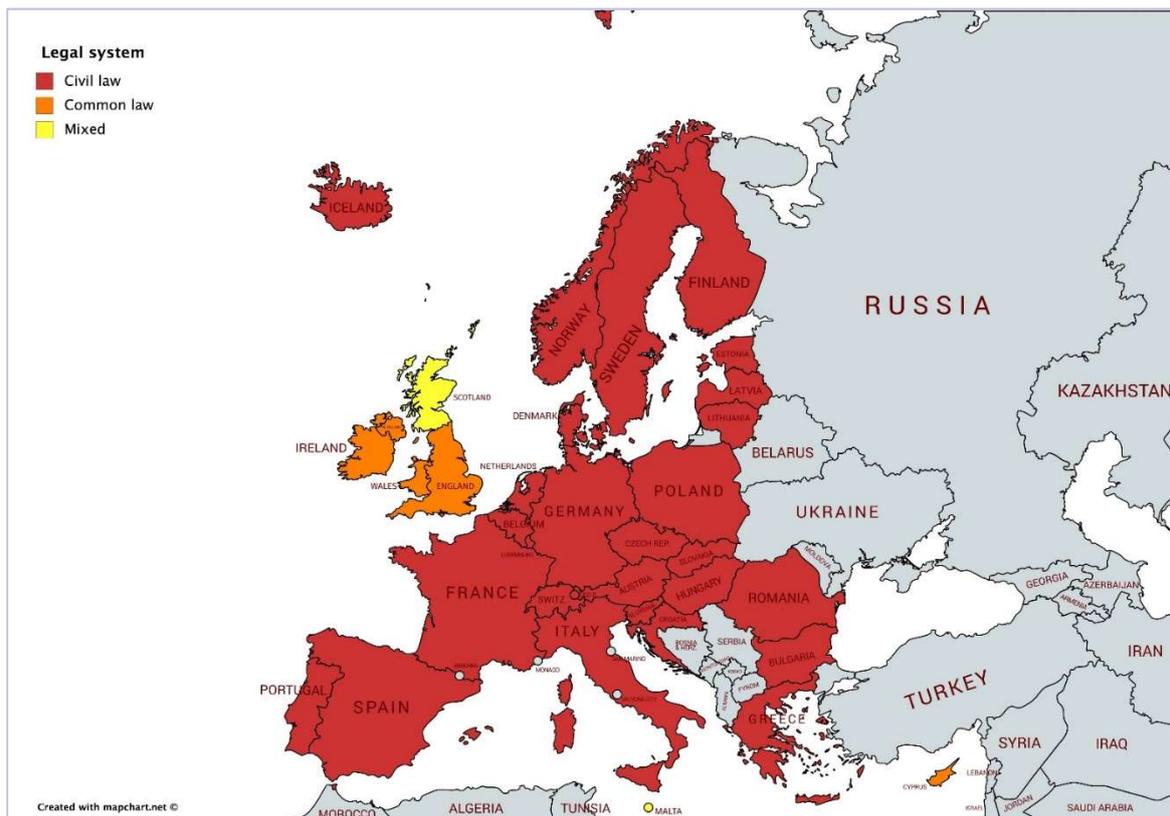
⁽²⁶⁾ The term 'civil law' has two meanings. It may refer to the non-criminal branch of law in a common law legal system, and to the continental law originating in continental Europe and based on Roman law. In this study by 'civil law system' we mean the latter, the legal system based on continental legal tradition.

⁽²⁷⁾ 'The Nordic countries lack a general civil code⁽²⁷⁾ and are using a system of less comprehensive statutes supplemented by analogies from statutory provisions, case-law and legal doctrine filling the gaps' (Berniz, p. 28).

- In the common law systems, the judge, except cases, must comply with what was decided by previous judgments. In civil law systems the precedent can be important, but it is never binding for a new decision and, in any case, it is not a source of law.

The difference between the different legal traditions and legal systems influences considerably the area of criminal procedural law (described below) and so the interaction and information flow with the different players namely, as far as concerns this report, the CSIRT, LE and the judiciary.

Figure 23 — Map Showing the Different Legal Traditions in the EU and EFTA (created with mapchart.net)



Annex D: The WHOIS registry

Most of the 21 subject-matter experts interviewed for this report expressed the opinion that, while the GDPR has an impact on the publicly availability of certain WHOIS data used for the criminal investigations/incident handling, in principle this has not impacted the way CSIRTs and LE cooperate. However, several interviewees highlighted that because of the fact that the GDPR is applicable only as of 25 May 2018, it is difficult to make a complete assessment of the changes or possible changes that might occur.

One of the WHOIS legitimate use indeed is for criminal investigations and incident managing (ICANN, 2018d). Domain names are essential for criminals to run their infrastructures and malicious campaigns online. They need domains for getting sensitive information from internet users (Phishing), to spread malicious software or to send Spam to internet users. Even though criminals use fake or stolen identities to register domain names most of the time, these identifiers are invaluable for detecting and preventing internet crime that depends on domain names, like any legal online business.

On 25 May, the international law-enforcement community and the CSIRT communities have lost direct access to personal data on registrants of domain names. This is having a very strong negative impact both on criminal investigations online and on the security and defence of networks in general and represents a challenge for LE and for the CSIRT community in the performance of their tasks. Therefore, timely access to what is now non-public WHOIS information (without court order) should be ensured for both the LEA community and the CSIRT.

LE now need to initiate formal legal process and MLA to obtain relevant information. This comes with a substantial administrative burden as well as long delays⁽²⁸⁾. The delays involved in obtaining WHOIS data from registries, registrars and lower-level providers through formal legal process may be much longer than the period for which the data in question is being retained. By the time formal procedures are concluded, the data may therefore no longer exist. This is significantly harming the public interest and has severe negative consequences for the rule of law online.

For the CSIRT community the situation is worse because they do not have the mandate to request a court order so they are dependent on the goodwill of registries and registrars to access the information.

ICANN community is currently trying to agree on a Unified Access Model to non-public WHOIS information for entities which have a legitimate need (public interest). It is absolutely essential that both LEA and CSIRT have this direct access because of their function.

Usage of WHOIS for Incident Handling and for Criminal Investigations

The 'WHOIS is indispensable to the smooth operation of the DNS' but it also 'used for many [other] legitimate purposes, including:

⁽²⁸⁾ EJCN statement on WHOIS database reform - WK 6398/2018 INIT – 29 May 2018.

- To establish or look into an identity in cyberspace, and as part of an incident response following an internet or computer attack (security professionals and law-enforcement agents use WHOIS to identify points of contact for a domain name.)
- 'To gather investigative leads (i.e. to identify parties from whom additional information might be obtained). Law-enforcement agents use WHOIS to find email addresses and attempt to identify the location of an alleged perpetrator of a crime involving fraud' (ICANN, 2018d).

WHOIS and GDPR compliance

Some preliminary considerations should be made when addressing the WHOIS and its compliance to the GDPR:

- The GDPR has been applicable as of 25 May 2018.
- The GDPR builds on existing principles, such as the principle of lawfulness, fairness and transparency, principle of purpose limitation and the principle of data minimisation.
- The GDPR concerns personal data on individuals, not to legal entities.
- In the context of the WHOIS some personal data, but not only personal data, are processed.
- As discussed above (see Section 3.2.2.1) the GDPR does not apply to the processing of personal data 'by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'. The data protection law enforcement directive applies instead.
- The legitimacy and the importance of access to WHOIS data for public policy purposes (firstly LE) is uncontested.
- LEs have a clear interest in having access to data in the WHOIS register when it is necessary for their investigations; reason why some access procedures should be designed to ensure that LE can obtain WHOIS data, not publicly available, within an appropriate time frame for the investigation (European Commission, 2018).
- The issue of the WHOIS and its compliance to protection of personal data rules was discussed also well-before the GDPR has started to become applicable: the 'EDPB [European Data Protection Board]'s predecessor, WP29 [Working Party Article 29], has been offering guidance to ICANN on how to bring WHOIS in compliance with European data protection law since 2003' (European Data Protection Board, 2018a).
- With the approaching of the GDPR applicability and now that the GDPR is applicable, this discussion seemed to have become more intensive.

Some recent developments of this discussion include:

- A dialogue within ICANN and between ICANN and the main stakeholders to find viable solutions to have a GDPR-compliant WHOIS while enabling legitimate uses by relevant stakeholders (including LE and CSIRTs) as well as unpublished WHOIS data. For instance, 'As work is ongoing within ICANN to make this database compliant with data protection rules, in particular the general data protection regulation [GDPR], the Commission sent a letter (European Commission, 2018) to ICANN on the dual objectives of ensuring quick access to its directories for public interest purposes whilst being fully compliant with EU data protection rules. The ICANN Government Advisory Committee, in which national governments and the Commission are represented, voiced its concerns and called on ICANN

to ensure continued access to the WHOIS, including non-public data, for users with a legitimate purpose.’ (European Commission, 2018). The European Commission in its ‘Technical input on proposed WHOIS Models on behalf of the European Union.’ (European Commission, 2018) made observations on the different proposed models to provide access by LE to certain WHOIS data not publicly but necessary for them for the performance of their task. Also the EDPB in its letter of 5 July 2018 provided ICANN with guidance to enable ICANN to develop a GDPR-compliant model for access for legitimate purposes to personal data that are processed in the context of WHOIS but are not publicly available (European Data Protection Board, 2018b).

- The development of technical solutions (e.g. logging to access non-public WHOIS data) as well as of accreditation programmes ‘allowing full access to non-public WHOIS data for LE and other legitimate third parties (IP Rights, cybersecurity, etc.)’ (ICANN, 2018e). See for instance the *Draft accreditation & access model for non-public WHOIS data* (ICANN, 2018f).
- The recent court case of ICANN before German Courts ⁽²⁹⁾, requesting an injunction against an accredited registrar to reinstate the collection of all WHOIS data required under their registrar accreditation agreement: the registrar had stopped to collect some of these data (e.g. administrative and technical contact information) when selling new domain name registrations because believing

⁽²⁹⁾Below are summarised the main steps of this court case (status: 9 August 2018):

- 17 May 2018: effective as of 25 May 2018 (starting date of GDPR applicability), ICANN adopted Temporary Specification for gTLD Registration Data (ICANN, 2018g), which ‘establishes temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR’ (ICANN, 2018g).
- 25 May 2018: ‘The internet Corporation for Assigned Names and Numbers (ICANN) [...] filed injunction proceedings against EPAG, a Germany-based, ICANN-accredited registrar [...]. ICANN has taken this step to ask the court for assistance in interpreting the European Union’s General Data Protection Regulation (GDPR) in order to protect the data collected in WHOIS. ICANN’s “one-sided filing” in Bonn, Germany, seeks a court ruling to ensure the continued collection of all WHOIS data, so that such data remains available to parties demonstrating legitimate purpose to access it, consistent with the GDPR’ (ICANN, 2018h).
- 29 May 2018: the Regional Court of Bonn decided that ‘it would not issue an injunction against EPAG. In rejecting the injunctive relief, the Court ruled that it would not require EPAG to collect the administrative and technical data for new registrations. However, the Court did not indicate in its ruling that collecting such data would be a violation of the GDPR’ (ICANN, 2018i) (sentence in German: (ICANN v. EPAG Domainservices GmbH, 2018) - non-official translation to English: (ICANN v. EPAG Domainservices GmbH, 2018b).
- 13 June 2018: ICANN appealed against the ruling of the Regional Court of Bonn to the Higher Regional Court of Cologne, Germany, and ‘again asked for an injunction that would require EPAG to reinstate the collection of all WHOIS data required under EPAG’s Registrar Accreditation Agreement with ICANN’ (ICANN, 2018c) (Appeal in German – Appeal in English non-official translation: <https://www.icann.org/en/system/files/files/litigation-icann-v-epag-immediate-appeal-redacted-13jun18-en.pdf>)
- 21 June 2018: ‘the Regional Court in Bonn, Germany, decided to revisit its ruling in the injunction proceedings, which it has the option to do upon receipt of an appeal (<https://www.icann.org/news/announcement-2-2018-08-03-en>)
- 18 July 2018: ‘the Regional Court [of Bonn] decided not to change its original determination not to issue an injunction against EPAG, and referred the matter to the Higher Regional Court in Cologne for the appeal’
- 3 August 2018: ICANN announced that the ‘German appeal court (Appellate Court of Cologne) has issued a decision on the injunction proceedings ICANN initiated against EPAG, a Germany-based, ICANN-accredited registrar that is part of the Tucows Group. The Appellate Court has determined that it would not issue an injunction [emphasis added] against EPAG. In making its ruling, the Appellate Court stated that the interpretation of the GDPR was not material to its decision, so there was no obligation to refer the matter to the European Court of Justice’ [emphasis added]’ (<https://www.icann.org/news/announcement-2-2018-08-03-en>)

that the collection of that particular data would be in violation of the GDPR; ICANN with this court case also aimed to seek assistance on the GDPR interpretation. It must be noted that on 3 August 2018 the Appellate Court has determined that it would not issue such injunction and in making its ruling, 'the Appellate Court stated that the interpretation of the GDPR was not material to its decision, so there was no obligation to refer the matter to the European Court of Justice' (ICANN, 2018c).

Annex E: Questionnaire to support the subject matter expert Interviews

The questions below have been prepared to support the interviews with subject-matter experts to collect data for drafting an ENISA report on 'Current cooperation between CSIRT and LEA community and on possible ways to further enhance their cooperation' (provisional title: 'The Interplay between CSIRTs, Law enforcement and the judiciary in the fight against cybercrime: Closing the cycle'). This report contributes to the implementation of Output O.4.2.2 (Support the fight against cybercrime and collaboration between CSIRTs and LEAs) of the ENISA's Programming Document 2018-2020 (link: <https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020>). The report is expected to be published by end of 2018.

ENISA selected some external experts from the List of NIS Experts compiled following the ENISA call for expression of interest (CEI) (Ref. ENISA M-CEI-17-T01) to support the data collection and drafting of this report. In addition to desk research and an online survey (planned), the data collection is done also via interviews with subject-matter experts.

The expected duration of the interview is 1 hour.

Some of the questions below are common to CSIRTs, LEAs and judiciary (judges and prosecutor), while others are tailored to CSIRTs, LEAs and judiciary.

For information regarding how your personal data are processed, see the privacy statement below (after the questions).

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

Interviewer:

Date of the interview:

Name of the interviewee:

Affiliation:

Position:

Country:

QUESTIONS COMMON TO CSIRTs/LEAs AND JUDICIARY (PROSECUTORS AND JUDGES)

1. What is your organisation legal basis?
2. What types of cyber incidents/cybercrime cases does your organisation deal with? (e.g. denial of service (DoS), phishing, unauthorised access, etc.)

3. Does your legal framework (i.e. the legal framework you are subject to) support the cooperation between CSIRT/LEA and the interaction/information flow with the judiciary (prosecutors and judges) in cybercrime proceedings and in general in responding to cybercrime? How?
4. What kinds of information does your legal framework allow and require you to share and with which subjects (CSIRT, Law-Enforcement Agencies (LEAs), judges and prosecutors as applicable)?
5. How often do you share information with your counterparts (CSIRTs, LEAs, prosecutors and judges as applicable) during the incident handling/investigation?
6. As far as it concerns cybercrime cases, could you briefly describe the information flow/interaction between CSIRT — national and governmental in particular — LEAs, prosecutor and judge?
7. Do you think that the interaction and the information flow CSIRTs/LEAs and judiciary (prosecutors and judges) work well?
8. What do you believe to be the most challenging aspects of this interaction/information flow?
9. Which aspects of this interaction/information flow you may be able change and/or improve?
10. Which of these aspects are out of your control?
11. Are you aware of the GDPR and any potential impact it may have on how you work with other organisations?
12. How would you see joint training for CSIRTs, LEAs and judiciary (prosecutor and judges)? Which topics should they cover?
13. When there is a disclosure (Coordinated Vulnerability Disclosure) of a newly discovered vulnerability in either hardware, software or a service are you aware of any cooperation or coordination between CSIRTs, LEAs and Judiciary for sharing the CVD.

CSIRT SPECIFIC QUESTIONS (TO BE ASKED ONLY TO CSIRTs)

- 1A. What kind of CSIRT team do you represent (e.g. national, government, private sector, regional, sectoral)?
- 2A. Are there situations/cases where you decide to advise the victim in your constituency to contact the LEA? Do you follow a specific procedure to determine when it is appropriate to advise the victim to contact law enforcement?
- 3A. Does your legal framework require you to inform LEA of identified activities that may be considered a crime?
- 4A. Are there situations/cases where you decide to contact the LEA? Do you follow a specific procedure to determine when it is necessary to inform the LEA?
- 5A. How do you think CSIRTs and LEAs could avoid duplication of efforts?
- 6A. What kinds of information that is relevant to criminal investigations is available to you?
- 7A. Who and on what basis decides that identified activity may be considered a criminal offence?
- 8A. What information do you advise the victim to provide or you provide to the LEA when reporting a criminal offence?
- 9A. How do you exchange information with the LEA? (offline, online, verbally...)
- 10A. Does your legal framework allow you to inform LEA of identified activities that may be considered a crime? Are there any limitations on the scope of information that you can share voluntarily with the LEA?

- 11A. Can you be called as a witness / expert in criminal proceedings? Does it happen often? Is this the only occasion where you get directly in contact with the prosecutor and with the judge in cybercrime cases?
- 12A. Are there any challenges in your information sharing/interaction with the LEAs? If yes, which kind of challenges you encounter (e.g. legal, organisational, cultural, technical)?
- 13A. Does the GDPR changes your way to get and process information? (*Question to be asked only if not yet covered by reply to Question 11*)
- 14A. Does the GDPR changes your way to interact and sharing data with the LEAs? (*Question to be asked only if not yet covered by reply to Question 11*)
- 15A. Are there any challenges in your information sharing/interaction with prosecutors and judges? If yes, which kind of challenges you encounter (e.g. legal, organisational, cultural, technical)?

LEA-SPECIFIC QUESTIONS (TO BE ASKED ONLY TO LEAs)

- 1B. Are you familiar with the CSIRT-type structures in your country and the technical capabilities that they have?
- 2B. What kind of CSIRT do you work with the most (e.g. national, government, private sector, regional, sectoral)?
- 3B. Do you have designated points of contact from/for your national / governmental / (other type) of CSIRT?
- 4B. Which kind of support do you request from CSIRTs?
- 5B. In what kind of investigations do you request CSIRT technical expertise?
- 6B. Does the CSIRT report to you criminal offences? Does the CSIRT help the victims in its constituency report criminal offences?
- 7B. Can you exchange data with CSIRTs? If yes, with which CSIRTs, which kinds of data and under which circumstances?
- 8B. What are the specific challenges you encounter (legal, organisational, technical, cultural)?
- 9B. What is to your point of view the added-value of information sharing and cooperation with the CSIRTs?
- 10B. In cybercrime cases, does the prosecutor meet the CSIRT? And does the judge meet the CSIRT? If so, on what type of occasion? Only where CSIRT representative is witnesses / expert in court?
- 11B. Are CSIRT representative sometime witnesses in court? Under which circumstances?
- 12B. Does the GDPR changes your way to interact with CSIRTs? And to get information via other channels (including data basis)? (*Question to be asked only if not yet covered by reply to Question 11*)
- 13B. Do you practice multilateral cooperation at supranational level with CSIRTs (through Europol/ENISA)?

JUDICIARY (PROSECUTORS AND JUDGES) SPECIFIC QUESTIONS (TO BE ASKED ONLY TO JUDICIARY)

- 1C. What data transmitted by CSIRTs is the most often used as evidence in a criminal trial?
- 2C. Have you ever had problems in a criminal trial with admissibility or usability of data received from CSIRTs? Could you give an example of such problems?
- 3C. What criteria must the data provided by a CSIRT meet to be admissible as evidence in criminal proceedings?

- 4C. Have you ever had legal constraints in asking CSIRT for data? If so, what were the constraints?
- 5C. Do you approach CSIRTs directly or via the LEA?
- 6C. Does a LEA need court order to request data from the CSIRT for the purposes of criminal investigation? Always? Under which circumstances?
- 7C. In cases where data belongs to foreign CSIRTs, how do you approach them?
- 8C. When do you use the letter rogatory, when the European Investigation Order, and when the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union to request data in criminal proceedings?
- 9C. Have you ever given up asking for data from a foreign CSIRT because you thought it was too difficult to get?
- 10C. Is it a problem for you that the IP address is kept for different times by CSIRTs of different countries?
- 11C. Have you had a request for data refused by a CSIRT of your country? And by a CSIRT from another country? If so, on what basis?
- 12C. Can a CSIRT representative be summoned in criminal proceedings as a witness or as an expert?
- 13C. What are the specific challenges you encounter when you interact with CSIRTs (legal, organisational, cultural, technical)?

QUESTIONS ON MENTIONING OF NAME, AFFILIATION, AND COUNTRY

- Do you agree on having your forename, surname, affiliation and country mentioned in the report (Note: it is not confirmed whether names of interviewees will be mentioned in the report)?
- Do you agree on having your forename, surname, affiliation and country mentioned in the acknowledgements of the report? (NOTE: it is not confirmed whether names of interviewees will be mentioned in the acknowledgements of the report)?
- Do you agree on having stated in the report that information on your country has been collected via an interview with a CSIRT/LE/judiciary (prosecutor/judge) representative?

Privacy Statement — ENISA Report on CSIRT-LE cooperation

Your personal data shall be processed in accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council (OJ L8 of 12.1.2001, p1) on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. [1]

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

The legal basis for the processing operation is:

- Article 5(a) of Regulation 45/2001/EC[2] based on Article 3(b)(v) of the Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, repealing Regulation (EC) No 460/2004[3],

stating that one of ENISA's tasks is: to 'support voluntary cooperation among competent public bodies, and between stakeholders'. With the view of contributing to the fulfilment of such task and according to the ENISA Programming Document 2018-2020 as approved by Management Board in Decision No MB/2017/11[4], ENISA is drafting a report on 'Current cooperation between CSIRT and LEA community and on possible ways to further enhance their cooperation' (see Output O.4.2.2 — Support the fight against cybercrime and collaboration between CSIRTs and LEA); or

- o Article 5(d) of Regulation 45/2001/EC based on the consent of the data subject.

The purpose of this processing operation is to collect data via an online survey and some subject-matter interviews for the drafting of the ENISA report on 'Current cooperation between CSIRT and LEA community and on possible ways to further enhance their cooperation'.

The following personal data are collected for the respondents of the online survey and of the interviews.

- a. Contact data: name, surname, community they belong to (e.g. CSIRT, LE, prosecutors, judges, etc.), position, affiliation, country, email address, phone number (optional).
- b. Knowledge-related data: While participating in the online survey and by replying to the questions during the interviews a respondent may produce data, for example data related to his or her knowledge and analysis in the field of information security.

The recipients of the data will be designated ENISA staff involved in the data collection and drafting of the report, and some external experts, selected by ENISA from the 'Call for Expressions of Interest — List of NIS Experts' [5], supporting ENISA with the data collection and the drafting of the report. Only when explicit written consent is provided by the data subject, name, surname, affiliation, country, might be included in the acknowledgements of the report that is expected to be published in December 2018. The data may also be available to EU bodies charged with compliance monitoring and inspection tasks.

While the online survey will be conducted by using the EU Survey tool [6], the interviews with subject-matter experts will be conducted face-to-face, over the phone, via skype or with other means to be agreed with the interviewee.

Personal data will be kept up to a maximum period of one year after the publication of the report, expected to be published in December 2018. After the end of this period, the contact data will be manually deleted. However, knowledge-related data are kept by ENISA beyond this period in an anonymised form (without linking to contact data) for future ENISA projects.

You have the right to access your personal data, the right to correct any inaccurate or incomplete personal data and the right to delete your data. Knowledge-related data will be kept in anonymised form (without linking to contact data). If you have any queries concerning the processing of your personal data, you may address them to the ENISA staff working on this report at CSIRT-LE-cooperation@enisa.europa.eu.

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

[1] http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32001R0045&model=guichett

[2] Whereby the processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties or other legal instruments adopted on the basis thereof.

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN

[4] <https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020>

[5] <https://www.enisa.europa.eu/procurement/cei-list-of-nis-experts>

[6] <https://ec.europa.eu/eusurvey/home/welcome>

Annex F: Questions in the online survey

Brief survey for 2018 ENISA Report on CSIRT-LE cooperation

Fields marked with * are mandatory.

This short online survey has been prepared by [ENISA](#), in conjunction with external experts, to support the data collection for the ENISA report on current cooperation between CSIRTs (computer security incident response teams) and law enforcement and their interaction with the judiciary (prosecutors and judges).

This report contributes to the implementation of 'Output O.4.2.2 — Support the fight against cybercrime and collaboration between CSIRTs and LEA' of the [ENISA Programming Document 2018-2020](#), in particular to what is foreseen as publication on 'Current cooperation between CSIRT and LEA community and on possible ways to further enhance their cooperation'.

All questions are with closed answers but some free text boxes are also included in order to allow the respondents to add additional comments/information if they wish to do so.

The estimated time to complete this survey is **maximum 15**.

For information on personal data processed within this specific survey, please download the following privacy statement: (The privacy statement is omitted from this report)

For information on personal data processed by the EUSurvey service itself, please click [here](#).

For any questions related either to this survey or to ENISA projects in the area of CSIRT and law enforcement cooperation, please contact: CSIRT-LE-cooperation@enisa.europa.eu

*Name and surname

*Organisation

*Country

Please select

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic [Czechia]
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- OTHER
- Poland
- Portugal
- Romania
- Slovak Republic
- Slovenia
- Spain
- Sweden
- Switzerland
- United Kingdom

Please specify OTHER country

*Which community are you from?

Please select one answer

- CSIRT
- Law enforcement
- Both CSIRT and law enforcement (e.g. from CSIRT seconded to law enforcement or vice versa)
- Prosecutors
- Judges
- Other

Please specify

1. How often in your country is information provided by CSIRTs — in particular national/governmental CSIRTs — used for **criminal investigations** [1]?

Please select one answer

- Often
- Occasionally
- Rarely
- Never
- I do not know

[1] By 'criminal investigation' we refer to the process of collecting (and preserving) evidence to be used to ascertain or prevent a fact or facts that might be considered as a criminal activity and determine who is responsible for it.

2. How often in your country is information provided by CSIRTs — in particular national/governmental CSIRTs — used as evidence **in criminal proceedings in court**?

Please select one answer

- Often
- Occasionally
- Rarely
- Never
- I do not know

3. In your country, how often are national/governmental CSIRTs called to write detailed expert reports to use in **criminal proceedings in court**?

Please select one answer

- Often
- Sometimes
- Hardly ever
- Never
- I do not know

4. In your country, how often national/governmental CSIRT is called as witness in **criminal proceedings in court**?

Please select one answer

- Often
- Sometimes
- Hardly ever
- Never
- I do not know

5. In your experience what kind of data provided by CSIRT is most often used for **criminal investigations**?

Select one or more answers

- IP addresses
- Indicators of compromise (IOC) (malware information, file hashes, mutex, etc.) other than IP addresses
- Personal information other than IP addresses
- Timeline of events
- Reconnaissance detection indicators prior to infection
- Details on personas/accounts on social networks / darknet places
- Information that supports proper coordination (e.g. information related to cases already monitored)
- Malicious campaign and context information
- Information on potential victims and/or attackers (e.g. credit card data obtained after taking down a phishing website)
- Decryption keys in cases of ransom attacks
- Information on the modus operandi of the attackers
- Details about specific cases CSIRTs are dealing/dealt with
- Statistics and reports on cases CSIRTs dealt with and on trends
- Other

Please specify

6. In your experience what kind of data provided by CSIRT is most often used as evidence **in criminal proceedings in court?**

Select one or more answers

- IP addresses
- Indicators of compromise (IOC) (malware information, file hashes, mutex, etc.) other than IP addresses
- Personal information other than IP addresses
- Timeline of events
- Reconnaissance detection indicators prior to infections
- Details on personas/accounts on social networks / darknet places
- Information that supports proper coordination (e.g. information related to cases already monitored)
- Malicious campaign and context information
- Information on potential victims and/or attackers (e.g. credit card data obtained after taking down a phishing website)
- Decryption keys in cases of ransom attacks
- Information on the modus operandi of the attackers
- Details about specific cases CSIRTs are dealing/dealt with
- Statistics and reports on cases CSIRTs dealt with and on trends
- Other

Please specify

7. Do personnel of CSIRTs — in particular of national/governmental CSIRTs — need to adhere to specific legal conditions and guidelines while collecting or assisting in the collection of evidence in support of an investigation?

- Yes
- No
- I do not know

Please use the box below to provide more information on conditions or guidelines that CSIRT personnel need to adhere to while collecting or assisting in the collection of evidence in support of an investigation?

8. In your country, have the national/governmental CSIRT a duty to inform the victim of a suspected cybercrime?

Please select one answer

- Yes, always
- No, never
- It depends

Please specify

9. Have the national/governmental CSIRT in your country a duty to report cybercrime to the law enforcement?

Please select one answer

- Yes, always
- Yes, but only in specific cases (e.g. serious cases)
- No, it does not have a duty but he can report
- No, it cannot report, it can only inform the victim and advice the victim on how to report
- I do not know
- Other

Please specify

9A. To whom does the national/governmental CSIRT in your country report cybercrime?

Please select one answer

- To the law enforcement (police)
- To the prosecutor directly
- Either to the law enforcement or to the prosecutor depending on the case
- Other

Please specify

10. In your country who takes the lead in criminal investigations?

- Law enforcement (police)
- Prosecutor
- Judge (e.g. magistrate in charge of preliminary investigations)
- It depends
- Other

Please specify

Please specify

11. Does the interaction and the information flow across CSIRTs, law enforcement and judiciary (prosecutors and judges) work well?

- Strongly agree
- Agree
- Partially agree (e.g. it works but can improve)
- Disagree
- There is no interaction
- I do not know

12. Are there any challenges hindering the interaction and information flow across CSIRTs, law enforcement and judiciary (prosecutors and judges)?

Please select one or more answers

- Organisational
- Legal
- Technical
- Cultural
- Other

Additional comments, if any

Please use this box for any additional information/comment you might wish to provide us with

Please specify

13. What are your suggestions to improve the information flow and the interaction across the CSIRT, law enforcement and judiciary communities?

Please select one or more answers

- Joint training
- Common tools (e.g. access to same platforms)
- Common taxonomy
- Appointment of liaison officers
- Regular meetings
- Feedback on the information provided/shared
- Memoranda of Understanding
- Other

Additional comments, if any

Please use this box for any additional information/comment you might wish to provide us with

13A. How important is/would be to have joint training for CSIRTs, law enforcement and judiciary?

Please select one answer

-
- Very important
- Important
- Not that important
- Not important at all

Additional comments, if any

Please use this box for any additional information/comment you might wish to provide us with

14. Which topics should joint training for CSIRT, law enforcement and judiciary cover?

Please select one or more answers

- Digital evidence collection
- Digital evidence handling
- Digital evidence analysis
- Drafting detailed reports to be used in criminal courts
- Helping the victim report the crime
- Helping the victim provide useful information for the criminal investigations
- Helping the victim provide useful information to be used as evidence in criminal courts
- Cooperation between CSIRT, law enforcement and judiciary (e.g. synergies, challenges, etc.)
- Other

Additional comments, if any

Please use this box for any additional information/comment you might wish to provide us with

Please specify

15. What are the strengths that national/governmental CSIRT in your country has and you would wish to see more in the law enforcement?

Please select one or more answers

- Technical skills
- Technical tools
- Agile processes, which requires little formalities, to respond to requests for information
- Consolidated trust relations with their peer in other Member States, which also helps get swift responses to request for information
- Well-established cooperation with the private sector
- Other

Additional comments, if any

Please use this box for any additional information/comment you might wish to provide us with

Please specify

16. What are the strengths that law enforcement in your country has and you would wish to see more in the national/governmental CSIRT?

Please select one or more answers

- Detective skills
- Knowledge of the chain of custody and requirements for admissibility of evidence in criminal proceedings
- Ability to draft detailed reports to be used in criminal courts
- Well-defined role, easy to understand by all parties involved in a case
- Other
- Additional comments, if any

Please use this box for any additional information/comment you might wish to provide us with

Please specify

Please use this free text box for any additional information/comment you might wish to provide us with

Thank you very much for your time and your input!

For any questions related either to this survey or to ENISA projects in the area of CSIRT and law-enforcement cooperation, please contact: CSIRT-LE-cooperation@enisa.europa.eu

Annex G: Examples of topics for CSIRT/LE/judiciary joint training

Examples of topics for CSIRT/LE/judiciary joint training include:

- information sharing (including the kind of information to share)
- information flow
- obligations and restrictions to the information sharing
- information tools, including platforms (e.g. MISP)
- communication channels
- crime reporting
- evidence collection
- digital investigations
- forensic tools
- digital evidence and chain of custody
- procedures e.g. formal request for data, MLA procedures
- cyber exercises
- cyber threat intelligence
- penetration testing
- vulnerability scanning
- reverse engineering
- how to draft reports to be used in court
- best practices on cooperation.

Annex H: Example of segregation of duties (SoD) matrix

Activities of crime	CSIRTs	LEAs	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
<i>Prior to incident/crime</i>					
<i>Delivering/participating in training</i>					<i>Problem-solving and critical thinking skills</i>
<i>Issuing recommendations for new vulnerabilities and threats</i>					<i>Knowledge of cyber threat intelligence landscape</i>
<i>During the incident/crime</i>					
<i>Discovery of the crime</i>					<i>Digital investigations; forensics tools; penetration testing; vulnerability scanning</i>
<i>Identify the type and severity of the compromise</i>					<i>Knowledge of cyber threats and incident response procedures</i>
<i>Evidence collection</i>					<i>Knowledge of what kind of data to collect; organisation skills</i>
<i>Providing technical expertise</i>					<i>Technical skills</i>
<i>Preserving the evidence that may be crucial for the detection of a crime in a criminal trial</i>					<i>Digital investigations; forensics tools;</i>
<i>Duty to report a cybercrime to law enforcement (LE)</i>					<i>Obligations and restriction on information sharing; communication channels</i>
<i>Duty to inform the victim of a cybercrime</i>					<i>Obligations and restrictions to the information sharing</i>
<i>Acting as a single point of contact (PoC) for any communication with other EU Member States</i>					<i>Communication skills;</i>

					<i>communication channels</i>
<i>Undertake the investigation of an incident</i>					<i>Well-prepared & well-organised to react promptly in an incident</i>
<i>Deciding the leads to follow, the targets to work on. Identifying the legal framework</i>					<i>Knowledge of the legal framework; decision-making skills</i>
<i>Lead of criminal investigation</i>					<i>Knowledge of the incident response plan; leadership skills</i>
<i>In the case of disagreement, the final say for an investigation</i>					<i>Knowledge of the legal framework; decision-making skills</i>
<i>Post incident/crime</i>					
<i>Systems recovery</i>					<i>Technical skills</i>
<i>Protecting the constituency</i>					<i>Drafting and establishing procedures; technical knowledge</i>
<i>Preventing and containing IT incidents from a technical point of view</i>					<i>Technical skills pertaining to system administration, network administration, technical support or intrusion detection</i>
<i>Investigating and judging who committed a crime</i>					<i>Technical knowledge and knowledge of the legal framework</i>
<i>Assess incident damage and cost</i>					<i>Evaluation skills</i>
<i>Review the response and update policies and procedures</i>					<i>Knowledge how to draft an incident response and procedures</i>





ENISA

European Union Agency for Network
and Information Security

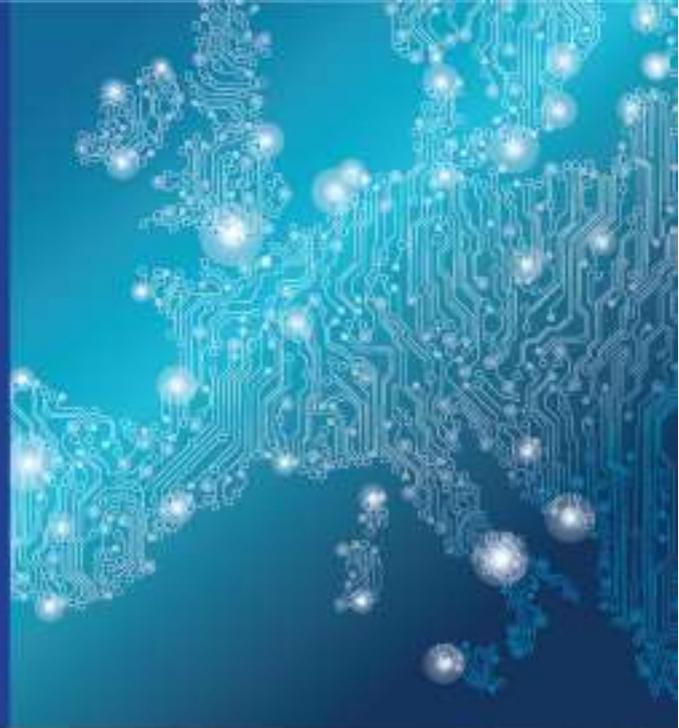
1 Vasilissis Sofias

Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)

Vassilika Vouton, 700 13, Heraklion, Greece



Catalogue Number: TP-06-18-246-EN-N



1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece

Tel: +30 2814409710

info@enisa.europa.eu

www.enisa.europa.eu

ISBN: 978-92-9204-259-2

DOI: 10.2824/274312

