Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects

VERSION 1.0

NOVEMBER 2017

www.enisa.europa.eu

European Union Agency For Network and Information Security

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 EU citizens. 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.

Contact

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

Acknowledgements

ENISA would like to thank:

- The subject-matter experts, selected from the List of NIS Experts compiled following the ENISA Call for Expression of Interest (CEI) (Ref. ENISA M-CEI-17-T01), who *ad personam* 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:
  - Italian National CERT (IT-CERT), Italy
  - Aljoša Špeh, Computer Crime Investigation Unit, Police Directorate Koper, Police Slovenia
  - Elena Vidotto and Diego Marson, Yarix s.r.l., Italy

- All CSIRT and law enforcement respondents to the online survey conducted to collect data for this report as well as EC3 EUROPOL's colleagues for their support to distribute the survey to the law enforcement community

- The subject-matter experts/organisations who performed peer-reviews of the report or parts of it, including:
  - Team CIRCL - Computer Incident Response Center Luxembourg
  - EC3 EUROPOL
  - Alexander Seger, Council of Europe

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

ISBN: 978-92-9204-229-5, doi:10.2824/451887

Table of Contents

Executive Summary

As it has been stated in the recent 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, p. 13), "Finding useful information for cybercrime investigations, mostly in the form of digital traces, is a major challenge for law enforcement authorities". Collaboration between Computer Security Incident Response Teams (CSIRTs) and Law Enforcement Agencies (LEAs) is key for finding such information and for fighting against cybercrime.

A number of attacks that recently hit critical sectors brought an increased level of cooperation, partly out of necessity, Wannacry (ENISA, 2017a) and 'NotPetya' (an updated version of Petya) attacks (Europol, 2017a) being the most recent examples. The legal and organisational aspects are an important component for the cooperation.

This report aims to support the cooperation between CSIRTs - in particular national/governmental CSIRTs - and LEAs in their fight against cybercrime, by providing information on the legal and organisational aspects, identifying current shortcomings, and formulating and proposing recommendations on legal and organisational aspects to further enhance the cooperation.

The data for this report was collected via desk research, interviews with subject-matter experts, and an online survey.

The data collected confirmed that CSIRTs and LEAs often exchange information during the incident handling/investigations, both formally and informally, and that trust is the key success factor for the cooperation. However, it is clear 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 in terms of the effectiveness to fight crime.

Core recommendations to improve legal and organisational aspects of the cooperation in particular between national/governmental CSIRTs and LEAs include:

- CSIRTs and LEAs should **place liaison officers on both ends and** ENISA should **propose ways to facilitate the liaison officers' coordination;**
- CSIRTs and LEAs, with the support of ENISA and Europol's EC3, should **formalise intelligence exchange;**
- CSIRTs and LEAs should **adopt and use simplified standardised forms for data requests and simplified standardised procedures for their information sharing**;
- National/governmental CSIRTs and national law enforcement training centres, with the support of ENISA and Europol's EC3, should **further invest in CSIRT-LEA training and skills development;**
- Member States, ENISA and Europol's EC3 should **further invest in networking events and trust-relationships between CSIRTs and LEAs**;
- ENISA should **analyse the implementation of the NIS Directive and the application of GDPR focusing on successes as well as challenges to ensure that shortcomings are addressed;**
- Member States should **clearly identify which information CSIRTs and LEAs are allowed/obliged to share between them under the current legal framework;**
- Member States should **have in place legislation that well define under which conditions CSIRTs and LEAs are allowed/obliged to share and accountability when they share, as well as reflect on turning information sharing between (national) CSIRTs and LEAs mandatory;**

- Member States, with the support of ENISA, should **promote a culture of information sharing between CSIRTs and LEAs within the country and cross-border**;
- Member States, ENISA and Europol's EC3, should **promote the improvement of maturity of LEAs and CSIRTs in order to better facilitate the information exchange**;
- CSIRTs and LEAs should **develop internal security policies permitting and supporting information sharing with CSIRT/LEAs counterpart**;
- CSIRTs, with the support of ENISA and Europol's EC3, should **make available and** LEAs **take advantage of CSIRTs dataset, expertise and contacts**.

In parallel to this report, ENISA has published a complementary report on *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement* (ENISA, 2017), which focuses on technical aspects and which is available on the ENISA website.

1. Introduction

1.1 Purpose

The purpose of this report on *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* is to understand the legal and organisational aspects of the cooperation between Computer Security Incident Response Teams (CSIRTs) and Law Enforcement Agencies (LEAs), including of their communication.

While this report focuses on the legal and organisational aspects, some considerations are also made about the technical aspects. However, the technical aspects of this cooperation are addressed in more detail in the ENISA report on *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement* (ENISA, 2017).

1.2 Background of the Report

The ENISA Programming Document 2017-2019 (ENISA, 2017b) includes “Objective 4.2. - CSIRT and NIS community building”. Under Objective 4.2, “Output 4.2.1 - 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. CSIRT, law enforcement, European FI-ISAC) to enhance mutually satisfactory ways to collaborate and support good practices among different stakeholders in operational communities in Europe” (ENISA, 2017b, p. 52).

This report contributes to the implementation of Output 4.2.1, in particular to what is foreseen as “Further improvement of communication between CSIRTs and LEA (based on 2011 report ‘Flair for Sharing’)” (ENISA, 2011a).

1.3 Report Objectives and Scope

1.3.1 Report Objectives

The main objectives of this report are to:

- Provide information on legal and organisational aspects of the cooperation between CSIRTs - especially national/governmental CSIRTs - and LEAs, in particular of their communication;
- Identify current[1] challenges - mainly legal and organisational ones - that CSIRTs and LEAs face in their cooperation to fight against cybercrime;
- Formulate and propose recommendations to enhance mutually satisfactory ways of cooperation, including communication, within the current legal framework and to further improve, if needed, the legal framework for the cooperation and the organisational aspects of it.

1.3.2 Report Scope

The geographical coverage of this report is limited to the EU (European Union, 2017) and EFTA (EFTA, n.d.)[2] countries. This does not mean however that all these countries are covered in the report and that no reference to other countries outside EU and EFTA is made therein.

[1] Cut-off date for this report: 1 November 2017.

[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.

The report does not target a specific sector; considerations made can apply to cooperation between CSIRTs and LEAs to fight against cybercrime in all sectors (from finance to energy, from transport to health).

The area of the fight against terrorism is outside the scope of this report, although many of the developed considerations can be extended to it.

Concerning CSIRTs, the report focuses in particular on national/governmental ones.

1.4 Target Audience

The intended target audience are CSIRTs - mainly national/governmental CSIRTs but not limited to them -, LEAs, and in general public and private organisations with an interest in NIS.

Additionally, policy and law makers may benefit from select aspects of analysis as well as recommendations of this report, as they prepare policies and legislation for the purpose of enhancing the cooperation between the two important communities in fighting cybercrime, being CSIRTs and LEAs.

1.5 Key Concepts and Definitions

In the context of this report, the following definitions – below 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 need to be overcome/removed, and where determination is required" (Portesi, 2008). In this report challenges – as well as the aspects of the cooperation - are grouped in "legal", "organisational" and "technical".
- **Classification** (of events or incidents) "is designed to group related things together and to define the relationship these things have to each other [… (ENISA, 2011b)]. In addition, classification is the repartition of events and incidents into classes, not to be confused with the level of classification of a document [… (ENISA, 2015a)]" (ENISA, 2016a, p. 59).
- **Communication** in most cases refers to the information sharing between CSIRTs and LEAs. Sometimes the term "communication" is also used in its legal sense of "policy document with no mandatory authority" (European Judicial Network, n.d.), 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 LEAs.
- **Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT)** is "an organisation that studies computer and network security in order 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** here are synonymous in this document. They refer to the joint work of CSIRTs and LEAs, their coordination of actions, their reciprocal help and their joining efforts to fight against cybercrime.
- **Criminal investigations** "refers to the investigatory phase beginning with a police officer becoming aware of the fact that criminal activity is going to be committed or has been committed and it ends when the case is solved" (Portesi, 2008, p. 109) and/or closed.
- **Cybercrime** is an umbrella term. An unequivocal definition of cybercrime does not exist. In general we refer by it to "Any offense 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, 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).

- **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 as well as to ensure cyber-crisis management" (ENISA, 2015c, p. 9).
- **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, 2016a).
- **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, 2016a).
- **Law enforcement** and **Law Enforcement Agencies (LEAs)** are terms used in this report as synonymous and they refer to "agencies responsible for maintaining public order and enforcing the law, particularly the activities of prevention, detection, and investigation of crime and the apprehension of criminals" (BJS, n.d.)
- **Legal aspects** refer to the dimensions of the CSIRT-LEA cooperation 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.
- **Malware Information Sharing Platform** (MISP) is an "Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing" (MISP, 2017) and it is "a combination of a community of members, a knowledge base on malware and a web-based platform" (NATO NCI Agency).
- **Methodology** is a term used in this report with two main meanings. First, in its meaning in research, it refers to which kind of data are collected (e.g. qualitative or quantitative) and how (i.e. methods of data collection; see for example Chapter 2 - Methodology). Second, in the sense of ways how CSIRTs and LEAs share information in their joint effort to fight against cybercrime.
- **National CSIRT:** 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).
- **National cyber security strategy** or **national strategy on the security of network and information systems** refers to the "framework providing strategic objectives and priorities on the security of network and information systems at national level" (European Parliament and Council of the European Union, 2016a).
- **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, pursuant to 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, 2016a).
- **Organisational aspects** refer to those dimensions of the CSIRT-LEA cooperation 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.).

- **Standard**: in a very broad sense means refers to something normally used or widely accepted. “In simple terms, a standard is a document that provides rules or guidelines to achieve order in a given context” (ETSI, n.d.). “Standards are produced for many different products and services, and may be created for company, national, regional or global application. They may be used on a voluntary basis, or made mandatory by company policy, national or international regulation, or by law.
  In Europe there are three different categories of standard:
  - international standard – a standard adopted by an international standardisation organisation
  - European standard – a standard adopted by a European standardisation body
  - national standard – a standard adopted by a national standardisation body and made available to the public” (ETSI, n.d.).
- **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-LEA cooperation that relate to the tools (e.g. applications, the platforms) and the methodologies used by CSIRTs and LEAs to share information in their effort to fight against cybercrime.
- **Traffic Light Protocol (TLP)** “is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs). The TLP can be used in all forms of communication, whether written or oral. […] The TLP is in principle easy to use: the sharer of information tags the information with a colour. Tagging information consists simply of adding “TLP:COLOUR” [Red, Amber, Green, White] on a document or part of it. The meaning of the colour indicates the possibilities for further spreading of the information. Over the years, different wordings of the TLP have surfaced, but the CSIRT community recently made an effort to clarify the TLP.” “Since the TLP’s use is ubiquitous in certain communities, it would be easy to think that it is the ultimate solution for sharing information. It is not. The TLP’s use of four categories is simple, if not simplistic. There will always be cases where it is not suited to the situation at hand. For example, a presentation in a meeting of representatives of CSIRTs could be TLP:RED for most of them, except for the one team present who is able to act on the information, for whom TLP:AMBER would be more suitable. It is possible to build more complicated examples ad libitum, where the only way out is old-fashioned, extensive, distribution lists. This does not mean that the TLP is useless. On the contrary, its simplicity and universality make it ideal for many real-life situations. It is just not a silver bullet” (ENISA, n.d.).

2. Methodology

To collect data for this report mainly a qualitative methodological approach has been adopted: indeed, due to the rather new field addressed, primarily qualitative research has been conducted, in other words a "Research for the purpose of developing "sensitizing concepts" [- which are "directions along which to look" (Blumer, 1954, p. 7) -] and verstehen (understanding) rather than quantitative measurement" (Hagan, 1997, p. 510).

However, some quantitative data has also been collected: an online survey has been conducted to validate and complement the findings from the desk research and the interviews. The quantitative research carried out allowed the collection of some "data in the form of numbers" and produced some simple "Descriptive statistics that includes frequency distributions such as rates, proportions, and percentages as well as graphic representations of data such as pie charts […and] bar graphs" (Bayens & Roberson, 2011, p. 25).

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 also for drafting of the questionnaire to support the interviews.

In addition to the material listed in Chapter 6 - Bibliography/References, examples of sources consulted and of material reviewed collected during the desk research can be found in Annex D: Samples of Material Collected During the Desk Research Not Included in the Bibliography/References.

A supplementary desk research was conducted to address 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 areas such as incident handling, information sharing taxonomies, information sharing tools and platforms, information sharing groups and initiatives, legislation and policies.

The findings from the desk research were particularly useful also for the drafting of the questionnaire to support the interviews.

2.1.2 Interviews

Structured interviews were conducted with four CSIRT representatives from three Member States and with five LEA representatives from three Member States. The interviews were conducted during the period from May 2017 and July 2017. They were mainly conducted via phone and they lasted each around ninety minutes. 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.

Two questionnaires were prepared to support the interviews, one for the interviews with the CSIRTs, one for the interviews with the LEA (see Annex B: Samples of Questionnaires to Support the Interviews). Some questions were open questions; most were yes/no questions. For all questions, including yes/no, interviewees could add comments and additional information.

May-June 2017 was a particularly challenging period to meet interviewees availably, not least because of their engagement in responding to incidents such as WannaCry and 'NotPetya' ransomware attacks.

Some data collected for the report on technical aspects mentioned above were also used to complete and validate the data collected for this report.

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 eight questions (see Annex C: 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. Several rounds of testing took place. The estimated time to fill in the online survey was less than ten minutes.

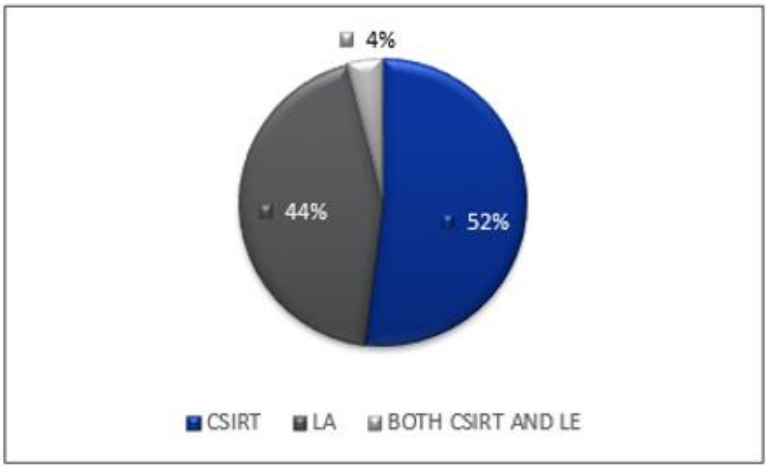
The survey was developed by using the EUSurvey, a survey tool which is "supported by the European Commission's ISA programme, which promotes interoperability solutions for European public administrations" (European Commission, n.d. a).

The invitation to fill the survey was sent to the closed ENISA mailing list of European national and governmental CSIRTs, which includes around forty-five teams. In addition, it was sent via Europol 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" (Council of the European Union, 2017a, p. 13).

The survey was launched in August 2017 and was open for around two weeks. The data collected via the online survey was used to validate the data collected through the desk research and interviews and also to produce some simple statistics.

Twenty-five replies were received: thirteen respondents were from CSIRT community, eleven from the law enforcement community and one belonged to both areas. An overview of the composition of the respondents based on the community they belong to is presented hereinafter in Figure 1.

Figure 1 – Overview of Respondents to the Online Survey Based on the Community They Belong to



Twenty-three respondents were from nineteen of the twenty-eight EU Member States (European Union, 2017), two respondents were from EFTA countries (EFTA, n.d.).

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

2.1.4 Data Used to Develop the Recommendations

The recommendations in Chapter 5.2 have been developed based on research findings and the results of this report as well as of the parallel ENISA report on *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement* (ENISA, 2017).

2.2 Selection and Classification of the Stakeholders

This research was carried out in order to understand how the cooperation, in particular communication, between the two mentioned communities can be further improved. This is aimed at supporting the fight against cybercrime and collaboration between CSIRTs and LEAs, as envisaged by the ENISA Programming Document 2017-2019 (ENISA, 2017b).

The stakeholders selected for the interviews were:

- First, CSIRTs, mostly, national CSIRTs and governmental CSIRTs. However, in order to better understand how communication between CSIRTs and LEAs really works, some CSIRTs have been interviewed, which were neither national CSIRTs nor governmental CSIRTs;
- Second, LEAs, in particular national LEAs from different European Union countries, were interviewed. However, some local LEAs were also interviewed for a better understanding of the local realities.

The key stakeholders for this report are all CSIRTs and LEAs exchanging data between each other. Additional report recipients are legislators and all those who can define policies and procedures for improving communication between CSIRTs and LEAs.

2.3 Contribution by Subject Matter Experts

ENISA selected four external subject-matter experts from the List of NIS Experts compiled following the ENISA Call for Expression of Interest (CEI) (Ref. ENISA M-CEI-17-T01), who contributed to this report *ad personam* by supporting the data collection and analysis. These experts contributed *inter alia* to the report with their legal expertise in NIS (including but not limited to policy monitoring activities, legal framework relevant to the information sharing, and digital forensics) and their expertise in NIS aspects of cybercrime and in incident response.

In addition to ENISA internal reviewers and project team reviewers, some external experts/organisations peer-reviewed this report (or part of it) and their feedback were incorporated in the final draft.

3. Overview of the Policy Context

3.1 Some General Remarks Regarding the Cooperation between CSIRTs and LEAs

Below follow some preliminary remarks related to the context surrounding the cooperation between CSIRTs and LEAs to fight against cybercrime.

3.1.1 Not all Incidents Are Cybercrimes and Not All Cybercrimes Are Incidents

In the absence of an unequivocal definition of cybercrime, in general by it we can refer both to crime having a computer as a target and crimes where computer is a tool to commit traditional or news crimes.

By "incident" is meant "any event having an actual adverse effect on the security of network and information system" (Article 7 (7) of the NIS Directive (European Parliament and Council of the European Union, 2016a)).

On the one hand, there might be accidental unforeseeable events that have an adverse effect on the security of a system and that can be considered as incidents. However, because they are not intentional and could not be even foreseen, in principle, they cannot be considered as a cybercrime. On the other hand, crimes where computer is merely a tool (e.g. storage of illegal images on a computer or using a computer to plan a murder) can be considered in a broad sense as cybercrime, but they are not defined as incidents.

3.1.2 Cooperation between CSIRTs and LEAs Does Not Take Place for All Cybercrime Cases

There are some cases where cooperation between CSIRTs and LEAs does not take place. For example, because the crime under police investigations involves computers but it is not an incident (see 3.1.1). The other example is when an incident is not reported as a crime, for instance, because the victim is afraid of possible reputational damages, or does not know how and to whom to report it.

3.1.3 CSIRT and LEAs are Different as Well as Their Objectives

CSIRTs focus on preventing and mitigating incidents and, as highlighted in previous ENISA's studies CSIRTs "compared to the investigatory character of LEAs […] [CSIRTs] operate on an informal basis [see (ENISA, 2011a)], which allegedly permits them to be agile in their response" (ENISA, 2012, p. 27). By comparison, LEAs are generally bound by a formal procedural approach of following rules and a hierarchical authority for the purpose of supporting criminal investigations and the producing evidence to be used before a Court of Law. This is partly due to the different objectives that each community is trying to achieve but it is also bound up with discreet features of each community. LEAs are for instance driven by Penal Law procedures because of the sort of standards that pervade their work (e.g. in maintaining the evidential chain, motivating and often justifying decisions, adhering to the framework concerning the rights of investigated parties, etc.) (ENISA, 2012, p. 27). When investigations end before a court, a clear path is required to justify the way evidence has been collected in a way that and legal objections of the suspect and her defence can be successfully confronted. Apart from that, LEAs work as any other hierarchical organization where usually justification of decisions may need to take place.

3.1.4 CSIRTs and LEAs, and Other Actors

CSIRTs and LEAs are not the sole actors when it comes to cope with cybercrime. Their cooperation in fighting cybercrime is accompanied by other actors and usually there is also interaction of CSIRTs and LEAs with other entities, there are several other actors that are part of the scene, such as:

- The **criminal** - or more correctly as far as he/she is not sentenced - the **suspect**;
- The **victim**, which can be an individual, a company, or a private organisation;

- The **judiciary**, in other words, public prosecutors and judges who come to play their important role in cases where the conditions to prosecute are met;
- The **telecommunication operators**;
- The **internet service providers**;
- The **systems and network administrators** (e.g. of the victim, of third persons or even of the criminal), that might have important pieces of information to support not only the incident handing but also the crime investigation;
- The **IT security companies**, that provide information and solutions, in some cases even in real time during the incident mitigations and criminal investigations;
- The **insurance companies**, with which the victims might have stipulated insurances to cover cybercrime damages;
- The **national cyber security authorities** (e.g. cyber security centres);
- The **intelligence community**;
- The **military**;
- The **subject-matter experts** who might belong to one of the organisations mentioned in this list or may act as individuals;
- The **CSIRTs Network** that as provided in Article 12 of the NIS Directive (European Parliament and Council of the European Union, 2016a) is “composed of representatives of the Member States' CSIRTs and CERT-EU” and **other national, supranational and international CSIRTs networks, ISACs and *fora*** (e.g. FIRST, TF-CSIRT, and European FI-ISAC);
- The **malware and threat information sharing groups**, including MISP project (MISP Project, n.d.).
- **ENISA** that provides the Secretariat of the CSIRTs Network and actively supports the cooperation among the CSIRTs and, together with Europol’s EC3, the cooperation between CSIRTs and LEAs;
- **Europol’s European Cybercrime Centre (EC3)** set in 2013 by Europol “to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime” (European Cybercrime Centre - EC3, n.d.);
- The **international law enforcement agencies**, including INTERPOL (INTERPOL, n.d.);
- **Academia**;
- **Other stakeholders**, for instance, subjects other than those mentioned above that might be affected by the incident handling/cybercrime response: examples are clients of the victims (for instance when the victim, for instance a bank or an electricity company, provide services) or other subjects somehow sharing – even involuntarily and unaware of the crime – hardware and software with the criminal.

3.1.5 Variety of CSIRTs, LEAs, and Ways of Cooperating

Services offered, consistency, size and maturity level vary considerably from CSIRT to CSIRT.

National and governmental CSIRTs play particularly important roles: “Currently in the EU, governmental CSIRTs are typically used to protect the cyberspace of governmental institutions including critical infrastructure as well as to ensure cyber-crisis management. National CSIRTs, on the other hand, are playing different roles in different countries. In some countries they are responsible for the whole IP address space of that country, in others they also take the role of ‘last resort’ when no security contact point for an IP address can be found. In any case, when another country has to be contacted regarding solving an incident, national CSIRTs are often asked to help to find the right contact person. Increasingly CSIRTs expect other teams with comparable competences to react to their requests in a timely manner and to handle shared information professionally” (ENISA, 2015c, p. 9).

In many European countries there are also sectorial CSIRTs. They handle incidents and assist in particular critical sectors (e.g. finance, health, energy). Their constituency is about the sector as a whole.

Like for CSIRTs, there are many kinds of LEAs. For instance, there are local, federal, national, supranational and international LEAs. Also responsibilities and powers might vary from LEA to LEA. There are LEAs that are specialised in cybercrime investigations. Also size and resources of LEAs might be quite different from LEA to LEA and, in general, depending on the country.

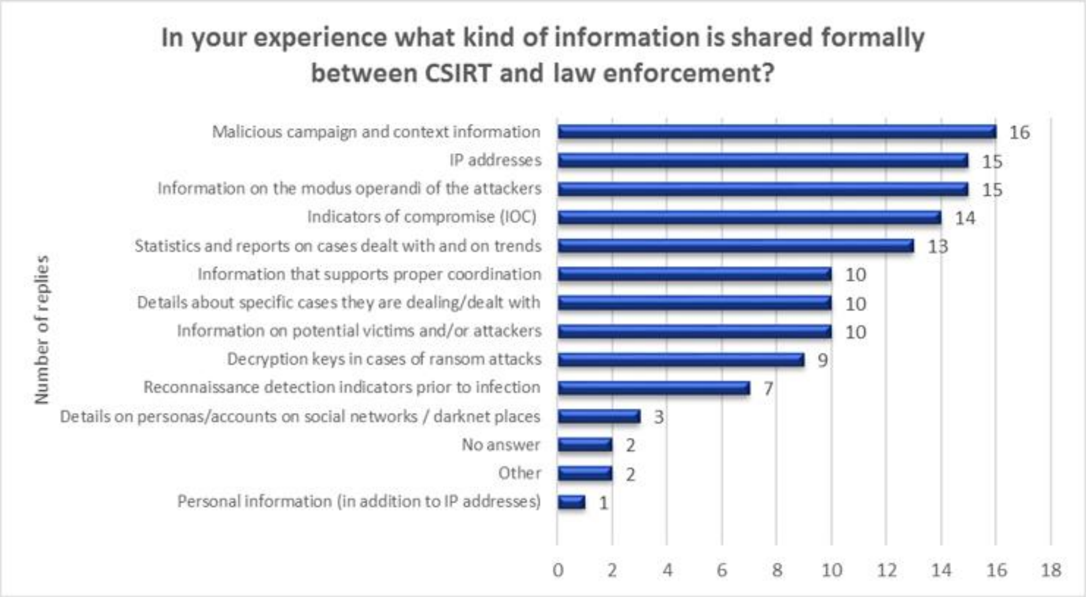
The overall cooperation between CSIRTs and LEAs is affected by the type of CSIRT and LEA involved, and whether liaison officers are appointed or not.

CSIRTs and LEAs share information both formally (e.g. in the context of an official written request for information regarding a specific case) and informally (e.g. when information is shared orally during an informal phone call). Both formal and informal channels require a legal basis and either type of information sharing between CSIRTs and LEAs need to be in line with applicable legislation.

The level and sophistication of information shared depends also on the level of formalisation of the cooperation between CSIRTs and LEAs.

According to the results from the online survey shown in Figure 2, CSIRTs and LEAs share mainly three types of information: malicious campaign and context information, IP addresses, and information on the *modus operandi* of the attacker and indicators of compromise (IOC).

Figure 2 - Information Shared Formally between CSIRTs and LEAs according to the Online Survey



In addition to formal information sharing, CSIRT and LEAs share information informally.

According to the results from the online survey shown in Figure 3, most information shared informally are indicators of compromise (IOC), malicious campaigns and context information, IP addresses, statistics and reports on cases dealt with and on trends, and information on *modus operandi* of the attacker.

Figure 3 - Information Shared Informally According to the Online Survey

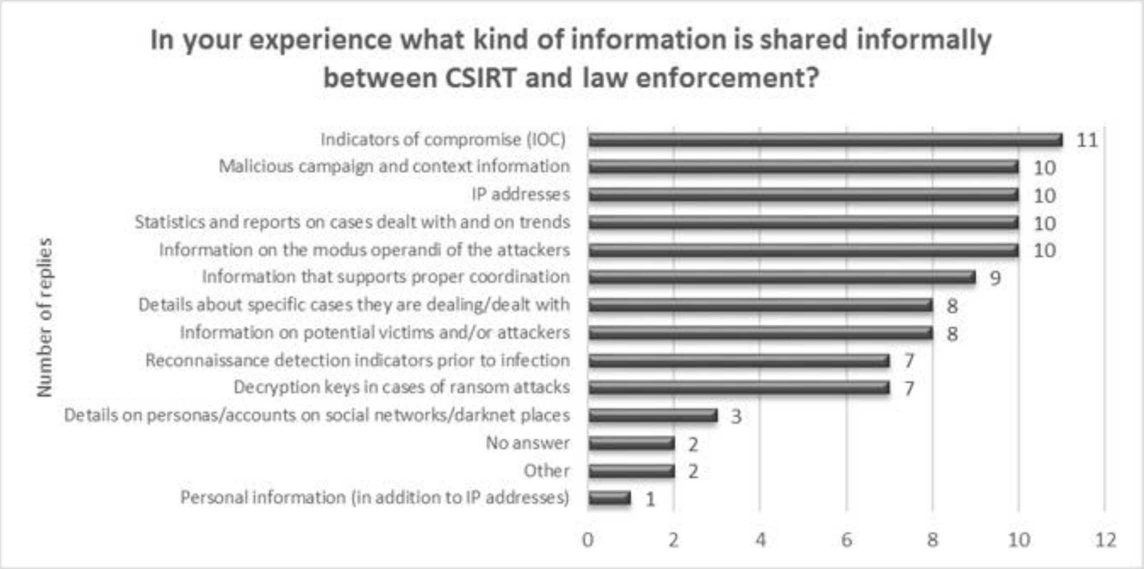
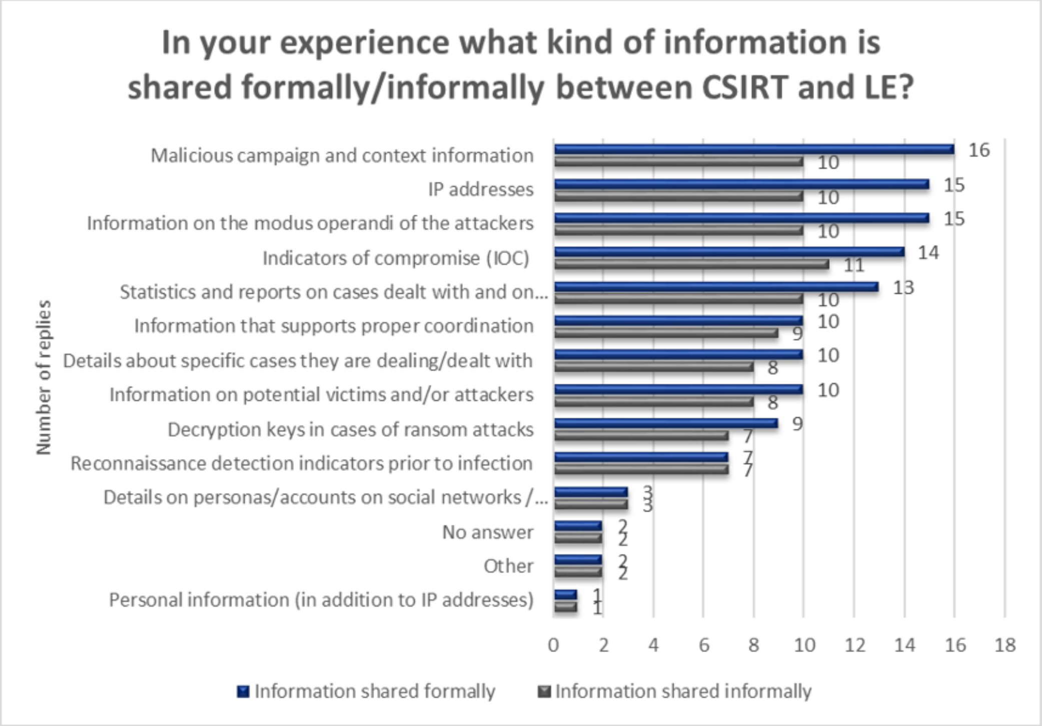


Figure 4 provides some compared data regarding which data are shared formally and informally.

Figure 4 - Comparison Between Kind of Information Shared Between CSIRTs and LEAs Formally and Informally, According to the Data Collected Via the Online Survey



According to the data collected via the online survey, personal information (other than IP addresses) does not often seem to be the object of information sharing between CSIRTs and LEAs, neither formally nor informally.

According to the data collected via the interviews, two different levels of cooperation between the CSIRTs and LEAs can be identified:

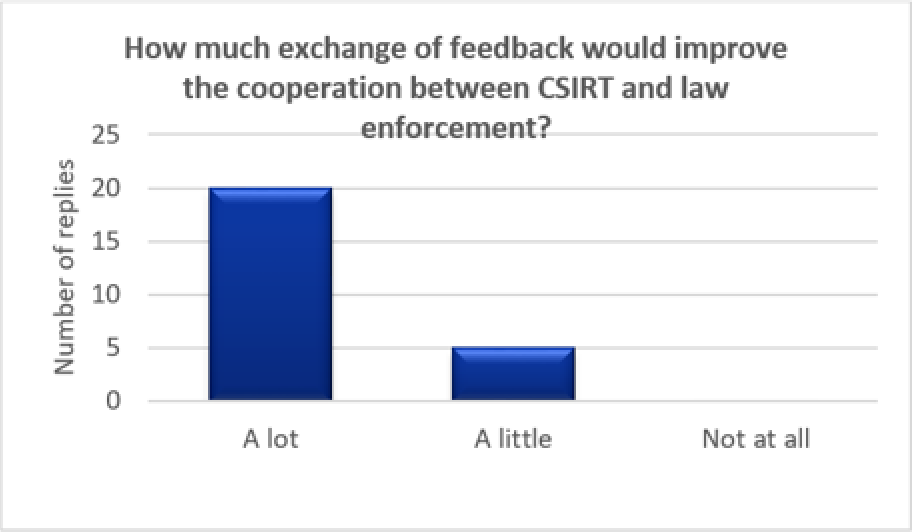
- A cooperation at higher level via the liaison officer (when there is a liaison office). At this higher level the general framework of the cooperation is set but the actual materialisation of this framework is often *ad hoc*, depending on the case
- *Ad hoc* specific cooperation is the cooperation between the CSIRT and LEA personnel working on the specific case dealt with

Level of formalities might also vary depending on the level of cooperation and on the country. The second level of cooperation is almost always facilitated by the liaison office, if present, and a result of the first level of cooperation.

3.1.6 Importance of Reciprocal Feedback

As it emerged both from the interviews and the online survey, feedback represents an important element to improve the cooperation between CSIRTs and LEAs. See Figure 5.

Figure 5: Overview of How Much Feedback Would Improve the Cooperation Between CSIRT and LE, According to the Data Collected Via the Online Survey



3.2 Main Legal and Policy Framework for the Cooperation between CSIRTs and LEAs

The legal and policy context plays an important role in governing and shaping the cooperation between CSIRTs and LEAs in fighting against cybercrime. The section hereinafter describes some of the most relevant international and EU legislation and policies in the field.

It is worth mentioning the need for technology-neutral laws. On the one hand, the cybercrime landscape is changing very fast; on the other hand, it usually takes a long time to create a piece of legislation, especially in the case of international law. This is why it is extremely important to create such legislative solutions which will be efficient not only today, but also in five and ten years' time or more.

3.2.1 Council of Europe Convention on Cybercrime ("Budapest Convention")

The Council of Europe (CoE) (Council of Europe, n.d.) was established in 1949 to uphold and strengthen human rights, democracy and the rule of law within Europe. The Council consists of forty-seven Member States, including all the Members of the European Union.

In 1995 the CoE presented a report concerning the adequacy of criminal procedures laws in the area of computer-related threats and hacking. Following this initiative, in 1997 the Committee of Experts on Crime in Cyberspace was established to prepare a convention which could facilitate international cooperation in the investigation and prosecution of computer crimes. The Convention on Cybercrime was opened for signature in Budapest, Hungary, in November 2001.

The Convention on Cybercrime (ETS No. 185) (Council of Europe, 2001) (Council of Europe, n.d. a), also called the "Budapest Convention", is the first international treaty and remains the most relevant international treaty on cybercrime and electronic evidence. It requires Parties to criminalise offences against and by means of computers in their domestic criminal law (Articles 2 to 11), to provide their law enforcement with the necessary powers to secure electronic evidence not only in relation to cybercrime but any crime entailing evidence on a computer systems (Articles 16 to 21) – while making these powers subject to rule of law safeguards (Article 15), and to engage in international cooperation on cybercrime and electronic evidence (Articles 23 to 35).

The Cybercrime Convention Committee (T-CY) representing the Parties to this treaty assesses the implementation of the treaty, issues Guidance Notes and may also prepare additional protocols to the Convention. The European Union (including the European Commission and the Council of the European Union, Eurojust, Europol and ENISA) are observers in this Committee.

The Convention is not only open to the Members of the CoE but any country committed and able to implement this treaty may accede. By October 2017, fifty-six States – European countries but also Australia, Canada, Chile, Costa Rica, Dominican Republic, Japan, Senegal, Sri Lanka, USA and others – had been Parties and a further fourteen had signed it or been invited to accede. All EU Member States had signed the Convention, and all except for two had also ratified it. The Chart of signatures and ratifications of the Convention is available on the Council of Europe website (Council of Europe, n.d. b).

The Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No.189) of 28 January 2003 "entails an extension of the Cybercrime Convention's scope, including its substantive, procedural and international cooperation provisions, so as to cover also offences of racist or xenophobic propaganda. Thus, apart from harmonising the substantive law elements of such behaviour, the Protocol aims at improving the ability of the Parties to make use of the means and avenues of international cooperation set out in the Convention […] in this area" (Council of Europe, n.d. c).

As also mentioned in the recent 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), "A possible addition of a protocol to the Convention is now being explored [(Council of Europe Cybercrime Convention Committee, 2017)], which could also provide a useful opportunity to address the issue of cross-border access to electronic evidence in an international context. Rather than the creation of new international legal instruments for cybercrime issues, the EU calls for all countries to design appropriate national legislation and pursue cooperation within this existing international framework". The negotiation of such a Protocol commenced in September 2017 and is expected to be completed by December 2019.

3.2.2 Directive on Attack Against Information Systems

The Directive on attacks against information systems (European Parliament and Council of the European Union, 2013), replacing Council Framework Decision 2005/222/JHA (Council of the European Union, 2005), entered into force in August 2013 and its implementation deadline was in September 2015. This Directive integrated elements of the Council of Europe Convention on Cybercrime (Council of Europe, 2001).

The Directive was an important step in the EU's effort to create the European rules to combat cybercrime. According to the Directive there are four main substantive offences (together, the "Substantive Offences") of:

- Illegal access to information systems
- Illegal system interference
- Illegal data interference; and
- Illegal interception.

The Directive also increases the cooperation between competent authorities to enable a response to urgent information requests with a response time of no more than eight hours and also to monitor and record statistical data and report on cybercrime offences and criminal convictions.

As foreseen according to the Directive, the European Commission has compiled a report assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive. This report was published on 13 September 2017 (European Commission, 2017a).

3.2.3 Europe 2020, the Digital Agenda for Europe (DAE), Digital Single Market Strategy for Europe (DSM), and the Cyber Security Strategy (CSS)

3.2.3.1 Europe 2020

In June 2010, ten-years strategy *EUROPE 2020 A strategy for smart, sustainable and inclusive growth* (European Commission, 2010a) from the European Commission was issued. It sets objectives for the growth of the European Union. One of the pillars was the Digital Agenda.

3.2.3.2 Digital Agenda for Europe

Launched in May 2010, *A Digital Agenda for Europe* (DAE) (European Commission, 2010b) is the action plan for Europe for making the best use of information and communication technologies (ICT) so that the sustainable digital future could be build. The main goal of the document was to take actions which will remove obstacles to maximising the potential of ICTs, with long-term investments to minimise future problems. The Digital Agenda "is aimed at boosting Europe's economy by delivering sustainable economic and social benefits from a digital single market" (European Commission, 2014).

3.2.3.3 Digital Single Market Strategy for Europe (DSM Strategy)

Creating the Digital Single Market is one of the seven goals of the Digital Agenda. As the continuation of this policy, in May 2015, *A Digital Single Market Strategy for Europe* (European Commission, 2015a) was adopted. It contains a number of initiatives, the implementation of which should open up digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy.

There are three pillars of the DSM Strategy:

1. Better access for consumers and business to online goods (helping to make the EU's digital world a seamless and level marketplace to buy and sell)

2. The right environment for digital networks and services (designing rules which match the pace of technology and support infrastructure development)
3. Economy and Society (ensuring that Europe's economy, industry and employment take full advantage of what digitalisation offers)

"Trust and security are at the core of the Digital Single Market Strategy, while the fight against cybercrime is one of the three pillars of the European Agenda on Security" (European Commission, 2015b). Without these two elements the European Union could not create right environment for digital economy to grow. The Commission leads a big number of projects whose aim is to boost internet trust and security.

In May 2017 the Commission has published the mid-term review of the DSM Strategy (European Commission, 2017b), which took stock of the progress made and called on co-legislators to swiftly act on all proposals already presented, as well as outlines further actions on online platforms, data economy and cybersecurity.

3.2.3.4 Cyber Security Strategy (CSS) and Joint Communication on Resilience, Deterrence and Defence

As one of the initiatives of the DSM Strategy supporting the Digital Agenda, in 2013 European Commission presented the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013). It was the first strategic document on the European level which only referred to cybersecurity. The document sets out the EU's approach on best preventing and responding to cyber disruptions and attacks. The Strategy also emphasises that fundamental rights, democracy and the rule of law need to be protected in cyberspace.

Achieving cyber resilience and drastically reducing cybercrime are given as strategic priorities and actions. To do it, it was recognised that the effective cooperation between public authorities and the private sector is absolutely crucial. The strategy also stressed that the national NIS competent authorities should collaborate and exchange information with other regulatory bodies.

In September 2017 the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented the *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). Three main goals for Europe are identified as:

1. Building EU resilience to cyberattacks
2. Creating effective EU cyber deterrence
3. Strengthening international cooperation on cybersecurity

Public-private cooperation against cybercrime is named as one of the most important activity's in the field of creating effective EU cyber deterrence. It is underlined that "cooperation with the private sector, including industry and civil society, is fundamental for public authorities to fight crime effectively" (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2017). The financial sector was pointed as an example of such cooperation (addressing online fraud and cybercrime). It is also emphasised that "private undertaking need to be able to share information on concrete incidents with law enforcement – including personal data – in full respect of data protection rules" (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2017).

The public-private cooperation in the field of fighting cybercrime accentuates the need of cooperation between LEA and CSIRT established in different sectors such as finance, energy or telecommunication. This creates new challenges, since every sector has its own specificities and CSIRT constituency might be different from sector to sector. The NIS Directive requires the establishment of CSIRTs for so called essential services operators (more about NIS Directive in the next section).

3.2.4 NIS Directive

The Directive (EU) 2016/1148 *concerning measures for a high common level of security of network and information systems across the Union* (European Parliament and Council of the European Union, 2016a) (so called "NIS Directive") was adopted in July 2016. The initial project of the NIS Directive was presented jointly with the European Cybersecurity Strategy in 2013 (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013).

The NIS Directive "lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market" (Article 1). The NIS Directive creates the culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the NIS Directive.

The NIS Directive provides obligations for all Member States to adopt a national cyber security strategy and to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems. Both the operators of essential services and the digital service providers are required to report the incidents. In addition, they are also required to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.

The NIS Directive also creates a new mechanism for cooperation among all the Member States. This cooperation will take place within the Cooperation Network, which is composed of the Cooperation Group and the CSIRTs Network. The Cooperation Group supports and facilitates strategic cooperation and the exchange of information among Member States. The CSIRTs Network supports and promotes promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks.

The CSIRTs Network already proved its effectiveness during two large scale incidents: WannaCry and 'NotPetya'.

3.2.5 Communication on Strengthening Europe's Cyber Resilience System and Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ("Blueprint")

The Communication from the European Commission on *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry* (European Commission, 2016) was presented in July 2016.

It has three goals:

1. Stepping up cooperation to enhance preparedness and deal with cyber incidents
2. Addressing challenges facing Europe's cybersecurity Single Market
3. Nurturing industrial capabilities in the field of cybersecurity

In the field of information sharing and cooperation among the Member States, the Commission decided to prepare a cooperation blueprint to handle large-scale cyber incidents on the EU level, facilitate the creation of an "information hub" to support the exchange of information between EU bodies and Member States as well as work in the close cooperation with Member States, ENISA, EEAS and other relevant EU bodies to establish a cybersecurity training platform.

Training and exercises are identified as one of the best tools to increase the cooperation between Member States, because they are the opportunity to practice and test the procedures and – if they are not efficient – to reformulate them.

In September 2017, the European Commission issued the *Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises* (European Commission, 2017c)*,* that recommends *inter alia* the following:

- "Member States and EU institutions should establish an EU Cybersecurity Crisis Response Framework integrating the objectives and modalities of cooperation presented in the Blueprint following the guiding principles described therein" (see point (1));
- "Member States should ensure that their national crisis management mechanisms adequately address cybersecurity incident response as well as provide necessary procedures for cooperation at EU level within the context of the EU Framework" (see point (4);
- "Member States should make full use of the opportunities offered by the Cybersecurity Digital Service Infrastructures (DSI) programme of the Connecting Europe Facility (CEF) [(European Commission, n.d. c)], and cooperate with the Commission to ensure that the Core Service Platform cooperation mechanism, currently under development, provides the necessary functionalities and fulfils their requirements for cooperation also during cybersecurity crises";
- "Member States, with the assistance of ENISA and building on previous work in this area, should cooperate in developing and adopting a common taxonomy and template for situational reports to describe the technical causes and impacts of cybersecurity incidents to further enhance their technical and operational cooperation during crises" (see point (7)).

3.2.6 European Agenda for Security

In April 2015 the *European Agenda for Security* for the period 2015-2020 (European Commission, 2015c) was adopted. The European Commission goal was to support Member States' cooperation in tackling security threats and step up common efforts in the fight against terrorism, organised crime and cybercrime. The Agenda sets out the concrete tools and measures which will be used in this joint work to ensure security and tackle these three most pressing threats more effectively.

Naming fighting against cybercrime as one of the three main goals, the document also confirms how important this issue has become for the whole of Europe. The international nature of cybercrime is very hard to fight and that was the reason to name reinforcing tools to fight cybercrime as the one of the key action.

3.2.7 European Investigation Order

Directive 2014/41/EU (European Parliament and Council of the European Union, 2014) concerns the European Investigation Order (EIO) in criminal matters.

The EIO is "a judicial decision which has been issued or validated by a judicial authority of a Member State ('the issuing State') to have one or several specific investigative measure(s) carried out in another Member State ('the executing State') to obtain evidence in accordance with this Directive" (Article 1).

The EIO replaces the traditional letters rogatory, freezing orders and the European evidence warrant. The mentioned Directive establishes a single investigative tool valid for any type of evidence. Therefore, the EIO may be relevant for digital evidence stored by CSIRTs of one or more other Member States that a LEA needs to gather.

The deadline for the transposition of this Directive into national law was 22 May 2017. However, the situation at 26 October 2017 is that the Directive 2014/41/EU is transposed into national laws in sixteen Member States.

3.2.8 European Public Prosecutor's Office (EPPO)

The regulation establishing the European Public Prosecutor's Office (EPPO) (Council of the European Union, 2017b) was adopted on 12 October 2017 by Member States which are part of the EPPO enhanced cooperation. So far, twenty Member States have joined such an enhanced cooperation, i.e. Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Germany, Greece, Spain, Finland, France, Italy, Latvia, Lithuania, Luxembourg, Portugal, Romania, Slovenia, and Slovakia (European Council, Council of the European Union, 2017c). The EPPO is an independent body of the EU which will be in charge of investigating, prosecuting and bringing to justice the perpetrators of offences against the EU's financial interests. The creation of the EPPO is aimed at improving transnational investigations and it is likely to play a role in facilitating the cooperation between LEAs and CSIRTs of different countries when they have to exchange data concerning offenses against the EU's financial interests.

3.2.9 EU Data Protection Legislation

3.2.9.1 Principle of EU Data Protection legislation

The main principles inspiring data protection legislation in the EU are the following:

- Article 8 (Right to respect for private and family life) of the Convention for the Protection of Human Rights and Fundamental Freedoms, also known as the European Convention on Human Rights (Council of Europe, 1950);
- Article 7 (Respect for private and family life) of the Charter of Fundamental Rights of the European Union (European Parliament, Council and Commission, 2000);
- Article 8 (Protection of personal data) of the Charter of Fundamental Rights of the European Union (European Parliament, Council and Commission, 2000);
- Article 16 (on the protection of personal data) (ex Article 286 TEC) of the Treaty on the Functioning of the European Union (TFEU) (The Member States).

3.2.9.2 General Data Protection Regulation (GDPR)

The Regulation (EU) 2016/679 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, also known as "General Data Protection Regulation" (European Parliament and Council of the European Union, 2016b), repealing Directive 95/46/EC (European Parliament and Council of the European Union, 1995), was adopted by the EU Parliament on 14 April 2016, it is already in force and, as provided in Article 99, it will apply from 25 May 2018. This new legislation was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizen's data privacy and to reshape the way organisations across the region approach data privacy (European Commision, 2017).

The GDPR is the answer to the development of modern technologies. It introduces significant changes in the EU Data protection legislation. First of all, it increases the territorial scope of the jurisdiction (it applies to all companies processing the personal data and data of subject residing in the Union). The GDPR also introduces significant penalties for companies for a breach of regulations. With the GDPR privacy by design (for more information on privacy by design see also (ENISA, 2014), which has existed so far as a concept, becomes now "essential elements in EU data protection rules" (European Commision, 2017).

With the definition of personal data as any information related to a natural person or "Data Subject", that can be used to directly or indirectly identify the person, there is also the common understanding that IP addresses are personal data. They can be directly or indirectly related to the individuals and those individuals could be identified.

Based on applicable legislation and the common interpretation, in principle also when dealing with IP addresses CSIRTs process personal data: according to the decision of the European Court of Justice on dynamic IP addresses (Court of Justice of the European Union, 2016), the IP addresses are personal data also if the data subject cannot be identified without the intervention of the third party.

According to the Article 23 of the GDPR those rules can be restricted in case of national security, defence, public security, the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding and the prevention of threats to public security. However, that creates uncertainty when personal data is processed in criminal investigations, defence, public and state security. Also the Recital 49 of the GDPR sets the legal ground for the processing of personal data by CSIRTs by affirming that: "The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, […] 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), computer security incident response teams (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."

The processing of personal data to the extent that is 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 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" attacks and damage to computer and electronic communication system.

With the GDPR regulation CSIRTs should carefully plan the collection and processing of data and information, personal data included. The CSIRT community should also avoid processing personal data which is not consistent with the purposes, processing sensitive personal data unless strictly required and sharing personal data that is not necessary or required to by law. Because of that, a close consultation and cooperation between CSIRTs and Data Protection Authorities is advisable.

3.2.9.3 Directive on Privacy and Electronic Communications

The *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector* (so called "Directive on Privacy and eCommunications") (European Parliament and Council of the European Union, 2002) as amended by Directive 2009/136/EC (European Parliament and Council of the European Union, 2009), aims to harmonise the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and to confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the European Union.

GDPR (European Parliament and Council of the European Union, 2016b) clarifies that Directive 2002/58/EC continues to apply after the adoption of the Regulation, but that once the GDPR is adopted, "Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation" (Recital 173).

There is a *Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC* (Regulation on Privacy and eCommunications) (European Commission, 2017d). The proposed regulation seeks to increase the protection of people's private life and open up new opportunities for business. Two areas of the proposal are of particular interest to this CSIRT-LE cooperation, namely:

- **Communications content and metadata**: privacy is an issue in terms of communications content and metadata, e.g. time and place of a call being made, as metadata is often relied upon to trace suspects and activities leading to the conclusion that anonymization and deletion might be privacy enhancing measures. According to the proposal processing can be carried out following consent of the parties involved, which clearly must be given at a time prior to the investigation;
- **New business opportunities**: once consent is granted for communications data (content and metadata) to be processed, telecoms operators can develop a broader set of business activities and services. In the proposed Regulation the case of heat maps indicating the presence of individuals is mentioned. Having an exact inventory of such business models along with their functionalities and impact for criminal investigations are likely to be of help to CSIRT and LE investigations.

This proposal follows the ordinary legislative procedure (ex-codecision procedure) (European Council, Council of the European Union, n.d.) (European Parliament, n.d.). The decision-making process related to this proposal can be monitored by consulting the related Procedure File (2017/0003(COD) (European Parliament, n.d. a) in the European Parliament Legislative Observatory database (European Parliament, n.d. b).

3.2.9.4 LEA DP Directive

The *Directive (EU) 2016/680 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* (referred as "LEA DP Directive") (European Parliament and Council of the European Union, 2016) repeals the Council Framework Decision 2008/977/JHA (Council of the European Union, 2008).

This Directive sets the legal basis for processing of personal data by competent authorities and law enforcement agencies in the framework of criminal investigation. According to Article 10, processing of personal data relating to criminal convictions and offences or related security measures should be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

3.2.10 Directive on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious crime

The Directive (EU) 2016/681 addresses issues related to the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (European Parliament and Council of the European Union, 2016c). Among the serious crimes, computer-related crime/cybercrime punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State is included.

Article 18 par. 1 states that “Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 25 May 2018”. The Directive (EU) 2016/681 provides that the effective use of PNR data is necessary to prevent, detect, investigate and prosecute terrorist offences and serious crime. This implies the need to process PNR data safely. For this reason, there should be CSIRTs specifically dedicated to ensuring the security of PNRs.

In addition, this Directive provides that the exchange of data between air carrier and LEA should only be carried out by means of a push method, i.e. the air carriers transfer the required PNR data to the authority requesting them, thus allowing air carriers to retain control of what data is provided. In particular, it is not recommended the use of a “pull” method, where the competent authorities of the Member State requiring the PNR data can access the air carrier's reservation system and extract a copy of the required PNR data.

3.2.11 ENISA Regulation

ENISA, the European Union Agency for Network and Information Security, was established in 2004. The Regulation (EU) No 526/2013 set out the current mandate and tasks for ENISA (European Parliament and Council of the European Union, 2013). ENISA is a “centre of expertise for cyber security in Europe” (ENISA, n.d. c). The Agency cooperates with Members States and private sector to deliver both advice and solutions. ENISA facilitates Pan-European Cyber Security Exercises (Cyber Europe), which main goal is to strengthen cooperation in the field of cybersecurity on both European and state level. Standard Operation Procedures, which were prepared during these exercises are the tool to exchange information on a European level.

Since 2013 the challenges related to network and information security have evolved. ENISA acquired also new tasks. According to the NIS Directive (European Parliament and Council of the European Union, 2016a), for instance, the Agency provides the Secretariat of CSIRTs Network.

The role that ENISA plays in the security of electronic communications is also highlighted by Proposal for a Directive establishing the European Electronic Communications Code (European Parliament and Council of the European Union, 2016d). In fact, such a proposal provides that “Competent authorities should ensure that the integrity and availability of public communications networks are maintained. ENISA should contribute to an enhanced level of security of electronic communications by, amongst other things, providing expertise and advice, and promoting the exchange of best practices” (Recital 92).

In September 2017 the European Commission presented a proposal for a new mandate for ENISA (European Commision, 2017a) (European Commission, 2017b). According to this proposal, the reformed ENISA would have a permanent stronger mandate with related adequate resources.

This proposal, submitted to the Council of the European Union and to the European Parliament, follows the ordinary legislative procedure (ex-codecision procedure) (European Council, Council of the European Union, n.d.) (European Parliament, n.d.).

3.2.12 Europol Regulation

The legal framework for the European Union Agency for Law Enforcement Cooperation (Europol) was set in Regulation 2016/794 (European Parliament and Council of the European Union, 2016e) adopted in May 2016, replacing and repealing previous Council Decisions concerning Europol (Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA). Europol assists the Member States in fight against serious international crime and terrorism.

In 2013 Europol set up the European Cybercrime Centre (EC3). EC3’s goal is to strengthen the law enforcement response to cybercrime in the EU. In fighting against cybercrime EC3 serves as the central hub for criminal information and intelligence, supports operations and investigations by Member States. It offers operational analysis, coordination and its considerable expertise, provides a variety of strategic-analysis products that enable informed decision-making at the tactical and strategic levels on combating and preventing cybercrime. EC3 supports also training and capability-building in Member States and provides technical and digital forensic support capabilities to investigate and operations.

3.2.13 Relevant ECJ Case Law

Case law from the Court of Justice of the European Union (ECJ) is also relevant for the CSIRTs and LEAs cooperation. There is case law related to the concept of personal data, jurisprudence on IP addresses and data retention.

An example is the ECJ Judgment of 6 November 2003 in *Case 101/2001 - Lindqvist* (Court of Justice of the European Union, 2003) where the Court endorsed a broad approach to the concept of personal data: "The term personal data used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, any information relating to an identified or identifiable natural person" (par. 24).

Concerning IP addresses, an important ECJ Judgement is that of the 24 November 2011 in *Case 70/10 Scarlet v. SABAM* (Court of Justice of the European Union, 2011). According to it, "an Internet Service Provider (ISP) could not be compelled to install a filtering system for all electronic communications, both incoming and outgoing, passing via its services and aimed at detecting and preventing an unlawful exchange of copyrighted works".

In its recent judgement of 19 October 2016 related to *Case 582/14 – Patrick Breyer v. Germany* (Court of Justice of the European Union, 2016), the ECJ refers to its judgement in case 70/10, by stating that "As a preliminary point, it must be noted that, in paragraph 51 of the judgment of 24 November 2011, Scarlet Extended (C-70/10, EU:C:2011:771), which concerned inter alia the interpretation of the same directive, the Court held essentially that the IP addresses of internet users were protected personal data because they allow users to be precisely identified" (par. 33) but that such "finding by the Court related to the situation in which the collection and identification of the IP addresses of internet users is carried out by internet service providers (par. 34). In Judgement in case 582/14, the Court ruled that "Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person."

Also ECJ case law in the field of data retention is relevant when discussing cooperation between CSIRTs and LEAs.

The Directive 2006/24/EC (European Parliament and Council of the European Union, 2006) - no longer in force - was related to the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amended Directive 2002/58/EC (European Parliament and Council of the European Union, 2002). The Judgment in *Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others* (Court of justice of the European Union, 2014), of 8 April 2014 of Grand Chamber, declared Directive 2006/24/EC invalid because of the breach of the principle of proportionality. This is for various reasons, including, in particular, the following:

- Directive 2006/24/EC did not require any relationship between the retained data and a threat to public security. This Directive did not foresee restrictions to a particular time period and/or a particular geographical zone. Moreover, it did not foresee restrictions to persons that could be involved, in one way or another, in a serious crime, or to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences (see par. 59).
- Directive 2006/24/EC did not provide any objective criterion aimed at determining the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences. In general, in case of offence, a national authority can interfere with the fundamental rights enshrined in Articles 7 and 8 of the Charter only if the extent and seriousness of the offence are so high to justify this. Each directive should be harmonised with the Charter (see par. 60).
- Moreover, Directive 2006/24/EC did not provide any objective criterion that could guarantee that the number of persons authorised to access and process the data retained is limited to what is strictly necessary.
- Furthermore, Directive 2006/24/EC did not provide substantive and procedural conditions about the access to the data and the related processing by the competent national authorities (see par. 61). In addition, the Directive was inadequate from the perspective of management of data retention period.
- Finally, it should be pointed out that the Directive did not establish that the acquired data are kept only in the territory of the European Union (see par. 68).

Also the Judgment of the Court of Justice (Grand Chamber) of 21 December 2016, in *Joined Cases C-203/15 and C-698/15* (Court of Justice of the European Union, 2016)*, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department (UK) v Tom Watson and Others,* has potential interest for CSIRTs who carry out the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.

The ECJ in this Judgement clarified that the measures related to the retention of data for the purpose of combating crime also fall within the scope of Directive 2002/58/EC in the light of the general structure of this Directive (see par. 73). In addition, it stated that every access of the competent national authorities to retained data requires a prior review carried out either by a court or by an independent administrative body, except in cases of validly established urgency (see par. 120).

The above mentioned ECJ case law concerns relevant issues such as IP addresses as personal data. This jurisprudence does not specifically address cooperation between CSIRTs and LEAs however it is discussed in this report as an example of case law that might be relevant also in the field of CSIRT-LE cooperation.

3.2.14 Some Article 29 Working Party Relevant Opinions

Opinions of Article 29 Data Protection Working Party might be relevant too when discussing cooperation between CSIRTs and LEAs.

An example is Opinion 4/2007 (Article 29 Data Protection Working Party, 2007), adopted on 20 June 2007, analysed the concept of personal data. In this regard, the opinion recalled the definition of personal data contained in the Directive 95/46/EC (European Parliament and Council of the European Union, 1995) and referred to the broad approach interpretation endorsed by the ECJ in *Case 101/2001 - Lindqvist* (Court of Justice of the European Union, 2003) mentioned above.

The opinion proposes a balanced solution. On the one hand, it recalled that European legislator adopts a wide notion of "personal data". On the other hand, it stated that the scope of the data protection rules should not be overstretched. In this opinion is stated that "unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side" (Article 29 Data Protection Working Party, 2007, p. 17).

3.2.15 National Legal and Policy Framework for the Cooperation between CSIRTs and LEAs

Also the national legal and policy frameworks govern and shape the cooperation between CSIRTs and LEAs.

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.

3.2.16 EU Cybersecurity Policy Funding Initiatives and EU Instruments to Support Cyber Security Collaboration at International Scale

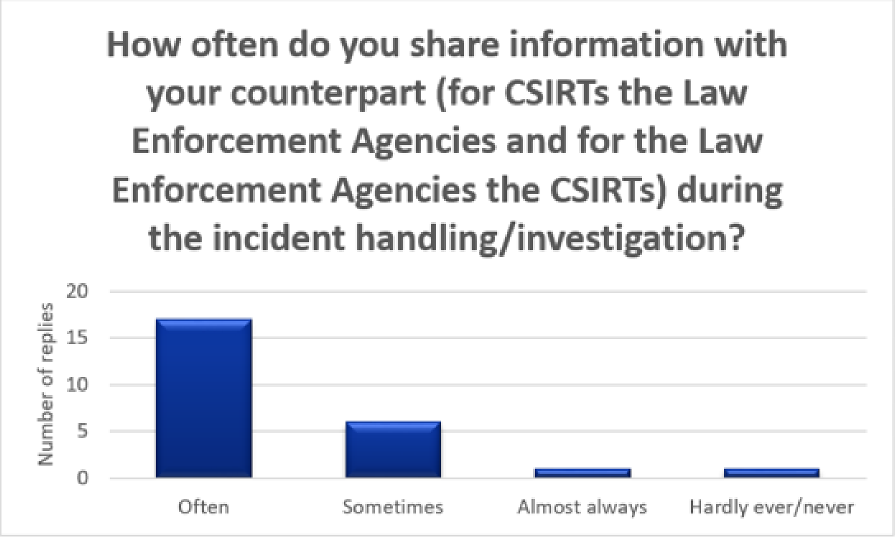
Among the EU funding initiatives in the field of cybersecurity (for an overview see: (European Commission, 2017c)), we can mention: Horizon 2020 (H2010) programme (European Commission, n.d. b) "to pursue cybersecurity research and innovation under the contractual public-private partnership on cybersecurity for the period 2017-2020" (European Commission, 2017c); Connecting Europe Facility (CEF) (European Commission, n.d. c), dedicated to the Digital Service Infrastructures (DSIs), cybersecurity being one of the areas supported under the DSIs stream within the CEF (MeliCERTes facility for instance, which "aims to facilitate swift and effective operational cooperation" for the CSIRTs Network (European Commission, 2017e) is an example of project conducted in the context of CEF); and the Internal Security Fund (ISF) to "promote the implementation of the Internal Security Strategy, law enforcement cooperation and the management of the Union's external borders" (European Commission, n.d. d).

In addition, there are some EU-instruments that play a role in support of the cyber security collaboration at international scale, such Instrument contributing to Stability and Peace (IcSP) (European Commission, n.d. e), European Neighbourhood Instrument (ENI) (European Union External Service, 2017) and Instrument of Pre-accession (IPA) (European Commission, n.d. f).

4. Challenges in the Cooperation between CSIRTs and LEAs

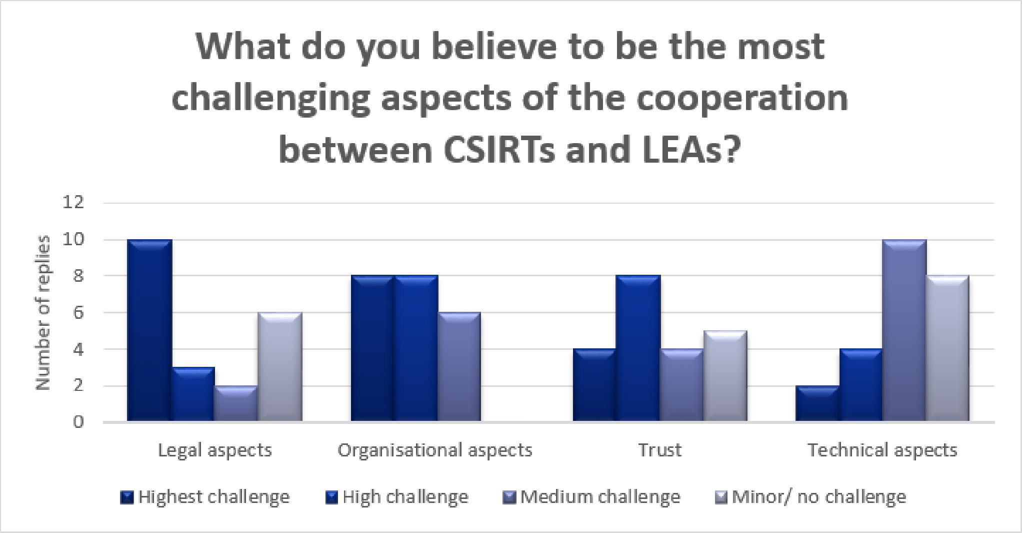
According to the data collected via the online survey, during the incident handling/investigation CSIRTs and LEAs often share information. See Figure 6.

Figure 6 - Frequency of Information Sharing between CSIRT-LE During Incident Handling/Investigation, According to Data Collected Via the Online Survey



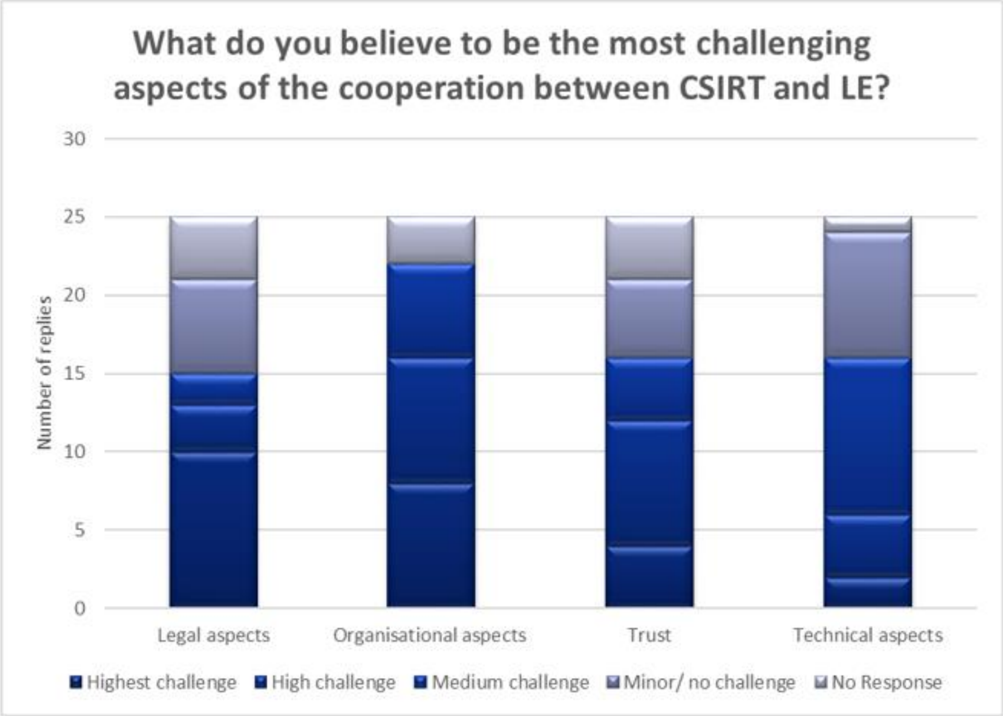
According to the data collected, in addition to building trust, there are some challenging aspects related to the cooperation between CSIRTs and LEAs. These can be classified into legal, organisational, and technical challenges. Figure 7 presents all these challenges.

Figure 7 – Overview of Challenging Aspects of the CSIRTs-LEAs Cooperation According to the Data Collected via the Online Survey - Clustered Columns



While overall for the CSIRTs and LEAs, the legal aspects represent the most challenging aspects of the cooperation, if we look at the aggregated replies on aspects representing the "highest challenge" and a "high challenge", we can observe that the organisational aspects are considered as the biggest challenge. According to the replies received from the online survey, the technical aspects are the smallest concern. See Figure 8 below.

Figure 8 - Overview of Challenging Aspects of the CSIRTs-LEAs Cooperation According to the Data Collected via the Online Survey - Stacked Columns



4.1 Legal Challenges

Below some legal challenges highlighted during the interviews are addressed. They belong mainly to two groups of challenges. First there are challenges related to the EU legislation under implementation. The second are those challenges which are related to the diversity in the national legal systems.

4.1.1 Relevant EU Legislation Currently Under Implementation

First, the transitions' period (periods during which an EU directive is transposed into Member States' national law) represents a challenge: during the transition period efforts and adjustments to new legal settings are required. Second, there are some challenges related to the implementation of specific pieces of legislation itself.

4.1.1.1 NIS Directive

Article 9 of the NIS Directive (European Parliament and Council of the European Union, 2016a) states that "Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I [requirements and tasks of CSIRTs], covering at least the sectors referred to in Annex II [i.e. energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, digital infrastructure] and the services referred to in Annex III [online marketplace, online search engine, and cloud computing service], responsible for risk and incident handling in accordance with a well-defined process".

One issue is that the spectrum of sectors in the NIS Directive is the minimum spectrum of sectors of operators of essential services, in other words, the list of sectors of essential services in the NIS Directive is not an exhaustive one. Moreover, the implementation of the NIS Directive could change the constituency of the current national/governmental CSIRTs and this might impact the current cooperation between LEAs and CSIRTs within the counties.

In addition, as provided in Article 2, par. 2 (a), the NIS Directive "lays down obligations for all Member States to adopt a national strategy on the security of network and information systems", in other words to adopt a "framework providing strategic objectives and priorities on the security of network and information systems at national level" (see Article 4 (3)). Most countries have already complied with this provision; however, a few still need to adopt such strategy to comply by the set deadline to the NIS Directive.

Finally, the NIS Directive anticipated that "Each Member State shall designate one or more national competent authorities on the security of network and information systems" (see Article 8, par. 1) and "have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive" (see Article 8, par. 5). Similar provisions (see Article 9, par. 2) in terms of resources are foreseen for the CSIRTs covering at least the sectors of essential services mentioned in Annex II and services in Annex III (see above). This means that Member States need to have adequate resources reserved to give an effective implementation to the NIS Directive and contribute to reach the achievement of "a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market" (see Article 1).

4.1.1.2 LEA Data Protection Directive

The main challenge in the implementation of the LEA Data Protection Directive is related to the cost factor. In order to ensure the right to the protection of personal data, the Directive provides for a number of obligations for the data controllers. Inevitably, the fulfilment of these obligations implies costs in terms of both staff and technical means. This could be a possible reason for resistance by data controllers to the application of the Directive in the processing of personal data.

4.1.1.3 GDPR

The GDPR (European Parliament and Council of the European Union, 2016b) shall apply from 25 May 2018 (see Article 99 - Entry into force and application).

From the interviews conducted, the issue of IP addresses as personal data was not identified as a challenge for the CSIRTs and LEAs cooperation. According to the data collected, IP addresses are usually considered as personal data and treated as such. It is however important that the Member States make the right application of the GDPR, in particular Article 23 (providing restrictions to data protections law in certain situations and under certain circumstances) and take in due account the Recital 49 (legal ground in processing of personal data by CSIRTs).

The retention of data and IP addresses as personal data could become an issue for the CSIRTs community and could cause serious issues in cybercrime investigation. This is why the Member States should be very specific in using the restriction provided in Article 23 and in applying the GDPR also in the light of Recital 49. Without that, the cooperation between CSIRTs and LEAs could become tougher. This could also impact the CSIRTs community by making the information exchange more formalised affecting the agile culture of CSIRTs.

4.1.2 Diversity of the Legal Framework between Member States

Finally, there are the challenges related to the variety of legal systems and legal provisions in the Member States. These challenges are particularly important. First, an event might be considered as a crime in one country, while in another country it is not a crime. Secondly, there is a problem related to the data retention. The diversity of conservation times between the various Member States represents a serious problem in terms of the effectiveness of the fight against crime.

4.2 Organisational Challenges

The world of ICT is constantly evolving, because of this the challenges faced in communication between CSIRTs and LEAs are also constantly changing. The following challenges should be recognised and discussed.

4.2.1 Limitations in Skills and Availability of Specialised Personnel

A major challenge is related to the available human resources. This is because, in some cases, the CSIRTs and LEAs have limited specialised personnel to meet actual needs. Generally, interviews have shown that, especially in time of high workload, the number of CSIRT/LEA personnel is not enough to facilitate their cooperation, including their communication.

4.2.2 Insufficient Training

Training, including publicly available online training resources, supports the development of skills within the CSIRTs community and law enforcement community. Such training is generally targeting either the CSIRTs - see for instance (ENISA, n.d. d) - or the LEAs, rarely both. Most of the time CSIRTs and LEAs do not perform common training, thus they do not have the chance to form a common ground and use the same tools, methods and terminology.

Training should concern technical but also legal and organisational aspects of the information sharing between CSIRTs and LEAs. According to the data collected, not always do personnel receive sufficient training on legal and organisational matters and in most cases personnel does not receive refresher training on possible new legislative developments.

4.2.3 Lack of Defined and Agreed Procedures for the Information Sharing between CSIRTs and LEAs

Another important challenge is the lack of defined procedures to fulfil the obligation to share. As emerged from the interviews, both CSIRT and LEAs sometime are lacking defined procedures, e.g. the CSIRTs to identify whether an incident is likely to be a crime, and the LEAs to provide information to CSIRTs.

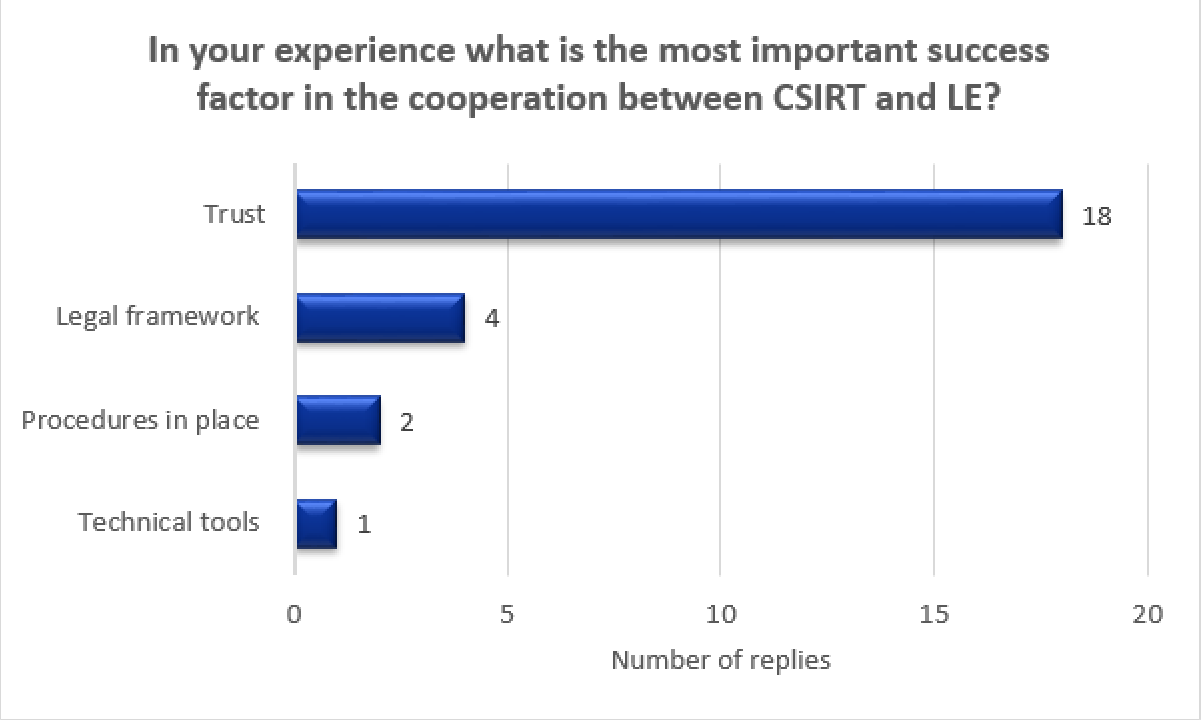
4.2.4 Need for a Better Knowledge of Recognised International Standards

A further challenge is the need for a better knowledge of standards relevant in the area of cooperation between CSIRTs and LEAs. There are indeed several standards, such as some standards developed by ETSI, ISO, and NIST, that play/could play a role in facilitating the cooperation between CSIRT and LEAs. However, in order for CSIRTs and LEAs to take advantage from the existing standards for further enhancing their cooperation, they need to have a better knowledge of such standards and their implementation.

4.2.5 Need for Building and Maintaining Trust between CSIRTs and LEAs

The mutual trust seems to be the main success factor determining the cooperation between CSIRTs and LEAs. The vast majority of the online survey participants agreed that the most important success factor in the cooperation between CSIRT and LEAs is trust (72%): 84% of the CSIRT community, 63% of LEA community. In Figure 9 an overview is provided on most important success factor according to the responses to the online survey.

Figure 9 – Most Important Success Factor in the Cooperation between CSIRTs and LEAs According to Data from the Online Survey



Knowing each other, understanding the culture of the other side (CSIRTs for LEAs and vice versa) and building mutual trust by working together on many cases and various occasions, have a significant impact on overall cooperation and collaboration within these two communities. It takes a while to build the mutual trust and to understand restrictions and culture of the other community (LEAs for CSIRTs and vice versa). For this reason, the personal relations are very important.

As emerged from the desk research and from the interviews, building and maintaining trust is a process that requires investment of resources and time. Moreover, turnover of personnel, especially of those who play the role of liaison officers, is a challenge for the cooperation between CSIRTs and LEAs because trust building requires time and investment also in establish and maintain good personal relations.

4.3 Technical challenges

In this report technical aspects, including technical challenges, of cooperation between CSIRTs and LEAs are addressed only very briefly. More information can be found in the ENISA report on *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement* (ENISA, 2017).

4.3.1 Keeping Information Systems and Tools Up-to-Date

A first technical challenge concerns the need for a continuous software update. The need to continuously upgrade the IT equipment involves a further challenge, related to the adequacy of the resources available to CSIRTs and LEAs. Interviews have shown that such resources are not always available but some economic weaknesses can be overcome thanks to the goodwill between the CSIRT and LEA personnel who, in many cases and under the condition that it is legal, spontaneously share both software and information.

4.3.2 Differences in the Modalities in Data Transmission

A second technical challenge identified concerns the need to overcome the different technical modalities used by the various CSIRTs and LEAs for data transmission between them. This diversity is due to the fact that CSIRTs and LEAs have different purposes. CSIRTs aim to counteract incidents, while LEAs aim to catch the criminal.

4.3.3 Differences in Toolkit Used

The toolkit that is used is also very different between CSIRTs and LEAs. The former are more inclined to use open-source tools and create custom ones. The latter usually need to have commercial, somehow verified or acknowledged tools, so that the result of their analysis is by no means questioned in the court of law.

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, a number of trends have become clear, more specifically regarding:

- CSIRTs and LEAs have different roles and objectives
- CSIRTs and LEAs often share information, both formally and informally
- Trust is a key factor for the information sharing
- Legal frameworks and organisational challenges to the cooperation can further be worked out in a way that cooperation between the two communities is further facilitated

5.1.1 Different Roles and Objectives

CSIRTs and LEAs have different but complementary roles and operate in different ways.

There is clear evidence that there are strong synergies between both communities. Findings from the interviews have found that CSIRTs operate more on an informal basis, while LEAs are generally bound by a more procedural approach of following rules and a hierarchical authority.

5.1.2 Information Sharing

CSIRTs and LEAs share often information both formally and informally. There is a lack of defined and agreed procedure for the information sharing. CSIRTs and LEAs use a variety of methods and tools for the representation and classification of data regarding incidents and events.

5.1.3 Trust

It is clear from the data collected that trust is of paramount importance for both CSIRTs and LEAs when it comes to information sharing. Trust is seen as an enabler while a lack of trust is seen as a challenge in turn hindering cooperation. In particular, the issue of reputational damage for a party involved in information exchange seems to be a significant concern which has an impact on the information exchange between both parties.

Trust is a process, not a state, which means that it is an ongoing effort that should be always sought and strengthened. Confidence building measures, cooperation and building of mutual interests between the two communities are key elements.

5.1.4 Legal Frameworks and Organisational Challenges

The data collected showed that there are challenges around the variety of legal systems and legal provisions in the Member States. One challenge to be considered is that an incident considered as a crime in a country, might not be a crime in another country. Furthermore, issues arise around data retention, and in particular the diversity of data retention periods between the various Member States. This seems to represent a serious problem in terms of the effectiveness to fight crime.

According to the data collected, there is a need for a better knowledge of standards relevant in the area of cooperation between CSIRTs and LEAs. Indeed, in order for CSIRTs and LEAs to take advantage from the existing standards for further enhancing cooperation, the knowledge of such standards and their implementation by both parties should be enhanced.

In addition to the key points outline above, it is clear that training should concern technical but also legal and organisational aspects of the information sharing. Training and skills development should cover changes or developments in the legal and policy framework relevant for the cooperation between CSIRTs and LEAs, including their communication.

5.2 Recommendations

In order to further improve the cooperation, including the communication, between CSIRTs - mainly national/governmental - and LEAs, some specific recommendations related to legal/organisational aspects of their cooperation are proposed.

It must be noted that these recommendations have been developed based on the data and results of this report as well as of the parallel ENISA report on *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement* (ENISA, 2017).

The recommendations below are as much as possible focused on CSIRT-LEA cooperation; they should be seen as additional to other more general and high level recommendations like to balance privacy and security, or promote, where appropriate, harmonisation of criminal law among the Member States.

5.2.1 Place Liaison Officers on Both Ends and Facilitate Coordination Among Liaison Officers Across Europe

It could be very useful to establish liaison officers within each organisation - LEA personnel into national/governmental CSIRTs and CSIRT personnel into LEAs. This would be beneficial in the process of trust building between CSIRTs and LEAs and in the process of providing reciprocal feedback. Placing officers from national/governmental CSIRT within LEAs and vice versa (LEA officers in national/governmental CSIRTs) would be of support for the development of a more uniformed approach to collaboration and information sharing.

Recommendation for:

- **ENISA**: to collect successful case studies of cooperation that has been enhanced by the presence of liaison officers and share them with CSIRTs and LEAs communities, propose a list of main requirements and tasks for liaison officers as well as models for liaison officers' appointment (e.g. via secondment, etc.)
- **ENISA**: to propose ways for facilitating the liaison officers' coordination across Europe
- **National/governmental CSIRTs and LEAs**: to identify liaison officers (LEA officers in national/governmental CSIRTs and vice versa)
- **Member States**: to foresee the role of the liaison as a translator between both parties and allocate resources for liaisons at national/governmental CSIRTs and LEAs
- **ENISA and Europol's EC3**: to propose a role description for liaison officers and models for such placement, in order to get a more uniform approach in the different Member States
- **ENISA and Europol's EC3**: to collect information on the working procedures of the liaisons and review them regularly

5.2.2 Formalise Intelligence Exchange

To establish a mechanism for monthly intelligence exchange between CSIRTs and LEAs, that would be also accompanied with the relevant and agreed statistics, would be of help for fighting against cybercrime. In addition, this will also help in trust building.

Recommendation for:

- **CSIRTs and LEAs**: to collect data and share them as much as they can and as much as they are allowed to
- **CSIRTs and LEAs**: to develop a methodology on how data quality can be evaluated (and improved)

- **CSIRTs**: to make the Traffic Light Protocol (TLP) more well-known outside CSIRT community, especially to the LEA community
- **ENISA and Europol's EC3**: to maintain and publish statistics of their respective constituencies (so other can learn from trending)
- **CSIRTs and LEAs Liaisons Officers**: to assist in simplifying the information exchange process and work out relevance check procedures before sharing, and review them regularly

5.2.3 Simplify and Standardise the Forms for Data Requests and the Procedures to Share Information Between CSIRTs and LEAs

To develop and to use the same forms for data requests from/to CSIRTs and LEAs and vice versa would improve the cooperation. The forms should be developed in a way that they are in line with the common taxonomy for CSIRTs and LEAs (Europol - European Cybercrime Centre, n.d.) - a new version of the common taxonomy for CSIRTs and LEAs is expected to be released at beginning of 2018. Regarding common taxonomy for CSIRTs and LEAs see (ENISA, 2015a), (ENISA, 2017). The forms should contain fields for as a minimum all the information included in the taxonomy and should clearly indicate whether the information received can be passed to other actors (e.g. other CSIRTs) involved in the investigation/incident handling.

Recommendation for:

- **CSIRTs and LEAs**: to articulate their requirements regarding how these forms and procedure should be used
- **ENISA and Europol's EC3:** to collect the requirements from the CSIRTs and LEAs regarding the forms and the procedures, to develop and propose standardised forms and standardised procedures to be adopted by the CSIRTs and LEAs communities
- **ENISA and Europol's EC3**: to promote the adoption of standardised forms and procedures
- **CSIRTs and LEAs**: to adopt and use standardised forms and standardised procedures for their information sharing

5.2.4 Further Invest in CSIRT-LEA Joint Training and in Skills Development

The creation of joint training and skills development between CSIRTs and LEAs would help share existing practices but will also allow the development of collaborative approaches in the future.

Good training plays a central role in improving the cooperation, including communication, of CSIRTs and. ENISA and Europol's EC3, possibly together with CEPOL, should work to extend the ENISA training material for the law enforcement operations. In addition, joint training for CSIRTs and LEAs should be facilitated.

Those training materials should focus mainly on mutual understanding of languages used by both CSIRTs and LEAs. There should be common understanding of legal the technical matters, including challenges faced by one or by both communities.

There should be joint exercises based on actual cases, where CSIRTs and LEAs will practice jointly fighting cybercrime.

If standardised forms for data exchange between CSIRTs and LEAs are developed and standardised procedures made available, they should also be covered during the training too. The training should also focus on (personal) data processing.

CSIRT and LEA senior management should also promote common training sessions; this can be carried out e.g. through conferences and access to virtual library. It is important to develop the awareness that such a joint training is necessary. Therefore, it should not be conceived as occasional, but instead continuously 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, including the one freely accessible on the ENISA site.

Recommendation for:

- **National/governmental CSIRTs and national law enforcement training centres**: to organise CSIRT-LEA joint training
- **ENISA and Europol's EC3, possibly together with CEPOL**: to extend the ENISA training material to be fitted for the law enforcement work
- **ENISA and Europol's EC3, possibly together with CEPOL**: to facilitate joint training for CSIRTs and LEAs
- **CSIRTs and LEAs**: to provide the training requirements to the facilitators of the joint training
- **CSIRTs and LEAs:** to participate in the joint training

5.2.5 Further Invest in Networking Events and Trust-Relationships between CSIRTs and LEAs

Events at national and EU level that bring together both CSIRTs - in particular national/governmental - and LEAs helps not only to improve their contacts and provide reciprocal feedback, but also to provide them with the opportunities to identify synergies and ways to further improve their cooperation. Some of such events are already organised at national level. At EU level, an annual workshop for CSIRTs and LEAs is organised jointly by ENISA and Europol's EC3. This kind of events should be continued and further promoted. Online meetings and seminars should be also considered.

Recommendation for:

- **Member States:** to organise – or where already existing – continue to organise such events for their CSIRTs - in particular national/governmental - and the LEAs at national level
- **ENISA and Europol's EC3**: to facilitate the setting-up of sessions and side-events dedicated to CSIRTs and LEAs cooperation during CSIRTs (e.g. FIRST, TF-CSIRT) and LEAs conferences
- **ENISA and Europol's EC3:** to continue organising events for the CSIRTs - in particular national/governmental and for the LEAs at EU level, to create and consolidate contacts, and to enhance trust
- **CSIRTs and LEAs:** to actively participate in the events with both technical teams and liaison officers and engage in an open discussion towards a further enhanced cooperation
- **ENISA**: to compile studies addressing aspects of cooperation between CSIRTs and LEAs and delving deeper into specific issues of their cooperation

5.2.6 Effectively Implement the NIS Directive and Apply the GDPR

In 2016 the EU put into force two important pieces of legislation, the NIS Directive and the GDPR. The effective implementation of the NIS Directive and application of GDPR will have positive effect on the common understanding between CSIRTs and LEAs in regard to the legal aspects of their work, and on their cooperation.

The NIS Directive aims at achieving a high common level of security of network and information systems across the Union. Legislators should work to transpose this directive into national law as soon as possible, in the view of the deadline of the 9 May 2018. Moreover, ENISA should provide reports on the implementation of this directive. In order to ensure any shortcomings are addressed, these reports should focus on both successes and challenges.

On the other hand, the GDPR is a Regulation which aims to harmonise the data privacy laws across Europe, and to better safeguard EU citizens' privacy. As discussed earlier in this report (see 3.2.9.2), Recital 49 of the GDPR sets the legal ground for the processing of personal data by CSIRTs. As a regulation, it is directly effective in Member States; however, it leaves room in certain occasions for Member States to legislate. For that reason, and since the GDPR will apply starting from 25 of May, 2018, Member States should work on national laws to cover those needs, as well as to promote the compliance of all affected entities to the GDPR. Similar to the NIS Directive, ENISA should provide reports on the application of GDPR, focusing on successes and challenges.

Recommendation for:

- **EU Member States**: to organise at national level events to promote the NIS Directive, and its effective implementation within country
- **EU Member States**: to organise at national level events to promote the GDPR, and its effective application within country
- **ENISA**: to analyse the implementation of the NIS Directive and the application of the GDPR focusing on successes as well as challenges to ensure that any shortcomings are addressed

5.2.7 Clearly Identify Which Information CSIRTs and LEAs Are Allowed/Obliged to Share between Them under the Current Legal Framework

To enhance the cooperation between CSIRTs and LEAs, it would be beneficial to have a clear identification of which information CSIRTs and LEAs are allowed/obliged to share between them under the current legal framework. This would help to point out possible legislative gaps and, accordingly, if appropriate, take actions to fill these gaps.

Recommendation for:

- **Member States:** to conduct studies to clearly identify which information under the current legal framework CSIRTs and LEAs are allowed/obliged to share between them and possible legislative gaps in their jurisdiction in relation to CSIRTs and LEAs cooperation
- **CSIRTs, in particular national CSIRTs, and LEAs:** whenever they identify a need for new legislation or for a change in the current legislation governing their cooperation, to express such need via their formal and informal channels
- **ENISA**: to collect data from the Member States and present an overview of which information CSIRTs - in particular national/governmental CSIRT - and LEAs can/are obliged to share between them under the current legal framework

5.2.8 Have in Place Legislation that Well Define Under Which Conditions CSIRTs and LEAs are Allowed/Obliged to Share Information Between Them and their Accountability When They Share and Reply to the Requests (CSIRT to LEA/LEA to CSIRT), as well as Reflect on Turning Information Sharing Between (National) CSIRTs and LEAs Mandatory

To further enhance the cooperation between CSIRTs and LEAs, is also important for members of those teams to have well-defined obligations and accountability to share information. This would also stimulate discussion at Member State level about the nature of information sharing, and ultimately conclude if information sharing, especially between national/governmental CSIRTs and LEAs, should be turned to mandatory (where it is not already mandatory).

Recommendation for:

- **Member States**: to have in place legislation that well define under which condition CSIRTs and LEAs are allowed/obliged to share and their accountability when they share information between them and reply to the requests (CSIRT to LEA/LEA to CSIRT), as well as to reflect on turning information sharing between (national/governmental) CSIRTs and LEAs mandatory (where it is not mandatory already)

- **Member States**: to reflect on turning information sharing between (national) CSIRTs and LEAs mandatory
- **European Commission and ENISA:** to assist the Members States by developing model legislation to govern and support CSIRTs and LEAs cooperation

5.2.9 Promote a Culture of Information Sharing Between CSIRTs and LEAs Within the Country and Cross-Border

Apart from the legal obligations for sharing and the standardisation of the form of requests that were described above, information exchange is also a culture that should be promoted between CSIRTs and LEAs. Best practices as well as use cases that information exchange assisted the efficient resolution of an incident/crime within the country of cross-border can be used as a basis for creating or further improving an information sharing mind-set among members of law enforcement and incident response teams.

Recommendation for:

- **ENISA**: to develop material specifically to promote the culture of information sharing between CSIRTs and LEAs.
- **Member States**: to use ENISA material as well as specific use cases in order to create or further improve a sharing mind-set between LEAs and CSIRTs

5.2.10 Promote the Improvement of Maturity of LEAs and CSIRTs in Order to Better Facilitate the Information Sharing

The maturity of an organisation in terms of people, processes and technology is an important factor of the ability of the organisation to share information efficiently with other parties. For CSIRTs there are already several maturity models which are used as an audit base for the acceptance of a team in closed groups that focus on information sharing; an example is the ENISA online maturity assessment (ENISA, n.d. b). On CSIRT maturity see: (ENISA, n.d. a), (ENISA, 2015c), (ENISA, 2017c), and (ENISA, 2016c)

The data collected did not provide any indication that similar models currently exist for the law enforcement. The formulation of maturity models for LEAs would give them the chance to compare and improve their capabilities based on commonly accepted standards, and thus reach and prove a level of maturity that would make information exchange with CSIRTs easier.

Recommendation for:

- **ENISA**: to promote the importance of maturity improvement and of maturity models
- **Europol's EC3**: to develop a maturity model for LEAs, similar to CSIRT models, that would describe people, processes and technology parameters based on which LEAs could measure and improve their maturity level
- **Europol's EC3**: to disseminate the maturity model to Member States LEAs and provide assistance on the way that it can be used for measurement and improvement of their maturity
- **Member States**: to promote the use of maturity models by their CSIRTs - in particular national/governmental - and LEAs for the improvement of their capabilities, with the view of further enhancing the cooperation between CSIRTs and LEAs

5.2.11 Develop Internal Security Policies Permitting and Supporting Information Sharing with CSIRTs/LEA Counterpart

It is important that the internal security policies of CSIRTs allow as much as possible the information sharing with the law enforcement and vice versa. So, when developing new internal security policies, both

CSIRTs and LEAs should take this into account in order not to run the risk that information sharing permitted by law might be hindered at the level of internal security policies.

Recommendation for:

- **CSIRTs and LEAs**: when developing their internal security policy to shape them in a way that they do not represent an obstacle to the information sharing with their CSIRT/LEA counterpart.

5.2.12 Make Available and Take Advantage of CSIRTs Dataset, Expertise and Contacts

CSIRTs can enrich LEAs intelligence that would be useful for LEAs investigations/prosecutions. LEAs could have access to CSIRTs data via Application Programming Interfaces (APIs) and thus enrich their own investigation data.

Practical examples of datasets that could be shared between CSIRTs and LEA are: annotation services for IP addresses such as Passive DNS, Passive SSL; public information leaks; datasets about crawled information from the darknet; and measurements based on backscatter in case of distributed denial of service attacks.

In addition, CSIRTs can provide technical expertise during LEAs investigations when needed/requested. The CSIRTs network of contacts can be very useful during LEAs investigations.

Recommendation for:

- **ENISA and Europol's EC3**: to work out procedures on how the trust relationship CSIRT-constituency can be maintained when allowing LEA access to datasets
- **ENISA and CSIRTs**: to develop methodologies to support LEAs coordination with CSIRTs during investigations
- **CSIRTs**: to provide enrichment services to LEAs for their investigations
- **CSIRTs**: to provide technical expertise during law enforcement investigation upon request
- **CSIRTs**: to provide access to their network of contacts to LEAs for their investigations
- **LEAs:** to make use of CSIRTs dataset, expertise and contacts and LEAs provide feedback on the quality of the dataset, expertise and contacts.

6. Bibliography/References

Article 29 Data Protection Working Party. (2007, June 20). *Opinion 4/2007 on the concept of personal data.* Retrieved August 6, 2017, from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Bayens, G. J., & Roberson, C. (2011). *Criminal Justice Research Methods.*

BJS. (n.d.). *Terms & Definitions: Law Enforcement*. Retrieved July 28, 2017, from https://www.bjs.gov/index.cfm?ty=tdtp&tid=7

Blumer, H. (1954). What Is Wrong with Social Theory. *American Sociological Review*, 3-10.

Cambridge University Press. (n.d.). *Cambridge Dictionary*. Retrieved July 28, 2017, from http://dictionary.cambridge.org/dictionary/english/practice

Casey, E. (2004). *Digital Edidence and Computer Crime.*

Council of Europe. (1950, November 4). *Convention for the Protection of Human Rights and Fundamental Freedoms.* Retrieved July 2017, 2017, from http://www.echr.coe.int/Documents/Convention_ENG.pdf

Council of Europe. (2001, November 23). *Convention on Cybercrime.* Retrieved September 14, 2017, from http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Council of Europe. (n.d.). *Council of Europe*. Retrieved August 31, 2017, from http://www.coe.int/en/

Council of Europe Cybercrime Convention Committee. (2017, June 09). *Meeting report 17th Plenary of the T-CY.* Retrieved September 29, 2017, from https://rm.coe.int/t-cy-17-meeting-report-/168072366d

Council of Europe. (n.d. a). *Details of Treaty No.185 - Council of Europe Convention*. Retrieved July 29, 2017, from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council of Europe. (n.d. b). *Chart of signatures and ratifications of Treaty 185*. Retrieved July 29, 2017, from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=urAI7A8y

Council of Europe. (n.d. c). *Details of Treaty No.189*. Retrieved July 28, 2017, from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

Council of the European Union. (2005, Febraury 24). *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.* Retrieved July 29, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1501311689888&uri=CELEX:32005F0222

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. (2017a, 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

Council of the European Union. (2017b, October 12). *Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO').* Retrieved November 1, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1939&qid=1510001416068&from=EN

Court of Justice of the European Union. (2003, November 6). *Judgment of teh Court of 6 November 2003, C-101/01 - Lindqvist.* Retrieved August 29, 2017, from http://curia.europa.eu/juris/liste.jsf?language=en&num=c-101/01

Court of Justice of the European Union. (2011, November 24). *C-70/10, Judgment of the Court (Third Chamber) of 24 November 2011. Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).* Retrieved August 28, 2017, from http://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10

Court of justice of the European Union. (2014, April 8). *Jundgement of the Court (Grand Chamber) of 8 April 2014, Joined Cases C-293/12 and C-594/12.* Retrieved August 28, 2017, from http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

Court of Justice of the European Union. (2016, October 19). *Judgement of the Court (Second Chamber), C-582/14, 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland).* Retrieved August 28, 2017, from http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

Court of Justice of the European Union. (2016, December 21). *Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others.* Retrieved August 28, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0203

Court of Justice of the European Union. (2016, October 19). *Press Release No 112/16, 19 October 2016, Judgment in Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland.* Retrieved July 31, 2017, from https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-10/cp160112en.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). *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. (2011a). *A flair for sharing – encouraging information exchange between CERTs - A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe.* Retrieved July 10, 2017, from https://www.enisa.europa.eu/publications/legal-information-sharing-1

ENISA. (2011b). *Ontology and taxonomies of resilience.* Retrieved July 07, 2017, from https://www.enisa.europa.eu/publications/ontology_taxonomies

ENISA. (2012). *Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime.* Retrieved July 29, 2017, from https://www.enisa.europa.eu/publications/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime

ENISA. (2014). *Privacy and Data Protection by Design – from policy to engineering.* Retrieved August 6, 2017, from https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

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. (2015a). *Information sharing and common taxonomies between CSIRTs and Law Enforcement.* Retrieved July 07, 2017, from https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

ENISA. (2015b). *ENISA – CERT Inventory.* Retrieved July 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. (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). *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity.* Retrieved November 1, 2017, from https://www.enisa.europa.eu/publications/study-on-csirt-maturity

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, May 17). *WannaCry Ransomware Outburst.* Retrieved September 6, 2017, from https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

ENISA. (2017b). *ENISA Programming Document 2017-2019.* Retrieved July 4, 2017, from https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019

ENISA. (2017c). *Study on CSIRT Maturity – Evaluation Process.* Retrieved November 1, 2017, from https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

ENISA. (n.d. a). *CSIRT Maturity.* Retrieved November 1, 2017, from https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

ENISA. (n.d. b). *CSIRT Maturity - Self-assessment Survey*. Retrieved from https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

ENISA. (n.d. c). Retrieved from https://www.enisa.europa.eu/about-enisa

ENISA. (n.d.). *Considerations on the Traffic Light Protocol*. Retrieved July 12, 2017, from https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol

ENISA. (n.d. d). *Training Resources*. Retrieved August 1, 2017, from https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material

ETSI. (n.d.). *What are standards?* Retrieved October 27, 2017, from http://www.etsi.org/standards/what-are-standards

European Commision. (2017, May 24). *European Commision GDPR*. Retrieved from http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm

European Commision. (2017a, September 13). *Proposal for a Regulation of the European Parliament and of The Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013.* Retrieved September 29, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN

European Commission. (2010a, March 3). *EUROPE 2020 A strategy for smart, sustainable and inclusive growth, /* COM/2010/2020 final */.* Retrieved July 29, 2017, from http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52010DC2020

European Commission. (2010b, May 19). *Communication from the Commission of 19 May 2010 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe [COM(2010) 245 final – Not published in the Official Journa.* Retrieved July 29, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0245

European Commission. (2014). *Digital agenda for Europe - The European Union Explained.* Retrieved July 29, 2017, from https://europa.eu/european-union/file/1497/download_en?token=KzfSz-CR

European Commission. (2015a, May 06). *Communication from The Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a Digital Single Market Strategy for Europe,.* Retrieved July 28, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192

European Commission. (2015b, February 10). *Strengthening trust and security*. Retrieved August 31, 2017, from https://ec.europa.eu/digital-single-market/en/policies/strengthening-trust-and-security

European Commission. (2015c, April 28). *Communication from the Commission to the European Parliament, the Council, The European Economic And Social Committee and the Committee of the Regions, the European Agenda on Security,COM(2015) 185 final.* Retrieved July 29, 2017, from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

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). *Report assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, COM(2017) 474.* Retrieved September 13, 2017, from http://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-474-F1-EN-MAIN-PART-1.PDF

European Commission. (2017b, May 10). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy, COM/2017/0228 final.* Retrieved July 29, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496330315823&uri=CELEX:52017DC0228

European Commission. (2017b, October 4). *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')* . Retrieved October 27, 2017, from https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

European Commission. (2017c, September 13). *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises C/2017/6100.* Retrieved November 1, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.239.01.0036.01.ENG&toc=OJ:L:2017:239:TOC

European Commission. (2017c, January). *EU cybersecurity initiatives*. Retrieved August 4, 2017, from http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

European Commission. (2017d, January 10). *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and eCommunications).* Retrieved November 1, 2017, from http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017PC0010

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

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. a). *EU Survey*. Retrieved July 4, 2017, from https://ec.europa.eu/eusurvey/home/welcome

European Commission. (n.d. b). *Horizon 2020.* Retrieved August 3, 2017, from https://ec.europa.eu/programmes/horizon2020/

European Commission. (n.d. c). *Connecting Europe Facility*. Retrieved August 3, 2017, from https://ec.europa.eu/inea/en/connecting-europe-facility

European Commission. (n.d. d). *Internal Security Fund - Police*. Retrieved August 3, 2017, from https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police_en

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 Council, Council of the European Union. (2017c, October 12). *20 member states confirm the creation of an European Public Prosecutor's Office.* Retrieved November 2017, from http://www.consilium.europa.eu/en/press/press-releases/2017/10/12/eppo-20-ms-confirms/

European Council, Council of the European Union. (n.d.). *The ordinary legislative procedure*. Retrieved September 29, 2017, from http://www.consilium.europa.eu/en/council-eu/decision-making/ordinary-legislative-procedure/

European Cybercrime Centre - EC3. (n.d.). Retrieved July 28, 2017, from European Cybercrime Centre - EC3: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

European Judicial Network. (n.d.). *Glossary*. Retrieved July 28, 2017, from http://ec.europa.eu/civiljustice/network/network_en.htm

European Parliament and Council of the European Union. (1995, October 24). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Retrieved Jully 29, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1501330255977&uri=CELEX:31995L0046

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 netwonetworks 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. (2009, November 25). *Directive 2009/136/EC of the European Parliament and of the Council, 25 November 2009, amending Directive 2002/22/EC, Directive 2002/58/EC and Regulation (EC) No 2006/2004.* Retrieved September 4, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0136

European Parliament and Council of the European Union. (2013, 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. (2013, 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. (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, 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 and Council of the European Union. (2016b, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* 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. (2016c, April 27). *Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.* Retrieved July 29, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1501331727751&uri=CELEX:32016L0681

European Parliament and Council of the European Union. (2016d, October 12). *Proposal for a Directive Establishing the European Electronic Communications Code, COM(2016) 590 final/2.* Retrieved September 08, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0590

European Parliament and Council of the European Union. (2016e, May 11). *Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/J.* Retrieved July 29, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1501326885447&uri=CELEX:32016R0794

European Parliament. (n.d.). *Legislative powers*. Retrieved September 29, 2017, from http://www.europarl.europa.eu/aboutparliament/en/20150201PVL00004/Legislative-powers

European Parliament. (n.d. a). *Procedure file 2017/0003(COD)*. Retrieved November 2017, from Legislative Observatory: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0003(COD)

European Parliament. (n.d. b). Retrieved November 2017, from European Parliament Legislative Observatory: http://www.europarl.europa.eu/oeil/home/home.do

European Parliament, Council and Commission. (2000, December 7). *Charter of fundamental rights of the European Union.* Retrieved July 29, 2017, 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. (n.d.). *Common Taxonomy for the National Network of CSIRTs.* Retrieved August 3, 2017, 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. (2017a, June 28). *New wave of ransomware affecting businesses: what to do?* Retrieved September 06, 2017, from https://www.europol.europa.eu/newsroom/news/new-wave-of-ransomware-affecting-businesses-what-to-do

Geberth, V. J. (1995). *The "Signature" Aspect in Criminal Investigation.* Retrieved July 31, 2017, from http://www.practicalhomicide.com/articles/signature.htm

Hagan, F. E. (1997). *Research Methods in Criminal Justice and Criminology.*

INTERPOL. (n.d.). *Interpol*. Retrieved August 3, 2017, from https://www.interpol.int/

MISP. (2017, July 28). Retrieved from http://www.misp-project.org

MISP Project. (n.d.). Retrieved July 28, 2017, from MISP Project: https://www.misp-project.org/

NATO NCI Agency. (n.d.). *Malware Information Sharing Platform.* Retrieved July 28, 2017, from https://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20(MISP).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.*

TF-CSIRT - Trusted Introducer. (n.d.). *Processes.* Retrieved November 1, 2017, from https://www.trusted-introducer.org/processes/certification.html

The Member States . (n.d.). *Consolidated version of the Treaty on the Functioning of the European Union.* Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

Annex A: Acronyms

ACRONYM	DESCRIPTION
API	Application Programming Interface
BJS	US Bureau of Justice Statistics
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, Agencies and Bodies
CoE	Council of Europe
CSIRT	Computer Security Incident Response Team
CSSCSIRT	Cyber Security Strategy Computer Security and Incident Response Team
DAE	Digital Agenda for Europe (DSM)
DG	Directorate General
DNS	Domain Name System
DP	Data Protection
DSI	Digital Service Infrastructures
DSM	Digital Single Market
EC3	European Cybercrime Centre
ECJ	Court of Justice of the European Union
EEA	European Economic Area
EEAS	European External Action Service
EFTA	European Free Trade Association
EIO	European Investigation Order
ENI	European Neighbourhood Instrument
ENISA	European Union Agency for Network and Information Security
EPPO	European Public Prosecutor's Office
EU	European Union
ETSI	European Telecommunications Standards Institute
EUCTF	European Union Cybercrime Task Force
FI-ISAC	Financial - Information Sharing and Analysis Center
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation
H2020	Horizon 2020
IcSP	Instrument contributing to Stability and Peace
ICT	Information and Communication Technology
IOC	Indicators of Compromise
IOCTA	Internet Organised Crime Threat Assessment
IP	Internet Protocol
IPA	Instrument of Pre-accession
ISA	Interoperability Solutions for European Public Administrations
ISAC	Information Sharing and Analysis Center
ISF	Internal Security Fund
IT	Information Technology
LE	Law Enforcement
LEA	Law Enforcement Agency
MISP	Malware Information Sharing Platform
MS	Member State
n.d.	no date
NCI Agency	NATO Communications and Information Agency
Par.	Paragraph
PNR	Passenger Name Record
PoC	Point of Contact
SO	Strategic Objective

SSL	Secure Sockets Layer
TEC	Treaty establishing the European Community
TF-CSIRT	Task Force - Computer Security Incident Response Team
TFEU	Treaty on the Functioning of the European Union
TLP	Traffic Light Protocol

Annex B: Samples of Questionnaires to Support the Interviews

B.1 Sample Questionnaire to Support the Interviews with the CSIRTs

Questions prepared to support the interviews with CSIRTs to collect data for the Report on further improvement of communication between CSIRTs and LEAs

The report on Further improvement of communication between CSIRTs and LEAs is foreseen in the ENISA's Programming Document 2017-2019, Output O.4.2.1 - Support the fight against cybercrime and collaboration between CSIRTs and LEAs (link: https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019)

This report will address legal and organizational/policy aspects of the cooperation between CSIRT and LEA. ENISA is carrying out a parallel project aiming at the drafting of ENISA Guidelines on emerging trends, tools and methodologies to support LEA and CSIRT cooperation in the fight against cybercrime. The parallel project addresses technical aspects of communication between CSIRT and LEA in the fight against cybercrime.

Interviewer:

Interviewee:

Date of the interview:

Expected duration of the interview: 1 hour

§ INTRODUCTION QUESTIONS

1. Name:

2. Affiliation:

3. Position:

4. What is your organisation's legal basis?

5. What is the constituency of your organisation?

6. What types of cases does your organisation deal with?

§ QUESTIONS ON ORGANISATIONAL/POLICY CHALLENGES

1.

a. Does your organisation cooperate with the LE (law enforcement) of your country?

[Yes/No]

b. Does it cooperate with the LE of other countries?

[Yes/No]

c. Only with the LE of other EU countries or also with LE from Third countries?

2. Which kind of cooperation does your organisation have with the LE (e.g. reply to LE requests in the context of criminal investigations, witnesses in court, forensic experts, joint training, common trainings, regular meetings, or any other type of bilateral trust-building events)?

3. What type of information does your organisation exchange with LE? How often?

4.

a. Is the communication that your organisation has with LE legally founded (e.g. you are required by law to communicate with the LE)?

[Yes/No]

b. Or is it more in an informal personal basis?

5.

a. Does your organisation have clear polices/internal procedures defining how to process requests from and cooperate with the LE?

[Yes/No]

b. Is a periodic review of these policies/internal procedures foreseen?

[Yes/No]

6. Does your organisation have a formalized way of receiving and processing requests from the LE?

[Yes/No]

7. Has your organisation set internal formal steps to take before accepting (or rejecting) a request from the LE to provide information in the context of criminal investigations?

[Yes/No]

8. Has your organisation set internal formal steps to obtain the internal approval on information to provide to the LE in reply to requests from the LE in the context of criminal investigations?

[Yes/No]

9. What type of communication channels has your organisation established with the LE of your country or of other countries (face-to-face meetings, secured email, online platform, etc.)?

10. Does your organisation have a formalised way to provide a reply to the LE to a request from the LE in the context of criminal investigations?

[Yes/No]

11.

a. Does your organization have criteria/guidelines set to assess whether an incident is likely to be a crime?

[Yes/No]

b. Does your organisation have procedures defining which actions to take or not to take when mitigating an incident likely to be a crime?

[Yes/No]

c. Which are these actions?

12.

a. Is LE personnel part of your organisation (e.g. seconded to)?

[Yes/No]

b. Is any member of your organisation seconded to LE?

[Yes/No]

c. Do you have in your country a national agency embedding both CSIRT and LE personnel?

[Yes/No]

13.

a. Does your organisation face any challenges when cooperating with the LE?

[Yes/No]

b. If yes, what type of challenges does it face (e.g. legal, organizational/policy, technical, etc.)?

c. How do you think these challenges could be overcome?

14. When your organisation cooperate with the LE, are the resources available to your organisation – in terms of human resources, equipment, tools, and means of communication, training - adequate?

[Yes/No]

15. How does LE submit requests for assistance during criminal investigation to your organisation?

16. Do you have defined polices/internal procedure on when you need to seek for legal (internal or external) advice?

[Yes/No]

17.

a. Does your organization sometimes refuse a request from the LE to provide data?

[Yes/No]

b. Is the refusal based on legal grounds?

[Yes/No]

c. On lack on human/technical resources?

d. [Yes/No]

e. On other grounds? Which grounds?

18.

a. Does your organisation request data from LE?

[Yes/No]

b. Are these requests generally fulfilled?

[Yes/No]

c. If not, on which grounds (e.g. organizational, legal, technical grounds)?

19.

a. Does your organisation receive feedback from LE on the information you provide to them during criminal investigations?

[Yes/No]

b. If yes, which kind of feedback (e.g. feedback on whether the information provided was useful, complete, etc.)?

§ QUESTIONS ON LEGAL CHALLENGES

20. Which kind of data do you share with LE?

21.

a. Which areas of law are relevant when your organisation cooperate with LE to fight cybercrime (e.g. data protection, data retention, criminal law and criminal procedure, contract law and confidentiality obligations, intellectual property rights, legal grounds of the CSIRT, NIS Directive, etc.)?

b. Which specific legal provisions do you take into account when you cooperate with the LE?

22.

a. Does your organisation have internal legal experts who solve legal issues you might face when performing your tasks, including when cooperating with the LE?

[Yes/No]

b. If yes, do you think their resources (e.g. expertise, time available, equipment, etc.) are adequate for the needs of your organisation?

[Yes/No]

c. Does your organisation relay on an external legal counselling?

[Yes/No]

d. When you do not know whether you can send data to LE and you cannot contact any legal expert, how do you proceed?

23. Do you receive training on how to deal with legal issues that you might face when performing your task and when cooperating with the LE?

[Yes/No]

24.

a. What are the legal issues that you face most frequently?

b. What are the legal difficulties that you cannot answer without consulting a legal expert?

25. Does your organization have a solid legal basis and a clear mandate (clear mandate in the sense, for instance, of clear definition of roles and responsibilities)?

26. Does your organization have a well-defined point of contact in the LE?

27. Do you have an obligation to report to the LE when you come across possible crimes?

28. How would you react if you (or some of your colleagues) were called as witness on a trial in your country? How would you react if you (or some of your colleagues) were called as witness on a trial another country?

29. Which legal provisions regulate the relation of your organisation with its constituency (e.g. contract, non-disclosure agreements, etc.)?

30. Do you notify the victim of an incident (whether it is likely or not to be crime)?

a. Do you encourage the victim to report to the LE what you believe it is likely to be crime?

[Yes/No]

b. Do you provide the victim with information on how to report it?

[Yes/No]

31.

a. Do you see the current legal system more as an enabler or as a barrier to your cooperation with the LE?

[Enabler/Barrier]

b. Could you suggest improvements?

32.

a. Would you see trust as an issue in the cooperation of your organisation with other CSIRTs in your country?

[Yes/No]

b. Would you see trust as an issue in the cooperation of your organisation with CSIRT in other countries?

[Yes/No]

c. Would you see trust as an issue in the cooperation of your organisation with the LE of your country?

[Yes/No]

d. Would you see trust as an issue in the cooperation of your organisation with the LE of other countries?

[Yes/No]

[ADDITIONAL QUESTIONS – IF TIME PERMITS]

33. Do you know if, according to your legislation, the IP address is personal data or not?

34. With which main categories of data subjects does your organization deal (e.g. persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; victim of a criminal offense; other parties to a criminal offence such as potential witness)?

QUESTIONS ON MENTIONING OF NAME, AFFILIATION, AND COUNTRY

35. Do you have any objections to have your name and affiliation mentioned in the report (NOTE: just not to raise false expectations, please mention that it is not confirmed whether names of interviewees will be mentioned in the report)?

36. Do you have any objections to have your name and affiliation mentioned in the acknowledgements of the report? (NOTE: just not to raise false expectations, please mention that it is not confirmed whether names of interviewees will be mentioned in the acknowledgements of the report)?

37. Do you have any objection to have stated in the report that information on your country has been collected via an interview with a member of a CSIRT.

B.2 Sample Questionnaire to Support the Interviews with the LEAs

Questions prepared to support the interviews with the LE to collect data for the Report on further improvement of communication between CSIRTs and LEAs

The report on Further improvement of communication between CSIRTs and LEAs is foreseen in the ENISA's Programming Document 2017-2019, Output O.4.2.1 - Support the fight against cybercrime and collaboration between CSIRTs and LEAs (link: https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019)

This report will address legal and organizational/policy aspects of the cooperation between CSIRT and LEA. ENISA is carrying out a parallel project aiming at the drafting of ENISA Guidelines on emerging trends, tools and methodologies to support LEA and CSIRT cooperation in the fight against cybercrime. The parallel project addresses technical aspects of communication between CSIRT and LEA in the fight against cybercrime.

Interviewer:

Interviewee:

Date of the interview:

Expected duration of the interview: 1 hour

§ INTRODUCTION QUESTIONS

1. Name:

2. Affiliation:

3. Position:

4. What is your organisation legal basis?

5. What types of cases does your organisation deal with?

§ QUESTIONS ON ORGANISATIONAL/POLICY CHALLENGES

1.

a.

i. Does your organisation cooperate with CSIRTs of your country?

[Yes/No]

ii. If yes, how often?

b.

i. Does it cooperate with the CSIRTs from other countries?

[Yes/No]

ii. If yes, how often?

c.

i. Does it cooperate with CSIRTs from other EU countries?

[Yes/No]

ii. If yes, how often?

d. Does it cooperate CSIRT from Third countries?

[Yes/No]

e. If yes, how often?

2. Which kind of cooperation does your organisation have with the CSIRTs (e.g. CSIRT replies to your requests in the context of criminal investigations, CSIRTs are called as witnesses in court, CSIRT provide you with forensic expertise, joint training, regular meetings, or any other type of bilateral trust-building events)?

3. What type of information does your organisation exchange with CSIRTs? How often? Only with the national/governmental CSIRTs or also with other CSIRTs?

4.

a. Is the communication between your organisation and a CSIRT legally founded?

[Yes/No]

b. Is the communication between your organisation and a CSIRT more on an informal personal basis?

[Yes/No]

c. Does this apply to your communication with all CSIRTs or only to specific CSIRT (e.g. national and/or governmental CSIRTs in your country)?

5.

a. Does your organisation have clear polices/internal procedures defining how to cooperate and process information with the CSIRTs?

[Yes/No]

b. Is a periodic review of these policies/internal procedures foreseen?

[Yes/No]

6. Does your organisation have a formalized way of receiving and processing information from the CSIRTs?

[Yes/No]

7. Has your organisation set internal formal steps to take before sending a request to the CSIRTs to provide information in the context of criminal investigations?

[Yes/No]

8. What type of communication channels has your organisation established with the CSIRT in your country or of other countries (face-to-face meetings, secured email, online platform, etc.)?

9.

a. Does your organisation have a formalized way of providing information to the CSIRTs?

[Yes/No]

b. Does your organisation have a formalized way of providing information to all CSIRTs in your country or only to some specific CSIRTs (e.g. the national/governmental CSIRTs)?

10.

a. Does your organisation provide the CSIRT with feedback on the information that they provide in reply to requests that your organization send to them in the context of criminal investigations?

[Yes/No]

b. Which kind of feedback (e.g. how the information was useful for the investigation, if information in a different format could have been even easier to process, etc.)?

11.

a. Is CSIRT personnel part of your organisation (e.g. seconded to)?

[Yes/No]

b. Is any member of your organisation part of the CSIRT (e.g. seconded to the national/governmental CSIRT)?

[Yes/No]

c. Do you have in your country a national agency embedding both CSIRT and LE personnel?

[Yes/No]

12.

a. Does your organization see sometimes a request for information sent to a CSIRT to provide data refused?

[Yes/No]

b. If yes, on which rounds is the refusal based (e.g. legal grounds or other grounds)?

13.

a. Does your organisation face any challenges when cooperating with the CSIRTs?

[Yes/No]

b. If yes, what type of challenges does it face (e.g. legal, organizational/policy, technical, etc.)? How do you think these challenges could be overcome?

14. When your organisation cooperate with the CSIRTs, are the resources available to your organisation – in terms of human resources, equipment, tools, and means of communication, training - adequate?

[Yes/No]

§ QUESTIONS ON LEGAL CHALLENGES

15.

a. Which areas of law are relevant when your organisation cooperate with CSIRT (e.g. data protection, data retention, criminal law and criminal procedure, contract law and confidentiality obligations, intellectual property rights, legal bases of the CSIRT you are cooperating with, NIS Directive, etc.)?

b. Which specific legal provisions do you take into account when you cooperate with the CSIRT?

16. Does your organisation have internal legal experts who solve legal issues you might face including, if applicable, issues that might raise when you cooperate with the CSIRTs during criminal investigation?

[Yes/No]

17.

a. Do you receive continuous training on how to deal with legal issues that you might face when investigating cyber crime?

[Yes/No]

b. Does the training cover how to cooperate with CSIRTs (e.g. which information you are allowed to request to them and which to share with them in order that they can at the best support you)?

[Yes/No]

18. What are the legal issues that you face most frequently? What are the legal difficulties that you cannot answer without consulting a legal expert?

19. Do you have particular legal provisions addressing the cooperation specifically with national/governmental CSIRTs?

20.

a. Does your organization have a well-defined point of contact in the CSIRT community?

[Yes/No]

b. Is this the national/governmental CSIRT?

21. Do CSIRTs have an obligation to report to the LE when come across an incident likely to be crime?

[Yes/No]

22. Do you notify the victim of a crime?

[Yes/No]

23. Do you see the current legal system more as an enabler or as a barrier to your cooperation with the CSIRTs?

[Enabler/Barrier]

24.

a. Could the current legal system be improved to facilitate cooperation between CSIRT and LE?

[Yes/No]

b. How?

25. Apart from the legal system, if applicable, what else would you propose to improve in the communication and collaboration with CSIRT and how?

26.

a. Would you see trust as an issue in the cooperation of your organisation with CSIRTs in your country?

[Yes/No]

b. Would you see trust as an issue in the cooperation of your organisation with CSIRT in other EU countries?

[Yes/No]

c. Would you see trust as an issue in the cooperation of your organisation with CSIRTs in Third countries?

[Yes/No]

[ADDITIONAL QUESTIONS – IF TIME PERMITS]

27. Do you know if, according to your legislation, the IP address is a personal data or not?

28. The deadline for the Member States to transpose the Directive (EU) 2016/680 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 is 6 May 2018. Do you know the status of its transposition in your country and if you think that this transposition implies particular changes in the way you deal with data during cyber crime investigations?

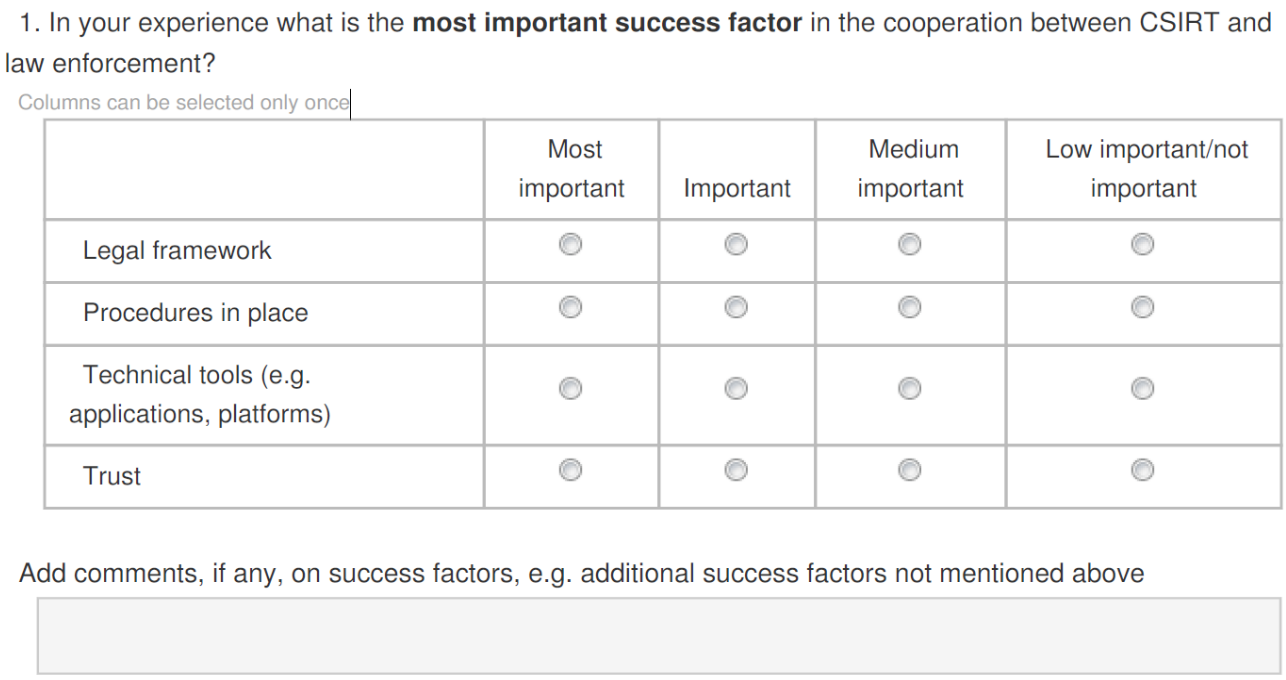
§ QUESTIONS ON MENTIONING OF NAME, AFFILIATION, AND COUNTRY

29. Do you have any objections to have your name and affiliation mentioned in the report (NOTE: just not to raise false expectations, please mention that it is not confirmed whether names of interviewees will be mentioned in the report)?

30. Do you have any objections to have your name and affiliation mentioned in the acknowledgements of the report? (NOTE: just not to raise false expectations, please mention that it is not confirmed whether names of interviewees will be mentioned in the acknowledgements of the report)?

31. Do you have any objection to have stated in the report that information on your country has been collected via an interview with a member of a CSIRT.

Annex C: Questions in the Online Survey

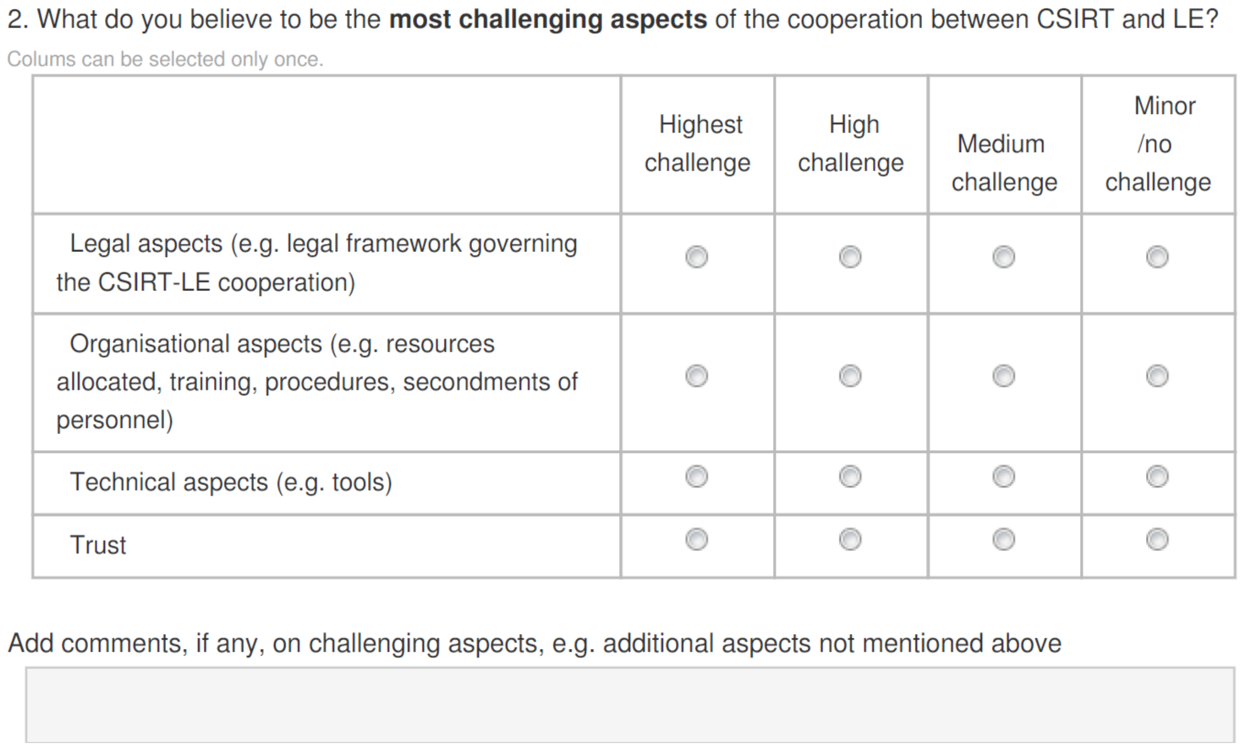


1. In your experience what is the **most important success factor** in the cooperation between CSIRT and law enforcement?

Columns can be selected only once

	Most important	Important	Medium important	Low important/not important
Legal framework	○	○	○	○
Procedures in place	○	○	○	○
Technical tools (e.g. applications, platforms)	○	○	○	○
Trust	○	○	○	○

Add comments, if any, on success factors, e.g. additional success factors not mentioned above

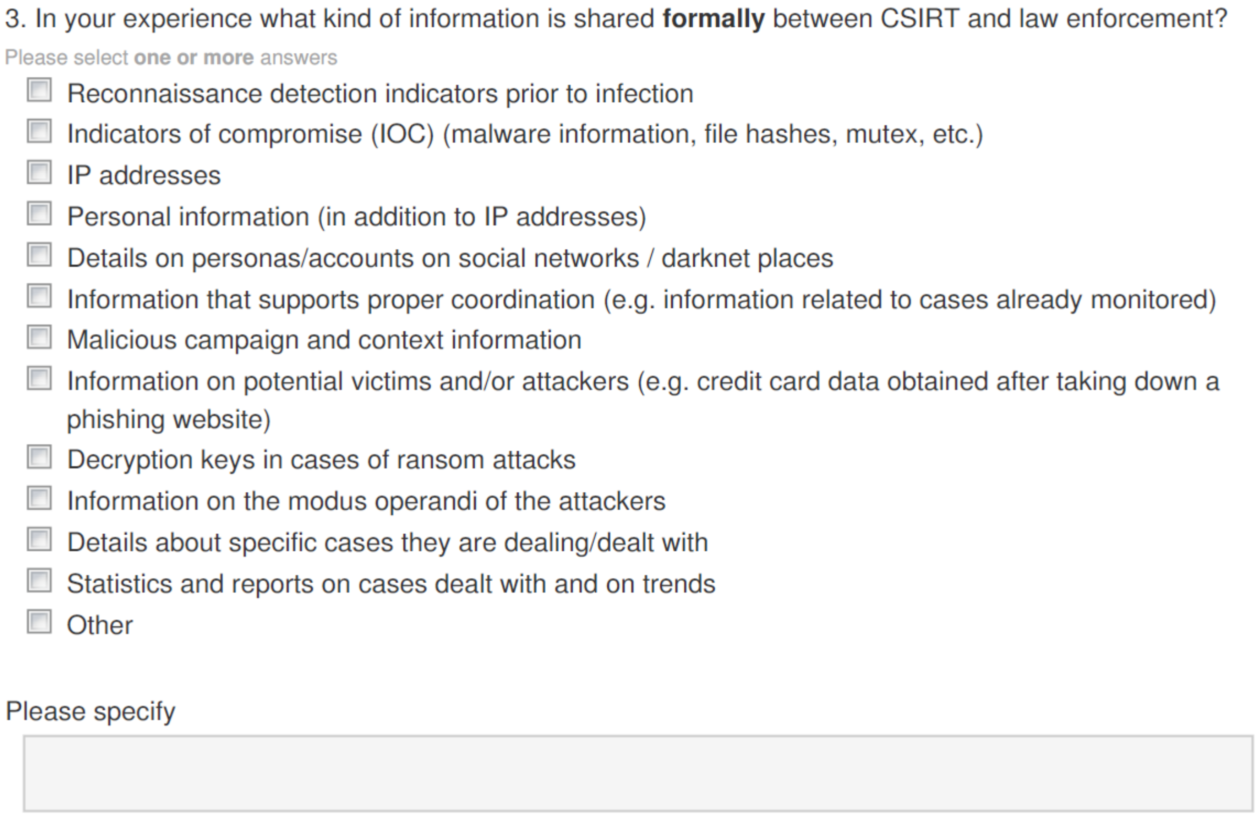


2. What do you believe to be the **most challenging aspects** of the cooperation between CSIRT and LE?

Colums can be selected only once.

	Highest challenge	High challenge	Medium challenge	Minor /no challenge
Legal aspects (e.g. legal framework governing the CSIRT-LE cooperation)	○	○	○	○
Organisational aspects (e.g. resources allocated, training, procedures, secondments of personnel)	○	○	○	○
Technical aspects (e.g. tools)	○	○	○	○
Trust	○	○	○	○

Add comments, if any, on challenging aspects, e.g. additional aspects not mentioned above

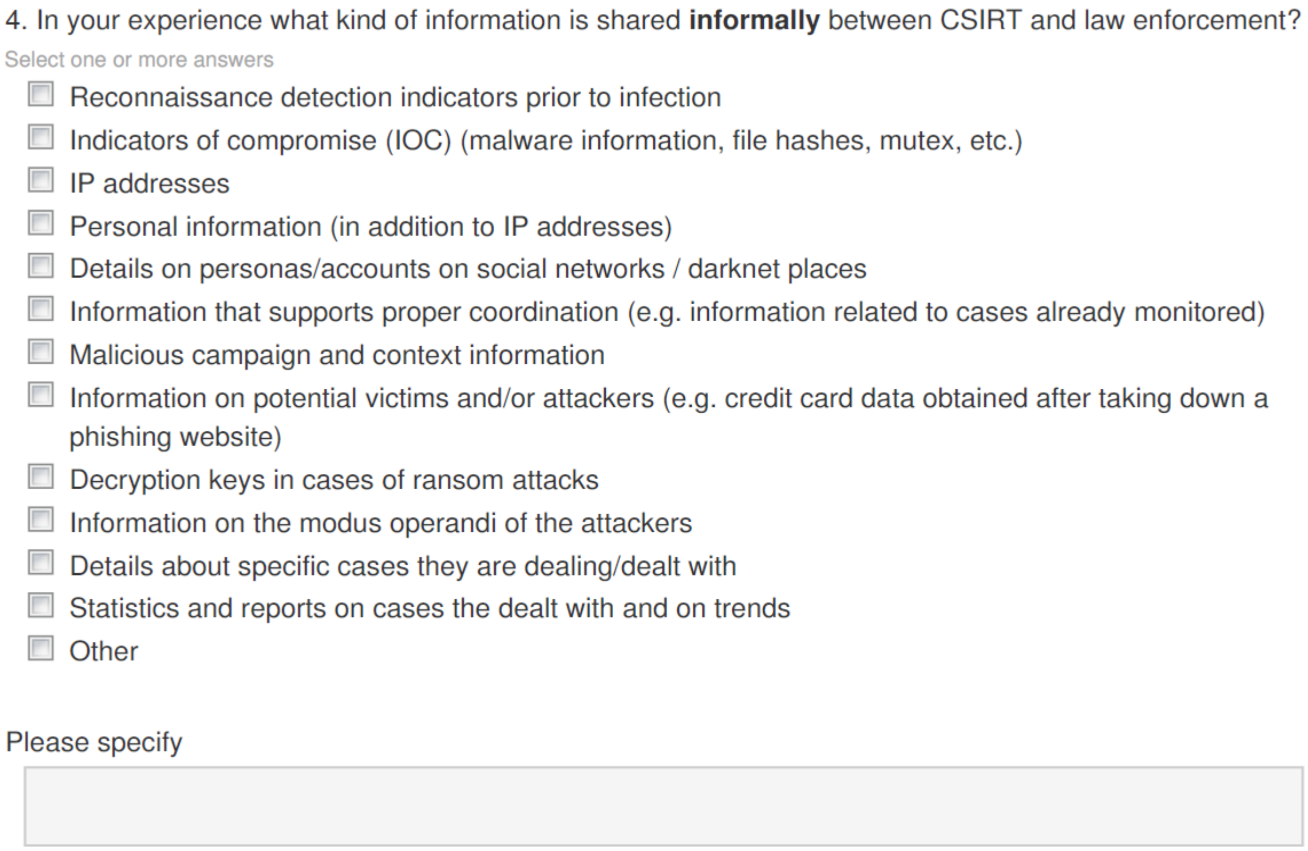


3. In your experience what kind of information is shared **formally** between CSIRT and law enforcement?

Please select **one or more** answers

- □ Reconnaissance detection indicators prior to infection
- □ Indicators of compromise (IOC) (malware information, file hashes, mutex, etc.)
- □ IP addresses
- □ Personal information (in addition to IP addresses)
- □ 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 they are dealing/dealt with
- □ Statistics and reports on cases dealt with and on trends
- □ Other

Please specify

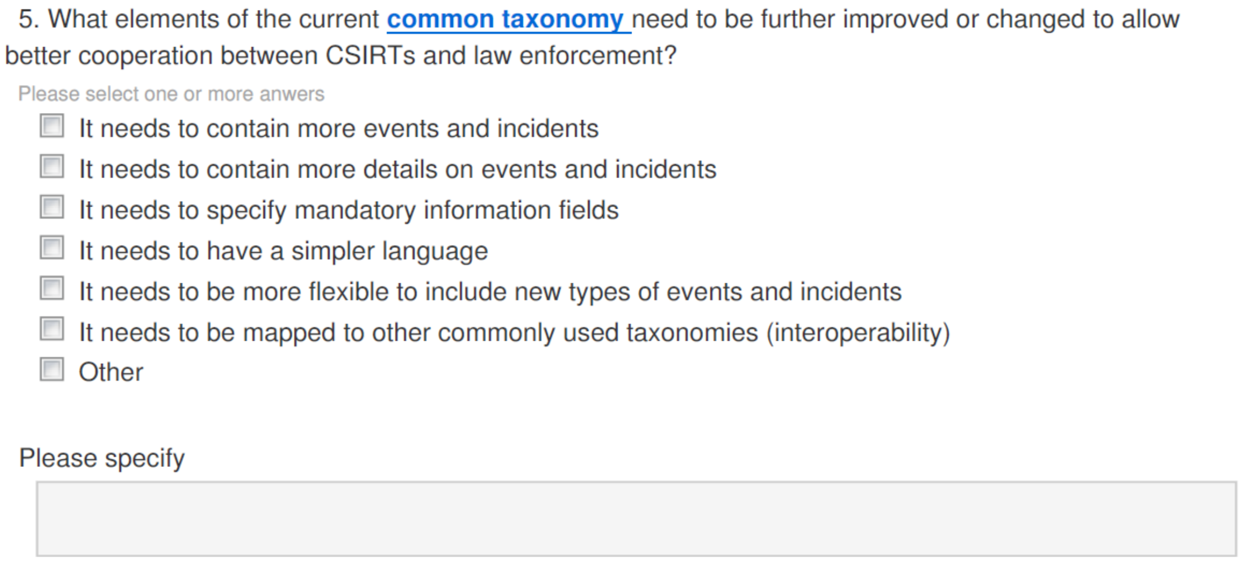


4. In your experience what kind of information is shared **informally** between CSIRT and law enforcement?

Select one or more answers

- □ Reconnaissance detection indicators prior to infection
- □ Indicators of compromise (IOC) (malware information, file hashes, mutex, etc.)
- □ IP addresses
- □ Personal information (in addition to IP addresses)
- □ 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 they are dealing/dealt with
- □ Statistics and reports on cases the dealt with and on trends
- □ Other

Please specify

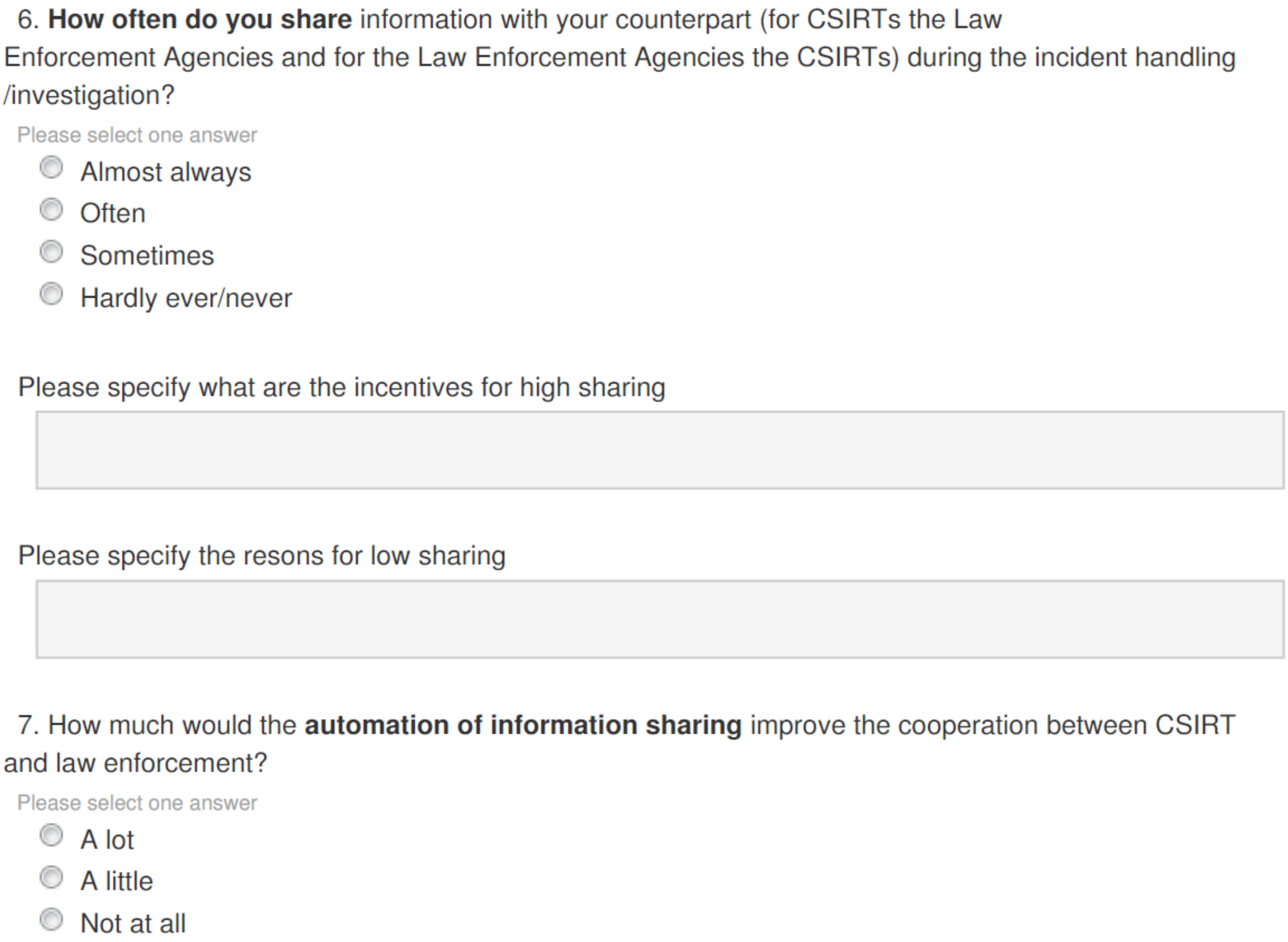


5. What elements of the current **common taxonomy** need to be further improved or changed to allow better cooperation between CSIRTs and law enforcement?

Please select one or more anwers

- □ It needs to contain more events and incidents
- □ It needs to contain more details on events and incidents
- □ It needs to specify mandatory information fields
- □ It needs to have a simpler language
- □ It needs to be more flexible to include new types of events and incidents
- □ It needs to be mapped to other commonly used taxonomies (interoperability)
- □ Other

Please specify



6. **How often do you share** information with your counterpart (for CSIRTs the Law Enforcement Agencies and for the Law Enforcement Agencies the CSIRTs) during the incident handling /investigation?

Please select one answer

○ Almost always
○ Often
○ Sometimes
○ Hardly ever/never

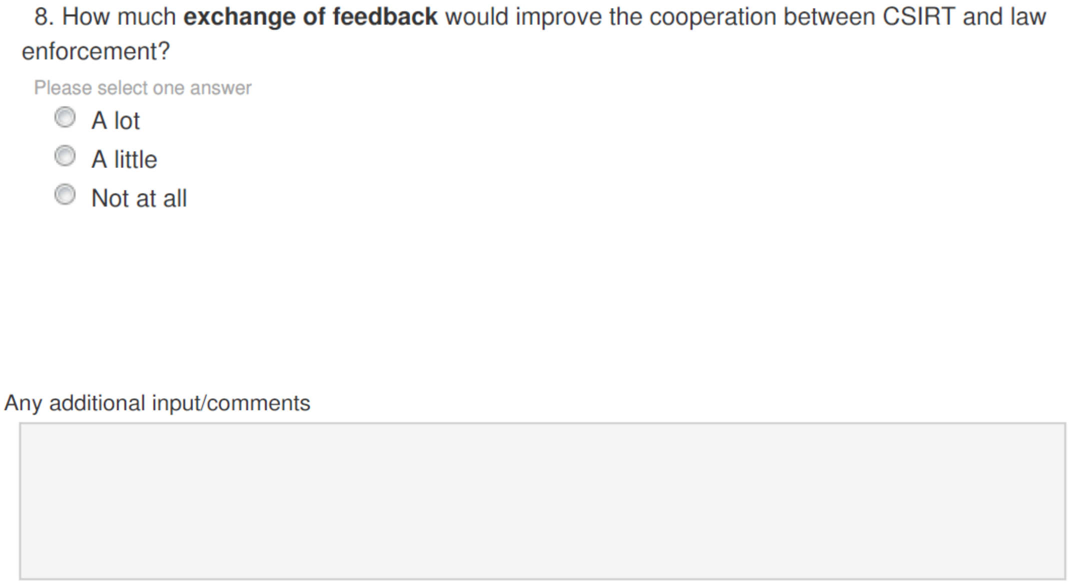
Please specify what are the incentives for high sharing

Please specify the resons for low sharing

7. How much would the **automation of information sharing** improve the cooperation between CSIRT and law enforcement?

Please select one answer

○ A lot
○ A little
○ Not at all



8. How much **exchange of feedback** would improve the cooperation between CSIRT and law enforcement?

Please select one answer

○ A lot
○ A little
○ Not at all

Any additional input/comments

Annex D: Samples of Material Collected During the Desk Research Not Included in the Bibliography/References

Bachmaier Winter, L., Section III – Criminal Procedure. Information Society and Penal Law., Revue internationale de droit pénal, 2014, p. 75 ff.

Benoliel, D., Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study. 16 North Carolina Journal of Law & Technology, 2015, p. 435.

Brenner, S.W., Cybercrime, cyberterrorism and cyberwarfare. Revue internationale de droit pénal, 2006/3, p. 453-471.

Cassim, F., Adressing the spectre of cyber terrorism: a comparative prospective. Potchefstroom Electronic Law Journal, vol. 15, n. 2, 2012

Cichonski P., Millar T., Grance T. and Scarfone K., "Computer Security Incident Handling Guide," U.S. Department of Commerce, National Institute of Standards and Technology (NIST), 2012.

Cormack, A., Can CSIRTs LawFully Scan for Vulnerabilities. Scripted, Vol. 11, Issue 3, 2014, p. 308-319.

Cormack, A., Incident Response: Protecting Individual Rights. Scripted, Vol. 13, Issue 3, 2016, p. 258-282.

Christou, G., Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy (New Security Challenges), 1st ed., Palgrave Macmillan, 2016.

Daniele, M., Evidence Gathering in the Realm of the European Investigation Order. From National Rules to Global Principles. *New Journal of European Criminal Law*, 2015, 6 (2), ff. 179-194.

Egan, B.J. and J.D., Remarks on new legal frontier: International Law and Stability in Cyberspace. 35 Berkeley Journal of International Law, 2017, p. 169 ff.

ENISA, Study on CSIRT Maturity – Evaluation Process, Athens, Greece, 2017.

ENISA, Deployment of Baseline Capabilities of National/ Governmental CERTs, Athens, Greece, 2012

European Parliament, Policy Department C: Citizens' Rights and Constitutional Affairs Civil Liberties, Justice and Home Affairs, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf [Accessed 02 October 2017]

European Parliament, "Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses," European Parliament, Brussels, Belgium, 2015.

Europol, "Internet Organised Crime Threat Assessment (IOCTA)," European Police Office (Europol), The Hague, Netherlands, 2016.

Hamed, E. M. and Sedky, M.H., A High Secured, Cost Effectively E-Voting System, 5 International Journal of Information Security and Cybercrime, Vol. 5, Issue 1, 2016, pp. 9-29.

Freitas, P.M. and Goncalves, N., Illegal Access to Information Systems and the Directive 2013/40/EU, 29 Int'l. Rev. L. Comp. & Tech., 2015, p. 1 ff.

Garrie, D. and Reeves, S.R., An unsatisfactory State of the Law: the limited options for a Corporation dealing with cyber hostilities by States, 37 Cardozo Law Review, 2016, p. 1827.

Klip, A., Section IV, International Criminal Law. Information Society and Penal Law. General Report. Revue internationale de droit penal, 2014, p. 386 ff.

Kelly, T.K. and Hunker, J., Cyber Policy: Institutional Struggle in a Transformed World, 8 A Journal of Law & Policy for the Information Society, 2012, p. 211.

Kostoris, R.E., A European Public Prosecutor Office against Euro-financial Crimes: which future? Journal of Eastern-European Criminal Law, 2015, 2, ff. 27-32.

Lalas, E., Mitrou, L., Lambrinoudakis C., ProCAVE: Privacy-Preserving Collection and Authenticity Validation of Online Evidence. TrustBus, 2013, p. 137-148.

Luiijf, E. and Klaver, M., Governing Critical ICT: Elements that Require, 2 Symposium on Critical Infrastructures, 2015, p. 263-270.

Mitchell, W., Electronic commerce Law: Towards a dynamic approach to enhancing international cooperation and collaboration in cybersecurity legal frameworks: reflections on the proceedings of the workshop on cybersecurity legal issues at the 2010 United Nations Internet Governance Forum, 37 Law Review, 2011, p. 1745.

Naseri, A. and Azmoon, O., Proposition of Model for CSIRT: Case Study of Telecommunication Company in a Province of Iran, International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, 201.

Ruefle, R., "Defining Computer Security Incident Response Teams," 24 01 2007. [Online]. Available: https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams [Accessed 11 May 2017].

Signorato, S., Types and features of cyber investigations in a globalized world, Diritto Penale Contemporaneo, Trimestrale, 2016, p. 190-200.

Sloan, P., The reasonable information security program, 21 Richmond Richmond Journal of Law & Technology, 2014, p. 2 ff.

TF-CSIRT Trusted Introducer, Services for Security and Incident Response Teams, https://www.trusted-introducer.org [Accessed 02 October 2017]

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

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

TP-05-17-115-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-229-5
DOI: 10.2824/451887