Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement

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 paper, please use CSIRT-LE-cooperation@enisa.europa.eu.
For media enquires about this paper, 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:

  - CERT.be, Belgium
  - Team CIRCL - Computer Incident Response Center Luxembourg
  - EC3 EUROPOL
  - Italian National CERT (IT-CERT), Italy
  - Walter Coenraets, FCCU - Belgian Police, Belgium
  - Mircea Grigoraș, CERT-RO, Romania
  - Floor Jansen, NHTCU.NL, The Netherlands
  - Biserka Radeva, CERT Bulgaria
  - Edgars Tauriņš, CERT.LV, Latvia

- 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

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

  - Team CIRCL - Computer Incident Response Center Luxembourg
  - EC3 EUROPOL
  - François Beauvois, French Cyberintelligence Division, CSIRT-POLICE JUDICIAIRE, France
  - Pieter Rogaar, NCSC-NL, The Netherlands

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: 978-92-9204-230-1, doi: 10.2824/177198

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 hit critical sectors brought about 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.

As mentioned in the Council Note of 31 May 2017 *Cybersecurity - Information from the Commission* (Council of the European Union, 2017a), "Conclusions drawn from the [WannaCry] attack include the need for CSIRTs, law enforcement authorities and the private sector to work together and the need for law enforcement authorities to have right tools to investigate these types of crimes and to prosecute criminals".

The technical aspects, including tools and methodologies used, are an important component of 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 framework and on the technical aspects of the cooperation, identifying current shortcomings, and formulating and proposing recommendations on technical aspects to enhance the cooperation. Moreover, the report presents a use case of cooperation between a CSIRT and a LEA as a real example of interaction between the different actors and of the methodology and the tools used for their cooperation.

The data for this report has been collected by means of a desk research, interviews with subject-matter experts, and an online survey.

The data collected confirmed that CSIRTs and LEAs exchange information often during incident handling/investigations, both formally and informally and that trust is the key success factor for the cooperation. CSIRTs and LEAs have different objectives and ways to collect and process information. However, between the two communities there is an increased reciprocal understanding of needs. According to the data collected, CSIRTs are more inclined to use open source tools, and the Malware Information Sharing Platform (MISP) is an example. The information sharing between CSIRTs and LEAs happens more *ad-hoc* than in a systematic manner. A common taxonomy for CSIRTs and LEAs has been developped (Europol - European Cybercrime Centre) and there are ongoing efforts towards a broader adoption and use of it.

CSIRTs and LEAs face some challenges when cooperate; these challenges are more legal and organisational than technical.

Core recommendations of this report to improve in particular the cooperation between national/governmental CSIRTs and LEAs in terms of tools and methodologies include:

- CSIRTs and LEAs community, ENISA, and Europol's EC3, should join efforts to **build and maintain a centralised repository of tools and methodologies, forms and procedures, used for the cooperation between CSIRTs and LEAs in the EU**;
- CSIRTs and LEAs community, ENISA, and Europol's EC3, should join efforts to **build and maintain a centralised repository of existing practices of cooperation between CSIRTs and LEAs in the EU**;

- LEAs should **maintain an updated list of LEAs Point of Contacts (PoCs) in which, whenever possible, liaison officers are indicated as PoCs;**
- ENISA and Europol's EC3, together with the CSIRT and LE communities should **keep up-to-date and further enhance, if needed, the common taxonomy for CSIRTs and LEAs and promote it**, **and** CSIRTs and LEAs should **adopt and use it**;
- CSIRTs and LEAs, with the support of ENISA and Europol's EC3, should **take advantage of MISP capabilities**;
- CSIRTs and LEAs should **define use cases for Threat Intelligence Platform (TIP) and real-time information sharing.**

In parallel to this report, ENISA has published a complementary report on *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (ENISA, 2017), which is available on the ENISA website.

1 Introduction

1.1 Purpose

The purpose of this report is to understand the technical aspects of the cooperation between CSIRTs - in particular national/governmental CSIRTs - and LEAs.

While this reports focuses on technical aspects, some considerations are also made about the legal and organisational aspects which are however addressed in more detail in the ENISA report on *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (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. CSIRTs, 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 “Provide guidelines on emerging trends, tools and methodologies to support LEA and CSIRT cooperations” (ENISA, 2017b).

1.3 Report Objectives and Scope

1.3.1 Report Objectives

The main objectives of this report are to:

- Discuss the current[1] general framework of cooperation between CSIRTs - mainly national/governmental - and LEAs;
- Provide information on technical aspects of this cooperation, in particular trends, tools and methodologies;
- Identify current shortcomings, especially technical, that CSIRTs - mainly national/governmental - and LEAs face in their cooperation;
- Formulate and propose recommendations on technical aspects to enhance the cooperation.

1.3.2 Report Scope

The report focuses on cooperation between in particular national/governmental CSIRTs and LEAs, although most considerations made are largely applicable to CSIRTs other than national/governmental too.

The geographical coverage is limited to the EU (European Union, 2017) and EFTA countries (EFTA, n.d.)[2]. 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 in the report.

[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.

1.4 Target Audience

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

Additionally, policy and law makers may benefit from select aspects of analysis as well 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 - listed in alphabetical order - apply:

- **BitCoin** is nowadays the most popular cryptocurrency (Bitcoin, n.d.).
- **Blockchain** is "a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions." (Blockchain Technologies, n.d.) Blockchain can be used for many applications, but it is mostly known as the mechanism that provides a ledger for cryptocurriences such as bitcoins.
- **Campaigns** are "instances of Threat Actors pursuing an intent, as observed through sets of Incidents and/or TTP, potentially across organizations" (STIX™ , 2017).
- **Capture-the-Flag (CTF)** competitions are educational exercises where participants are tasked to respond to a challenge e.g. exploit a web application, analyse a malware sample, and decipher a given ciphertext.
- **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, p. 112). 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, 2011)]. 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** here in most cases refers to the information sharing between CSIRT 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*. 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 and 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, 2015c, p. 12) (ENISA, 2016b, p. 10).

- **Cooperation** and **collaboration** here in this report are used as synonymous. They refer to the joint working together of CSIRTs and LEAs, their coordination of their actions, reciprocal help and joint 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.
- **Cryptocurrency** is a digital currency that uses cryptographic concepts for securing transactions and creation of currency units.
- **Cybercrime** is an umbrella term. An unequivocal definition of cybercrime does not exist, but in general we refer to it as "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, 2017b).
- **Dark web** is the web content that exist on overlay networks, which can only be accessed by using specific software and/or configurations and it's not indexed by standard search engines, while users also benefit from certain degree of anonymity in accessing it.
- **Encryption** is the application of a given algorithm on plain text to encode it so that the resulting ciphertext is no longer readable, except by someone in possession of the decryption key or password. Pretty Good Privacy (PGP) is proprietary encryption software used to secure (email) communications and data (files). It is based on the OpenPGP standard (defined by RFC4880) (IETF, 2007). GnuPG or GPG is a free implementation of the OpenPGP standard encrypting data and communication (GNU Privacy Guard, n.d.). Encryption is used to protect information and communications (for an overview of the use of encryption, see for instance (ENISA, 2016c, p. 10ff)). Encryption is essential to achieve secure internet communication. "[W]hile secure communication services have many legitimate purposes, they may also be used to plan and conduct criminal activities" (Europol and ENISA, 2016). It must be noted that "Law enforcement have a legitimate right to intercept communications in certain circumstances" (ENISA, 2016c, p. 9).
- **Governmental CSIRTs** are teams which 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, 2015e, p. 9).
- **Honeypot** is a security control that appears to be legitimate but is intentionally vulnerable so that it attracts the attackers' attention. Honeypots are closely monitored and the value of using them is the intelligence that can be extracted from the interaction of the attackers with them.
- **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).
- **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, 2019, p. 9).
- **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-LE 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 is collected (e.g. qualitative or quantitative) are collected and how (i.e. methods of data collection; see for example Chapter 2). 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).
- **Open Source Intelligence (OSINT)** is information that is gathered from publicly available sources such as the Internet, traditional media, photos, geospatial information (e.g. maps), conference proceedings, etc., used in an intelligence context.
- **Organisational aspects** in this report refer to those dimensions of the CSIRT-LE 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.)
- **Taxonomy** "is defined as a classification of terms. Three characteristics define a taxonomy:
  - a form of classification scheme to group related things together and to define the relationship these things have to each other;
  - a semantic vocabulary to describe knowledge and information assets; and
  - a knowledge map to give users an immediately grasp of the overall structure of the knowledge domain covered by the taxonomy, which should be comprehensive, predictable and easy to navigate" (ENISA, 2016a, p. 7)

  "There is currently no consensus on concepts and definitions related to taxonomies" (ENISA, 2016a, p. 5).
- **Technical aspects** refer to the dimensions of the CSIRT-LE cooperation that relate to the tools (e.g. applications, the platforms) and the methodologies used by the CSIRTs and LEAs to share information in their effort to fight against cybercrime.
- **Threat Information Sharing Platform or Threat Intelligence Platform** (TIP) is an emerging technology discipline that supports organisations' threat intelligence programmes. TIPs help organisations collect, normalise, enrich, correlate, analyse and share/disseminate threat related information and thus

playing a critical role in the threat management operations of the organisations (ENISA, to be published).

- **Tools** in this report refer to technical means employed in the cooperation between CSIRTs and LEAs to fight against cybercrime, such as the applications and the platforms used.
- **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. a).
- **Trends** is a word used with a variety of meanings but for the purposes of this report is taken to mean "a change or development towards something new or different" (Collins, n.d.).

2 Methodology

This chapter outlines the research methodology that was chosen and the data collection approaches used to conduct the research for this report.

To collect data for this report mainly a qualitative methodological approach has been used: 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 was also collected: an online survey was 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 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 certain specific topics that the project team deemed appropriate to examine in more depth following the analysis of the data collected via the interviews. These included areas such as information sharing taxonomies, information sharing tools and platforms, information sharing groups and initiatives, malware and cybercrime trends (ransomware, distributed denial-of-service, darknet markets, cybercrime as a service, payment fraud, social engineering, etc.) and crypto currencies used by cybercriminals.

2.1.2 Interviews

Structured interviews were carried out with sixteen subject-matter experts from eleven Member States; eight experts were from the CSIRTs community, six from the LEA community, and two belonging to both communities. In addition, an interview was carried out with a representative from Europol.

In one instance an interviewee instead of providing data via interview validated the data collected from a previous interview with other representatives of his country.

The interviews were carried out in May, June 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.

A questionnaire (see Annex B: Samples of Questionnaires to Support the Interviews) was prepared to support the interviews both with CSIRTs and LEAs. Some were open questions, while most were yes/no questions. For all questions, including yes/no questions, 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 with incidents such as the WannaCry and 'NotPetya' ransomware attacks.

The questionnaire - although initially conceived mainly as a support for the interviews - was also used to collect some written replies from interviewees who, also in the light of their direct engagement in the response to aforementioned attacks, were not available for an interview and they preferred to provide input by replying to the questionnaire.

Some data collected for the ENISA report on *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (ENISA, 2017) 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.

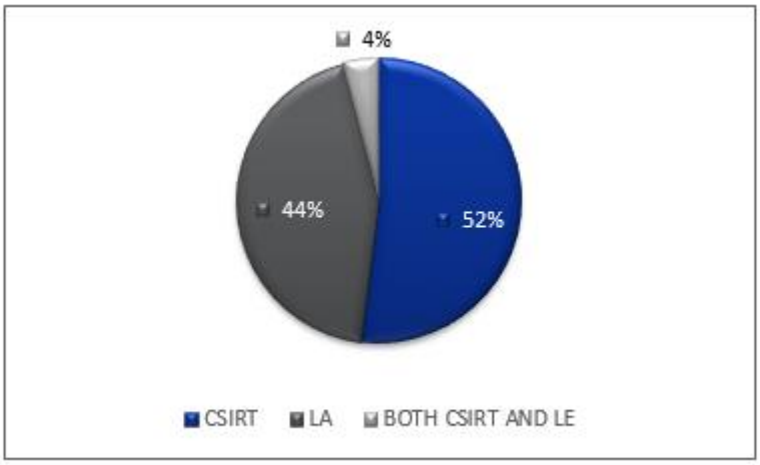
The survey was developed by using the EUSurvey, a survey tool which is "supported by the European Commission's ISA programme, which promotes interoperability solutions for European public administrations" (European Commission, n.d. b).

The invitation to complete the survey was sent to a 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, 2017b, 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 the interviews and used to produce some simple statistical graphs.

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 the Communities To Which the Respondents to the Online Survey Belong



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 *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (ENISA, 2017).

2.2 Selection and Classification of the Stakeholders

The project team discussed and agreed on some criteria to use to ensure contribution of a wide range of stakeholders. The following criteria were used for the selections of interviewees and peer-reviewers:

- CSIRTs/LEA community
- Geographical location
- Size of country in terms of population
- Level of maturity in CSIRT-LEA cooperation
- Size of the CSIRT

The stakeholders interviewed, consulted and taken into account for this report include:

- CSIRTs, in particular national/governmental CSIRTs
- LEAs
- European Commission and other EU institutions/agencies, including Europol’s EC3

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* with their expertise in NIS aspects of cybercrime, including but not limited to CSIRT and law cooperation and operational cooperation and information sharing to handle incidents and to fight cybercrime.

In addition to some ENISA reviewers, four external experts/organisations from the CSIRT and LE communities peer-reviewed this report in two rounds: one reviewer reviewed an intermediate draft in August 2017, three a semi-final draft in September/October 2017. Their feedback was incorporated in the final draft.

3 Cooperation Framework

3.1 Preliminary Observations

This chapter gives some preliminary remarks related to the context surrounding the CSIRTs and LEAs cooperation to fight against cybercrime.

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

In the absence of a globally accepted unequivocal definition, cybercrime in general can refer both to crimes having a computer as a target and crimes where computer is a tool to commit traditional or new crimes. By incident it is meant "any event having an actual adverse effect on the security of network and information system" (European Parliament and Council of the European Union, 2016a) (see in particular Article. 7 par.7).

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 the 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 do no not fall into the concept of incident.

3.1.2 Cooperation Does Not Take Place for All Cybercrime Cases

There are some cases where cooperation between CSIRTs and LEAs does not occur. For example, a crime under police investigations involving computers which is not an incident (see 3.1.1), or an incident which is not reported as a crime. Some CSIRTs have a legal obligation to report "crimes" but in practice this seems not to be feasible for all reported computer security incidents. The cooperation often depends on the willingness of the victim to report the crime to the police or the judgement of the CSIRT on the seriousness of the issue report themselves (if feasible).

3.1.3 CSIRTs and LEAs are Different Communities with Different 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.

The situation might be different than described above however for the national/governmental CSIRTs located in the intelligence community. Those CSIRTs are generally bound by a strict procedural approach of following procedures and hierarchical authority, save the requirement to adhere to Penal Law procedures. For this reason, those teams might be more similar in their culture and procedures to the LEAs.

3.1.4 CSIRTs and LEAs, and Other Actors

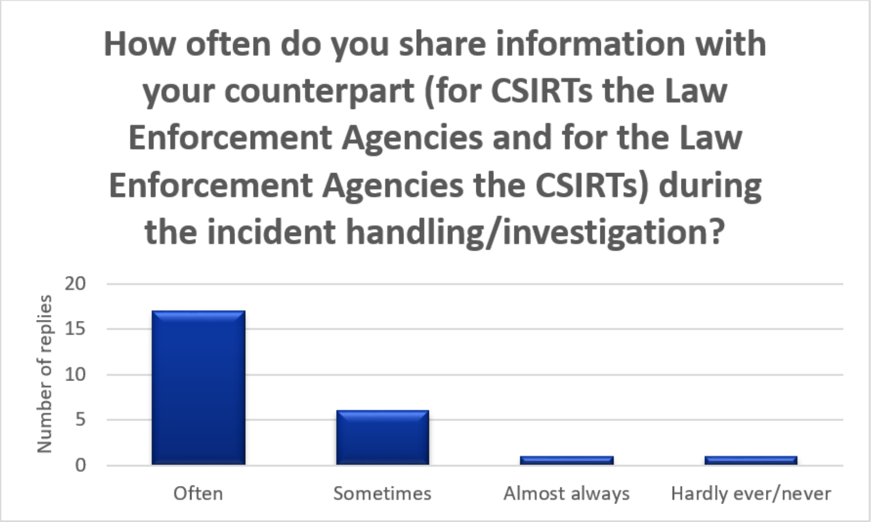
CSIRTs and LEAs are not the sole actors when it comes to dealing with cybercrime. Their cooperation does not occur in an environment where no other actors play a role and where there is no interaction between CSIRTs and LEAs with other subjects. On the contrary, there are several other actors that are part of the scene. Some examples of actors are listed below. It must be noted that there might be overlaps between the different actors mentioned below and that some of them are public, other private, other might be either private or public.

- The **criminal** - or more correctly as far as they have not been 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 the incident handing and the crime investigation;
- The **IT security companies**, and private sector in general, that provide information and solutions, in some cases even in real time during the incident mitigations and criminal investigations;
- The **national cyber security authorities** (e.g. cyber security centres);
- The **intelligence community**;
- The **military**;
- The **subject-matter experts** who may belong to one of the organisations mentioned in this list or may act as individuals;
- The **CSIRTs Network** that as provided in art. 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 and *fora***, including FIRST;
- The "**informal" 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'sEC3, 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" (Europol, n.d. a);
- **CERT-EU**, the "Computer Emergency Response Team […] for the EU institutions, agencies and bodies" (CERT-EU, n.d.);
- The **international law enforcement agencies**, including INTERPOL (INTERPOL, n.d.);
- **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 Frequency of the Information Sharing between CSIRTs and LEAs During the Incident Handling/Investigation

According to the data collected via the online survey, during the incident handling/investigation both CSIRTs and LEAs exchange often between with their counterpart's information. See Figure 2.

Figure 2 - Frequency of Information Sharing between CSIRT-LE During Incident Handling/Investigation, According to Data Collected Via the Online Survey



3.1.6 Modes of Cooperation

There are public and private CSIRTs. Services offered, consistency, size and maturity level vary considerably from CSIRT to CSIRT.

National and governmental CSIRTs - which together with law enforcement are the main focus of this report - 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, 2015d, p. 9).

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

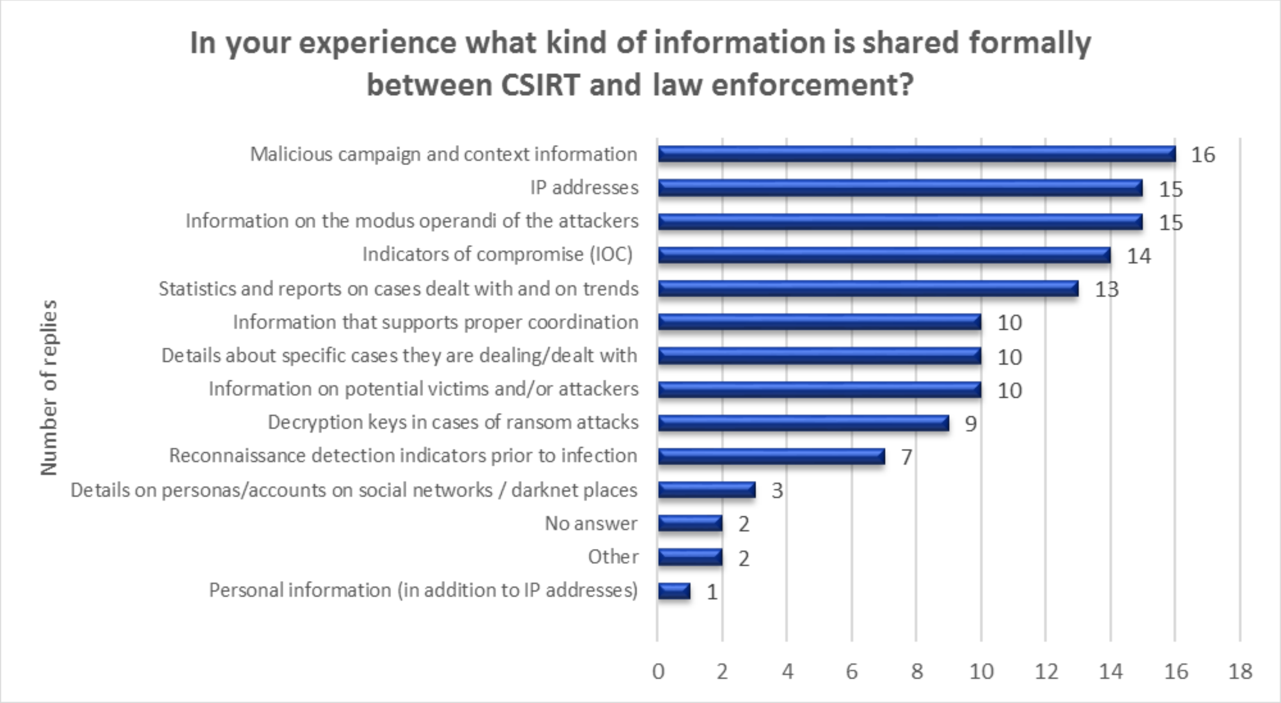
Like CSIRTs, there are many kinds of LEAs. For instance, there are local, federal, national, supranational and international LEAs. Also responsibilities and powers might vary from LEA to LEA. There are LEAs that specialise in cybercrime investigations. Also size and resources of LEAs might be quite different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

The kind of CSIRT and the kind of LEA may influence their cooperation in their fight against cybercrime. This in addition to other possible factors such as the presence or not of liaison officers or of seconded personnel, whether the employees of the CSIRT are government employees or not, country (including the national legal framework).

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.

According to the results from the online survey shown in Figure 3, the kind of information most shared formally between CSIRTs and LEAs are: malicious campaign and context information, IP addresses, and information on the *modus operandi* of the attacker and indicators of compromise (IOC).

Figure 3 - Information Shared Formally between CSIRTs and LEAs according to the Online Survey



In addition to information share formally, CSIRT and LEAs share information informally.

According to the results from the online survey shown in Figure 4, 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 4 - Information Shared Informally According to the Data from the Online Survey

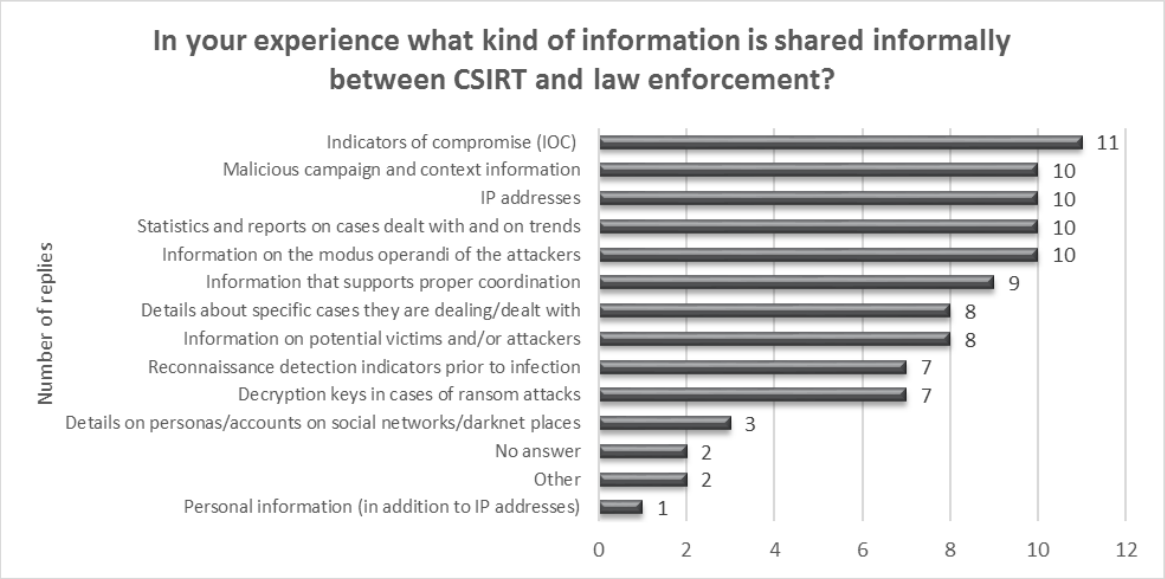
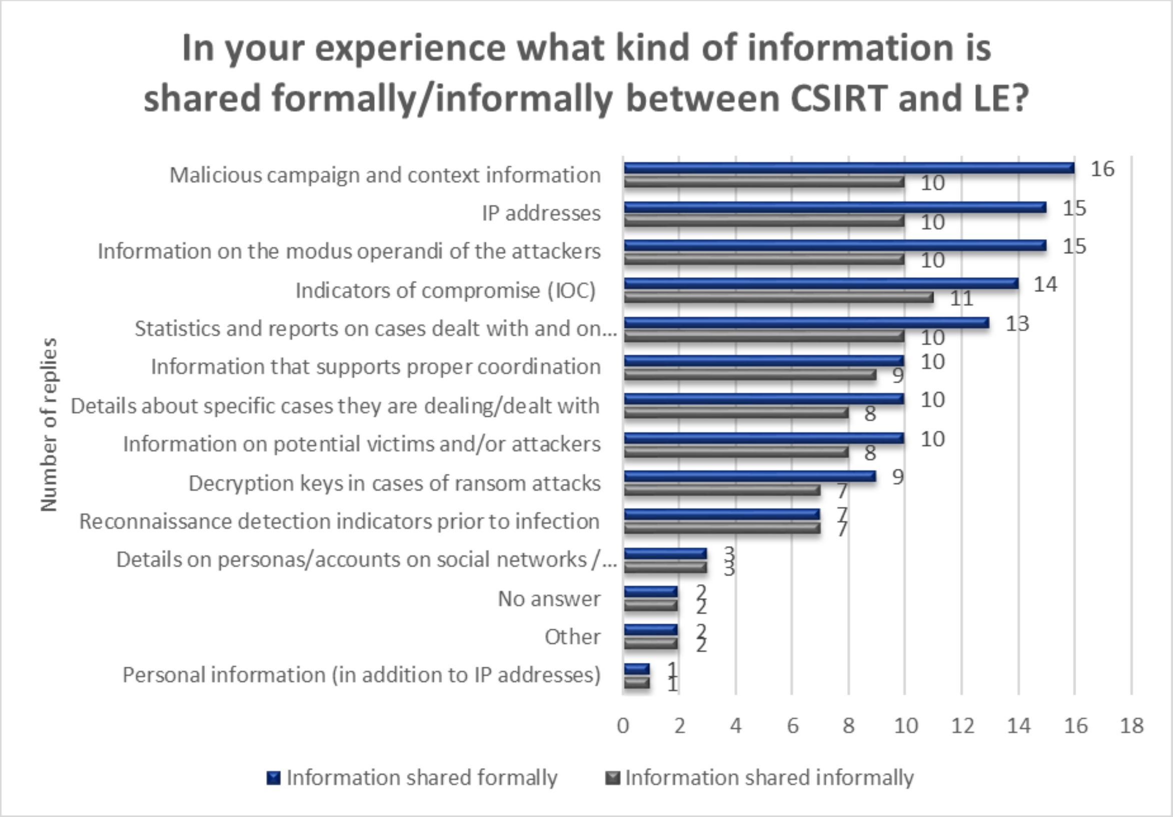


Figure 5 provides some compared data regarding which data are shared formally and informally.

Figure 5 - 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) do not seem to be often object of information sharing between CSIRTs and LEAs, neither formally, not 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 officer). 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.

The usage of cyber security frameworks as reference in the cooperation or the need for using one was not the object of specific questions neither in the interviews nor in the online survey. Respondents however had the opportunity to add additional information to their replies, but none indicated that they use cyber security frameworks specifically for cooperation or they feel that there is a need for it in their cooperation. Similarly, the data collected did not provide indication that specific severity levels classifications are used for the cooperation or that CSIRTs and LEAs are reciprocally aware of the severity levels that they refer to. These might be topics that could be explored in future studies and reports.

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

The legal and policy context play an important role in governing and shaping the cooperation between CSIRTs and LEAs in fighting cybercrime. A brief overview of the main legislative framework is given below. More information on the legal aspects of the CSIRT-LEA cooperation can be found in ENISA report on *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (ENISA, 2017).

At the international level, the Council of Europe Convention on Cybercrime (Council of Europe, 2001), often referred to as “Budapest Convention” is the first international treaty and remains the most relevant international treaty on cybercrime and electronic evidence. It is the “only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty” (Council of Europe, n.d.).

At EU level several legal and policy instruments are particularly relevant when discussing the cooperation between CSIRTs and LEAs, *inter alia*:

- Directive on Attack against Information System (European Parliament and Council of the European Union, 2013a)
- Europe 2020 (European Commission, 2010a)
- Digital Agenda for Europe (European Commission, 2010b)
- Digital Single Market Strategy for Europe (DSM) (European Commission, 2015a)
- Cyber Security Strategy (CSS) (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013)
- Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2017)
- Commission Reccomandation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (“Blueprint”) (European Commission, 2017a)

- NIS Directive (European Parliament and Council of the European Union, 2016a)
- Commission Communication on Strengthening Europe's Cyber Resilience System (European Commission, 2016)
- European Agenda for Security (European Commission, 2015b)
- European Investigation Order (European Parliament and Council of the European Union, 2014)
- Regulation establishing the European Public Prosecutor's Office (EPPO) (Council of the European Union, 2017)
- EU data protection legislation, including the General Data Protection Regulation (GDPR) (European Parliament and Council of the European Union, 2016b), Directive on Privacy and Electronic Communications (European Parliament and Council of the European Union, 2002), Law Enforcement Data Protection Directive (LEA DP Directive) (Council of the European Union, 2008)
- Directive on 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)
- ENISA Regulation (European Parliament and Council of the European Union, 2013b)
- Europol Regulation (European Parliament and Council of the European Union, 2016d)
- EU funding – H2020 programme (European Commission, n.d. c), e.g. Secure Sociaties
- EU funding – Connecting Europe Facility (CEF) (European Commission, n.d. a) – Digital Service Infrastructures
- EU funding – Internal Security Fund (ISF) (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).

Also the national legal and policy framework governs and shapes 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.

4 Emerging Trends, Tools and Methodologies, and Challenges of the Cooperation between CSIRTs and LEAs in the Fight against Cybercrime

This chapter addresses emerging trends, tools and methodologies as well as challenges of cooperation between CSIRTs and LEAs.

Before discussing these topics, a use case is described below with the aim to provide the reader with a real example of interaction between the different actors and of the methodology and the tools used for their cooperation.

A Use Case of CSIRT-LEA Cooperation

Context

In the second half of 2016, The Romanian National CSIRT - CERT-RO received a written request from the LE (Romanian Police) to provide technical support in a cyber-crime investigation related to a phishing campaign targeting a Romanian bank and its clients. That request was made in the context of the already established cooperation framework and according with the pre-defined form for data exchange between the two entities.

CERT-RO received copies of three KVM[3] based virtual machines acquisitioned by LE because they were found to be part of the phishing campaign, with the task to conduct a Digital Forensics analysis to try to identify potential victims and useful data that could help in the process of attribution.

Cooperation Methodology and Tools

Initially, CERT-RO provided various technical findings like the roles of the virtual machines (network traffic tunnelling through other compromised systems, hosting of phishing webpages, scanning for additional vulnerable hosts etc.) and used scripts and tools. After this phase, a closer cooperation was established on this case, with LE experts being more involved in defining what information is more important for the success of the investigation and in which order. LE experts provided CERT-RO with feedback on how the information provided was useful for the investigations.

It was determined that one important piece of information would be to determine the list of potential victims of the phishing campaign investigated, a type of information also requested by the prosecutor.

Further on, after potential victims were identified, the investigation moved to extracting information that could help to the attribution of the attacks: IP addresses used to connect to machines via SSH, source code of the scripts identified on the machines (including comments).

The tools used for cooperation and information exchange between CERT-RO and LE were OpenPGP encrypted emails and phone calls. A special role was played also by the LEA liaison officer, a seconded employee from LEA to CERT-RO.

One particular whois tool developed in-house by CERT-RO proved to be very useful in the investigation process of this case, in the sense that helped to automatically find useful information about more than

[3] Kernel-based Virtual Machine (KVM) is a virtualization infrastructure for the Linux kernel that turns it into a hypervisor (KVM, n.d.).

130.000 IP addresses identified during investigation, used by the victims or by the attackers, like geolocation and ISP.

Results

CERT-RO experts were able to identify a list of IP addresses that connected to the phishing pages (potential victims) and a collection of data from the victims (login credentials for different accounts and banking services).

Using Digital Forensics tools and techniques, it was discovered that access logs corresponding to one of the phishing pages were previous deleted from two IP addresses located in Romania, a finding that proved to be of great value in solving the case. Moreover, the suspicion that the attackers are form Romania has been strengthened by the fact that source code of the attacker tools contained comments in Romanian.

In the first part of 2017 a number of four people have been charged in this case for fraudulent financial operations and organised criminal grouping.

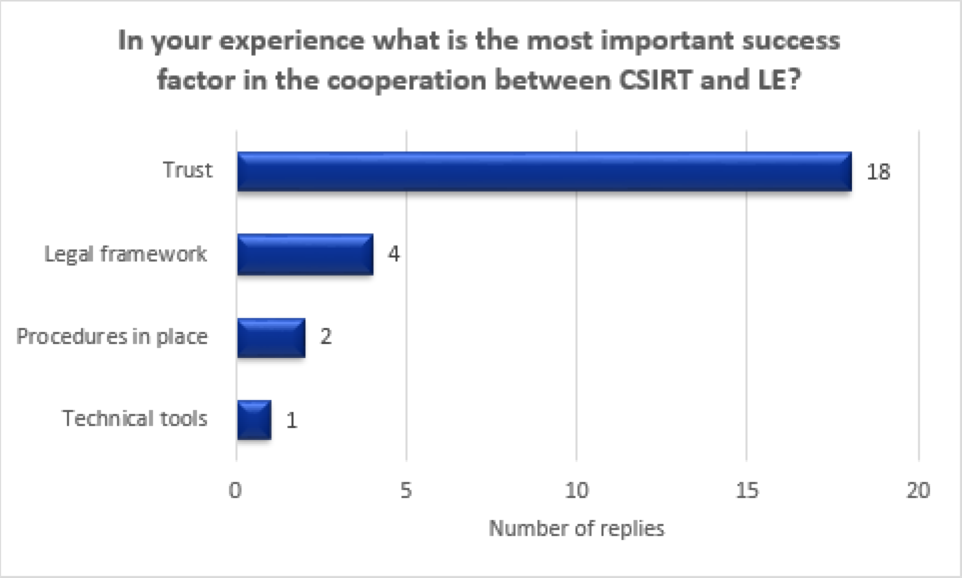
4.1 Emerging Trends

4.1.1 Trust Remains a Key Component for the Success of the Cooperation

According to the data collected, CSIRTs and LEAs agree that the most important element to facilitate their cooperation is the human factor. The vast majority of the respondents to the online survey (84% of the CSIRT community, 63% of LE community) replied that the most important success factor in the cooperation between CSIRT and law enforcement is the **trust**.

In Figure 6 an overview is provided on the most important success factors according to the respondents to the online survey.

Figure 6 – Most Important Success Factor in the Cooperation between CSIRTs and LEAs According to Data from the Online Survey



Although technical solutions certainly help to exchange the low-level bits and bytes, the real strength of cooperation lies in a common level of trust and understanding established by connecting humans.

To improve and further expand their mutual collaboration, trust is needed, at all levels. CSIRTs and LEAs organise regular meetings to which all their partners participate to exchange information. These meetings allow the participants to get to know each-other and build up better personal relationships. Eventually it should evolve to a situation where “everybody knows everybody”.

CSIRTs can bring forward their expertise in setting up these formal and informal networks/meetings. These networks (such as TF-CSIRT, FIRST, the CSIRTs Network) have a proven track record for increasing the understanding and trust between the teams and their individual team-members. We now see similar initiatives emerging in the CSIRT-LEA world. Without the essential trust, no cooperation will take place.

4.1.2 Increased Need for Cooperation between CSIRTs and LEAs

The evolving threat landscape affecting Europe is a primary driver for the cooperation between CSIRTs and LEAs. The collaboration gets more and more intense: a number of attacks that hit almost all sectors increased the collaboration, partly out of necessity.

“In May 2017 the WannaCry ransomware attack affected more than 400,000 computers in over 150 countries. A month later, the "Petya" ransomware attack hit Ukraine and several companies worldwide” (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2017, pp. Footnote 5, p. 2). As stated in the Council Note of 31 May 2017 *Cybersecurity - Information from the Commission* (Council of the European Union, 2017a), the “Conclusions drawn from the [WannaCry] attack include the need for CSIRTs, law enforcement authorities and the private sector to work together and the need for law enforcement authorities to have right tools to investigate these types of crimes and to prosecute criminals.”

This increased collaboration also showed that CSIRTs and LEAs have more things in common than first thought of. However, differences remain, but this is mostly because of the difference in objectives between CSIRTs and LEAs. Because of this, cooperation and information exchange mostly happens in an *ad-hoc* manner and not systemically; this changes somewhat if liaison officers or seconded personnel are present. This does not alter the fact that there are some common driven investigations.

With this increase in the cooperation, it also became clear that it is important to document the collaboration procedures and communicate them to the outside world.

The increased collaboration is also highly facilitated by the engagement of CSIRTs - in particular national/governmental CSIRTs - and LEAs with ENISA and the different initiatives that were started out of this engagement. This includes the development of a taxonomy for CSIRTs and LEAs but also the design of a threat level assessment for signalling.

Installing the liaison officers (from national/governmental CSIRT to LE and vice versa), formalising information exchange and establishing common platforms has had a very positive impact on the cooperation, a conclusion that also results form the use case presented in the current report.

Although cooperation between CSIRTs and LEAs to fight terrorism is outside the scope of this report, it can be noted that none of the CSIRTs or LEAs interviewed reported that the changes in the terrorism threat level influenced their collaboration; they reported that they observed in some cases an increase in received calls but afterwards things tended return to “normal”. Some CSIRTs and LEAs reported the use of dedicated teams to handle terror threats but these work independent from the cybercrime team.

4.1.3 Information Sharing Remains Highly Dependent on Environment

As described above (see 3.1.5), according to the data collected via the online survey, during the incident handling/investigation both CSIRTs and LEAs share often information with their counterpart.

As emerged from the interviews, this information sharing is highly dependent on the environment and the type of information that is being requested.

There is a model where information sharing happens regularly, either weekly or monthly, also in the form of written reports. For example, the CSIRT provides some sort of "end-of-week" bulletin with the most important events that happened during the week. This is already a good practice in some Member States. As most organisations have a lack of resources and they are already overwhelmed with information streams it is important that this information is brought forward in an interesting and convenient format. It should entice the receiver to actually read the information and not merely glance through the message.

Longer term written reports are useful to present data on certain trends or changes in the landscape, for example an increase or decrease in cryptoware or a change in focus for criminals to a certain sector. A common problem for LEAs is that they suffer from the fact that a lot of cases are not reported to law enforcement, mainly due to the fact that this is often dependent on the victim. These long term written reports can then help LEAs to be better aware of what is going on, and as such provide them with improved situational awareness information.

Most of the longer term reporting is made available to the public, e.g. ENISA Threat Landscape (ENISA, n.d. b) and the Europol's Internet Organised Crime Threat Assessment (IOCTA) (Europol, 2017b).

Some agencies prefer to have these trending reports on a longer term basis whereas other agencies prefer to have this on short term notices. The latter with the specific motivation that it is the type of information that has to be signalled immediately for follow-up and not after a month in long-term trending reports.

A variant of short term reporting is the "on request" reporting. This is reporting where one organisation can ask the other if they have specific details on a new campaign or threat. This can happen for example when a LE wants to collect all available information on a certain victim. Some of these "on request" or *ad-hoc* reporting happens via the liaison officer.

4.1.4 Different Objectives, But Increased Reciprocal Understanding between CSIRTs and LEAs

Usually CSIRTs produce big data sets. This may represent a challenge for LEAs that may want to avoid being inundated by incident data. In addition, there is a difference in how CSIRTs and LEAs collect information. Whereas CSIRTs often process large sets of data and then distribute the relevant information to their constituency, LEAs require very specific information. LEAs often ask for a very specific piece of information and not a "bulk" set of data. Automation and basic filtering could be used to reduce the amount of data that a LEA needs to analyse to get the very specific data needed.

This difference in processing information can also be challenged by the different objectives (see 3.1.3) of CSIRTs and LEAs. It is important to clearly document what the participants are going to do with the information and to undertake a relevance check firstly and then inquire if the other organisation can process the data.

4.2 Tools, Methodologies and Joint Efforts to Develop and Make Tools Available

Based on the data collected, some considerations are made below on tools, methodologies. Some examples are also provided on joint efforts to develop/enhance tools and make them available to the community.

4.2.1 Tools

4.2.1.1 Basic/Standard Tooling

According to the data collected, the preferred tool of choice for exchanging information remains email. Because a considerable part of the cooperation between CSIRTs and LEAs happens in an *ad-hoc* manner, email is still the best tool to exchange information and to get the work done.

The data collected showed that, although GPG is highly adopted within the CSIRT world, it proves to be difficult to use it when exchanging information with LEAs. This is sometimes because of the fact that LEA personnel involved in the information sharing do not always have full control of their working environment (for security reasons, LE operates within secure network where only a few people have admin rights) and not all LEAs are able to support GPG.

Next to email, telephone communication is the preferred way of exchanging information.

Some teams collaborate via chat applications. Other viable options for secure communication include secure file exchange tools (over e.g. TLS) as well as secure audio and video conferencing tools (over e.g. TLS).

It appears that personal contact, for the moment, remains very important when it comes to a means of communication between CSIRTs and LEAs. The use of personal contacts and simple means of communication such as email and phone could be due to a number of reasons:

- As it is also apparent from the use case presented, email and phone are very well-known tools that are already used in day-to-day work and personal activities;
- They are a very flexible, efficient, convenient way of communicating at nearly no additional cost.
- From the operational point of view, any additional or increase in tools or platforms may lead to less efficiency and loss of focus;
- They do not raise the issue of "who owns and maintains the tool/platform".

4.2.1.2 Secure Communication over Government Networks

In several Member States there is an already established and secure (and sometimes segregated) Government network that can be used for secure communication. These types of network could be used as a communication path for exchanging information.

It seems that at least one Member State has an existing network and platform that is already used for regular (meaning non-IT) crisis handling. Participants to this network already speak the “crisis” language. The CSIRTs - in particular national and/or governmental - and LEAs can plug into this system during an IT crisis and use it for communication and information exchange.

4.2.1.3 Custom Tools

According to the data collected, CSIRTs seem to be more inclined to develop/maintain open source and in-house tools that they can configure according to their needs. When not developing in-house tools or using open source ones, CSIRTs prefer to buy very specialised software for their analysis e.g. reverse engineering software.

Although in some cases also LEAs develop in-house tools, it seems that more often they buy commercial licenses: LEAs might not have either the capabilities or the admin control of the system to be able to adapt or just install an open source tool (for security reasons, LE operates within secure network where only a few people have admin rights); in addition to this, LEAs cannot trust open source code without a deep insight analysis which usually results in acquiring a commercial software where they can ask for a trustable certification (regarding court issues) and responsbilities for possible bugs/backdoors.

LEAs work and needs seem to be well-addressed by the vendors and already existing hardware and software tools which cannot be said about CSIRTs community. As mentioned by some interviewees, sometimes the vendors try to treat CSIRTs as LEAs and propose them hardware and software known to be used by the law enforcement community.

4.2.1.4 Encryption

The data collected via the interviews showed that while CSIRTs generally support and use OpenPGP (standard as defined by RFC4880) implementations, LEAs seems to be less inclined to make full use of open source encryption tools. There are cases however where CSIRTs and LEAs make use of OpenPGP, as also highlighted in the use case presented in this report.

Some of the reasons that might make LEAs less inclined to use OpenPGP could be:

- OpenPGP is not formally recognised as a way of signing and encryption of documents (it must be noted that if any link in the chain of the investigation is not officially recognised by the court, the investigation might fail in its aims because the evidence collected might be declared inadmissible)
- Not all LEA personnel can fully manage their work devices and installed software (e.g. for security reasons, only a few people have admin rights), which represents a problem also for private keys management
- LEAs have formal secure communication channels to exchange information among the LE community

In some countries the law enforcement community uses special communication channels and platforms/tools that make use of commercial/proprietary encryption technologies. When it comes to CSIRTs, usually only the national/governmental ones are included in those special communication frameworks.

4.2.1.5 MISP

According to the data collected, open source tools like MISP are seen as the most suitable for future tooling. MISP usage is much more widespread in CSIRTs compared to LEAs. This is partly because of historical reasons (MISP is a community-driven project in which CSIRTs have played and play an important role) but also because of the fact that LEAs often exchange information via their own closed networks.

It is worth noting that there is an ongoing increase in the use of MISP by LEAs. One of the avenues taken to have more LEAs on board is by defining how information is going to be treated once it is put in MISP.

According to the data collected, some of LEAs see ENISA as a potential facilitator for adopting/promoting a taxonomy for CSIRTs and LEAs (ENISA and Europol, together with CSIRTs and LEA communities, are actually already working towards this end) that should be implemented in popular tools. The aforementioned taxonomy for CSIRTs and LEAs is already implemented in MISP.

MISP is a dedicated tool for information sharing primarily about malware samples and related malicious campaigns related to specific malware samples/variants. Some of the characteristics and advantages that explain the high adoption of the tool are:

- MISP is used for the sharing of structured information (primarily consumed in an automated manner – machine to machine) and unstructured information (allowing also human interaction)
- It offers architectural flexibility allowing the utilisation as a centralised platform (e.g. CIRCL and FIRST instances), but also as a decentralised (peer-to-peer) platform

- It allows the utilisation of separate sharing communities based on different criteria (per sector/country/special interest, etc.)

It is important to note that a separate community (or even better a separate MISP instance) can be used for information exchange between CSIRT and LEA. This way, there is no risk for potentially disclosing sensitive information with parties that should not.

4.2.2 Methodologies

4.2.2.1 TLP Used When It Comes to Cooperation Outside Law Enforcement

The Traffic Light Protocol (TLP) "can be used in all forms of communication, whether written or oral" (ENISA). As also highlighted in previous ENISA work (ENISA, 2015a, p. 9), most CSIRTs use the TLP, "while many LEAs use the NATO classification system [(NATO)]".

The FIRST Traffic Light Protocol Special Interest Group (TLP-SIG) governs the standard definition of TLP for the benefit of the worldwide CSIRTs community and its operational partners (FIRST, n.d.).

4.2.2.2 Multiplicity of Taxonomies and the Common Taxonomy for CSIRTs and LEAs

Several taxonomies have been developed in the past especially in the CSIRT community. An overview of the most common taxonomies and some "pros" and "cons" of each is available in the ENISA report on *Information sharing and common taxonomies between CSIRTs and Law Enforcement* (ENISA, 2015a). As observed in the ENISA report *A good practice guide of using taxonomies in incident prevention and detection* (ENISA, 2016a), "The high number[..] of taxonomies does not provide a clear indication on which taxonomy should be used for what use case". This becomes even more complicated when different communities, like CSIRTs and LEAs, are involved.

According to the data collected, the majority of CSIRTs use a taxonomy but it is not adopted for communication with LEAs. Most CSIRTs use a specific taxonomy (e.g. CIRCL, CERT.pt), but when working with LEAs they use different or simpler ones.

A common taxonomy for LEAs and CSIRTs exists. It has been developed (Europol - European Cybercrime Centre) based on the CERT.PT taxonomy, considered by the Operational Action Plan (OAP) 4.1 European Multidisciplinary Platform against Criminal Threats (EMPACT) (on OAP 4.1 working group see also (ENISA, 2015a, p. 11)) as an appropriate candidate for the exchange of information between the communities. The ENISA report on *Information sharing and common taxonomies between CSIRTs and Law Enforcement* "proposes the CERT.PT taxonomy as a common taxonomy for the exchange of information between CSIRTs and LEAs" (ENISA, 2015a, p. 48). The common taxonomy has been developed also taking into account most of the good practices gathered by ENISA from the CSIRT community (on this topic, see also (ENISA, 2015a)). Those include simple top level categorization, categories being mutually exclusive, an appropriate level of ease of use, and ease of understanding by external non-CSIRT entities, especially law enforcement community.

This common taxonomy has been already implemented and imported in MISP (GitHub, n.d. a).

ENISA and Europol's EC3, together with CSIRT and LEA representatives, work to further enhance, if needed, the taxonomy for CSIRTs and LEAs, and to keep it up-to-date. The taxonomy is expected to be reviewed and if needed updated annually. An updated version of the taxonomy is expected to be released at beginning of 2018.

This common taxonomy for CSIRTs and LEAs could be seen as a step towards a wider EU cyber taxonomy to support information sharing among different actors involved in the fight against cybercrime; this also in the light of Point (7) of the Commission Recommendation of 13 September 2017 on *Coordinated Response* *to Large Scale Cybersecurity Incidents and Crises* ("Blueprint") that advises that "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" (European Commission, 2017a).

4.2.3 Joint Efforts to Develop/Enhance Tools and Make them Available to the Community

Below two examples of joint efforts to develop/enhance tools and make them available to the community are briefly described.

4.2.3.1 Engagement with Academia

Some CSIRTs and LEAs currently engage universities on different levels and for different purposes but in general where there is an opportunity for collaboration to focus on research which is designed to provide "real world" solutions to given problems.

There is the opportunity for universities to provide a *forum* for academics and CSIRTs/LEAs to share research findings and explore knowledge transfer opportunities (on the topic of platforms to share knowledge, including between LE and accademia, see SPACE (Secure Platform for Accredited Cybercrime. Experts (Europol, n.d. b)).

In addition to research, universities may be able to support development of open source and in-house tools.

There is also the potential for the provision of skills development, vendor neutral training and certification from universities to CSIRTs and LEAs.

Academia could support the exploration of new technologies and problem domains identifying evidence sources especially those where no parsers currently exist. Additionally, academia could provide the resources for the development and provision of robust testing datasets and procedures for the evaluation of the accuracy of forensic tools.

4.2.3.2 No More Ransom Project

The "No More Ransom" website is "an initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre and two cyber security companies - Kaspersky Lab and McAfee - with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals" (No More Ransom, n.d.). The No More Ransom platform is available in twenty-eight languages and has one hundred twenty partners, the project is expected to continue playing a significant role against the ever-growing ransomware threats worldwide. The number of free decryption tools on www.nomoreransom.org is now fifty-two; they can be used to decrypt eighty-four ransomware families. This can be considered as an example of what "should be done to prevent and mitigate the impacts of cybercrime on end-users" (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2017, p. 11).

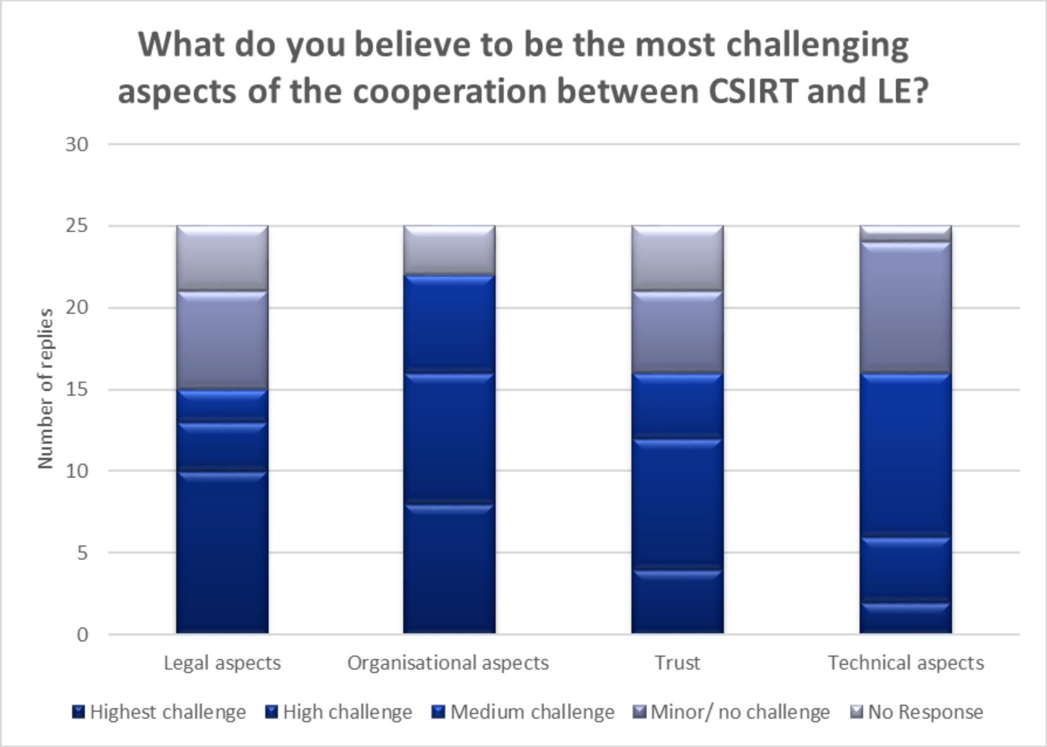
4.3 Challenges to the Cooperation

As mentioned above, this report focuses on technical aspects of cooperation between CSIRTs and LEAs to fight against cybercrime. For this reason, below the technical challenges are addressed in detail while the legal and organisational challenges only briefly. The legal and organisational challenges are addressed in detail in the ENISA report on *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (ENISA, 2017).

Before discussing the technical aspects, it is interesting to note that according to the data collected, in general, challenges are considered more related to legal and organisational aspects, and once these challenges have been resolved a technical solution will follow.

Also the results from the online survey showed that most challenging aspects of the cooperation between CSIRTs and LEAs are not technical. See Figure 7 below.

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



4.3.1 Technical Challenges

Among the few technical challenges are those described below.

4.3.1.1 Continuous Software Update

CSIRTs and LEAs have different tooling needs: in-house compared to acquiring software (see section 4.2.1.3). This can result in a situation where CSIRTs have continuous updating of their tooling as being part of the development lifecycle, whereas LEAs might be more dependent on their provider. This can complicate cooperation if there is no backwards compatibility or because LEAs cannot make (promptly) use of new features. The issue with backwards compatibility can be countered by agreeing on a data exchange format, possibly with versioning.

In addition, because most CSIRTs can manage the software and hardware configuration of their own workstations they can make use of tools that are more difficult to get installed on LEAs workstations (for example PGP, see 4.2.1.4 - Encryption).

4.3.1.2 Different Technical Modalities Used by the Various CSIRTs and LEAs for the Information Sharing and for the Data Transmission Between Them

The exchange of information can happen via existing tools, for example MISP (see 4.2.1.5 - MISP). Most technical challenges for exchanging the structured information via MISP are covered within the MISP platform.

However, as the exchange often happens *ad-hoc,* the technical challenges are more to be found in the secure transmission of the information instead of in the actual information exchange toolset.

4.3.1.3 Lack of Common Tools and Technical Platforms, Integration Interfaces and Automation

There is a need for development of integration interfaces for different tools used and utilisation of a common language (taxonomy).

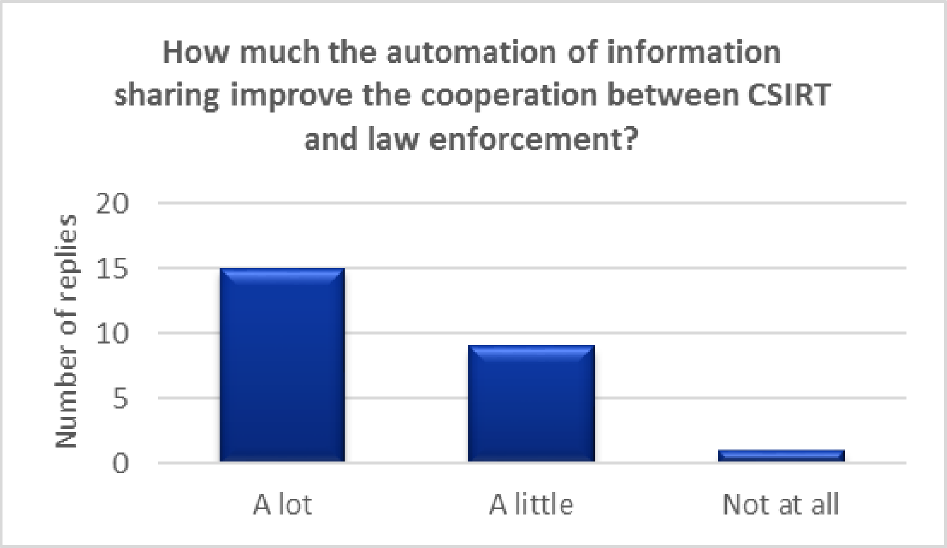
Coordination mechanisms need to be implemented in the tools/platforms used, in order to achieve a certain degree of automation in that regard. The use of similar functioning tools but even more the use of a common taxonomy would be of help to reach this objective.

4.3.1.4 Limited Real Time Means of Communication and Coordination, and Need for Increased Level of Automation

Phone and email have been identified as the most used means of communication. One generic challenge in terms of cooperation between CSIRTs and LEAs would be to adopt additional real time means of communication and coordination, especially to address those cyber threats, attacks or crimes that are characterised by short time periods of manifestation and high volatility in terms of digital evidence.

Real time communications need to be accompanied by an increased level of automation in terms of action taken by both CSIRTs and LEAs. As shown in Figure 8, according to the data collected via the online survey, automation of information would much improve the cooperation between CSIRTs and LEAs.

Figure 8 - Overview on How Much Automation Improves the Cooperation between CSIRTs and LEAs According to the Data Collected via the Online Survey



4.3.2 Legal and Organisational Challenges

As mentioned above, in this report only an overview of the legal/organisational challenges is provided. More information on this topic can be found in the ENISA report on *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (ENISA, 2017).

4.3.2.1 LEA Obligations and Constraints

According to the data collected, reporting incidents to LEAs is often see as a unidirectional. That is because LEAs have a legal obligation not to disclose when they deal with cases and the investigation is ongoing.

One of the challenges faced by CSIRTs and LEAs is the "you have to collaborate" versus "you cannot share information". A solution to address this would be both CSIRT and LEA writing down their current procedures for information sharing allowing the development of solutions.

Law makers need to be able to clearly see the existing processes and procedures of both CSIRTs and LEAs when drafting new laws. So when drafting new legislation or revising existing ones, law makers have a clear understanding of the practical framework that exists between CSIRT and LEA, allowing them to develop a legal context that has no negative impact on the cooperation, or even better that facilitates it.

When information is part of an ongoing investigation it might not be the appropriate moment to share it with external parties, due to the impact of data protection regulations as well as the confidentiality or secrecy of the investigation (which barrier or instantiation disallow the sharing of information with "external" partners). However, there might be other options for information sharing, for instance when LEA has the agreement of the prosecutor to communicate, e.g. for remediation purposes.

4.3.2.2 Coordinated Vulnerability Disclosure and Prosecution Risk

LEAs may not be able to cooperate in coordinated disclosure of vulnerabilities. There might be a prosecution risk unless there is a legal agreement with the organisation. On the contrary, sometimes national CSIRTs might act as a coordinator and neutral mediator, mediating the disclosure with the vendor and avoiding the exposure of the researcher.

Coordinated vulnerability disclosure has been investigated by the Dutch National Cyber Security Centre (NCSC) in depth and brought forward as a possible working concept. Some CSIRTs have provided guidelines on coordinated vulnerability disclosure, (see for instance, (National Cyber Security Centre, Ministry of Security and Justice, The Netherlands, 2013)). Some guidelines on this matter issued by LEAs and Data Protection Authorities might be of help too.

In addition, it must also be noted that some CSIRT members that are government employees might be required by law to report criminal acts (even if the discovery of a vulnerability was in good faith) and they might run into disciplinary measures or prosecution risks if they do not abide by applicable legal obligations.

4.3.2.3 Timely Collection and Court Order

From the CSIRTs and LEAs perspective, a major challenge is the timely collection of information, e.g. logs from Remote Access Tools (RATs) or logs from cloud services, since a court order is needed.

There are also differences in national legislation on when a LEA and a CSIRT should cooperate on seizing requests.

4.3.2.4 Protection of the Distributed Information

From the LEAs perspective, a major challenge is the protection of the distributed information (police officers are accountable and they need to know what information to share). This may hinder the information sharing between CSIRTs and LEAs and may act as a restraint on LEAs participation in MISP communities (or other information sharing communities). If LEA and non-LEA organisations participate in a common information sharing group (this could be a MISP group) there is a risk of an accidental sharing of the details of an ongoing investigation. However, it must be noted that in many cases there are only Indicators of Compromise in MISP, no details on victims or alike.

Instead of placing all of the information in the sharing process, it is important to ensure a relevance check on the information is undertaken beforehand to prevent the other partners being overwhelmed with data. A quality check is also needed so that the quality of the shared information can be guaranteed. The quality check could be enabled by technology e.g. mandatory fields of data, and input data verification. Customised MISP warning lists could be an initial verification means especially when LEAs use a Threat Intelligence Platform for sharing information (GitHub, n.d. b) (MISP Community).

The way in which information is shared is important as well as the type of information that can be shared and to whom. Data sharing depends on the degree of understanding and the background of individual actors. A good understanding of what a partner is going to do with the information allows sharing partners to assess how information is going to be processed and what possible consequences and actions might follow. Respecting the data markings (e.g. TLP) is critical so that mishandling of sensitive information as well as operation failures does not occur.

4.3.2.5 Lack of Resources, Especially for LEAs

One major challenge for LEAs is the lack of resources and people so that they can for example participate in training/exercises related with their duties. Examples are training on forensics, malware reversing, programming and analysis capabilities, which are the disciplines needed by a cybercrime investigator on a daily basis. Some interviewees also mentioned CTF (Capture-the-Flag) and red/blue team exercises. As mentioned above in 1.5 - Key Concepts and Definitions, CTF are educational exercises where participants are tasked to respond to a challenge e.g. exploit a web application, analyse a malware sample, and decipher a given ciphertext. In the red/blue team exercises, the attacking team(s) - red team(s) - challenge the cyber security preparedness and response capabilities of the defending team(s) - blue team(s).

Limited resources also prevent LEAs from contributing data to Europol’s MISP. Lack of resources is identified as another reason for not very close collaboration and the “extra miles” between CSIRTs and LEAs. Some LEAs are seriously understaffed.

Maintenance of resources is also a major challenge.

From an organisational point of view, some LEAs are centralised, others are de-centralised making building a single model that fits all is very difficult.

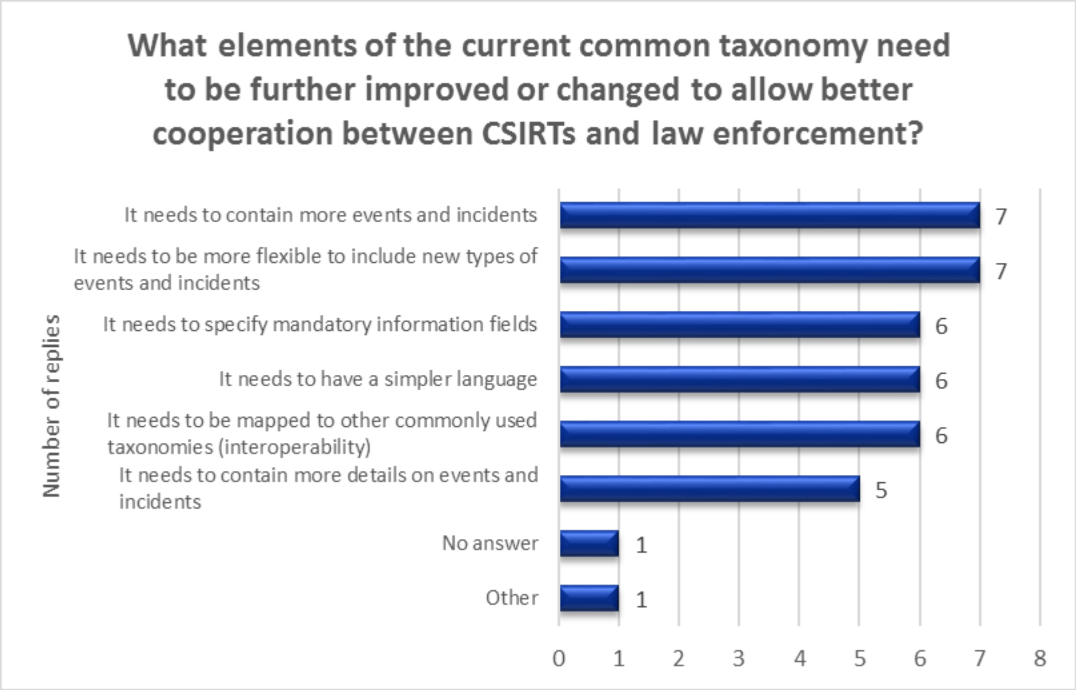
4.3.2.6 Need for Improving and Aligning Taxonomies

According to data collected, the majority of CSIRTs use a reference taxonomy but it is not always adopted for exchanging information with LEAs, an aspect that is also impacting the level of automation of the information sharing between the two communities. One practical solution could be the use of a common taxonomy or, if this is not possible, improve used taxonomies on both sides in order to facilitate an automatic translation between the two.

As usually CSIRTs have the capacity to automatically process structured but also unstructured data (data feeds, reports) received from various sources, they could also export the data in aggregated reports that can be passed to LEAs, based on an agreed taxonomy.

According to the data collected via the online survey, some elements of the version available in August 2017 of the common taxonomy for CSIRTs and LEAs (Europol - European Cybercrime Centre) could be further improved. An overview of the elements that could be improved are showed in Figure 9. It must be noted that the common taxonomy for CSIRTs and LEAs is expected to be revised and updated annually and a new version is expected to be released at beginning of 2018; therefore these elements might have been already further improved in the version available at the time of the publication of this report or after.

Figure 9 – Overview of Elements of the Current (“Current” Refers to the Version Available in August 2017) Common Taxonomy to Be Further Improved, According to the Data from the Online Survey



4.3.2.7 The Use of Honeypots

Due to legal constraints LEAs are not always able to set up honeypots or sinkholes if they are not part of an ongoing investigation and often they do not have the appropriate equipment or resources to deploy a honeypot or sinkhole and process the large data sets. This is where CSIRTs can be of help with LEAs by providing the necessary technical expertise and by disseminating the information to their constituencies to help out victims.

5 Conclusions and Recommendations

The report identifies some emerging trends, tools and methodologies of CSIRTs and LEAs cooperation, as well as challenges.

In this report, after some initial background information and a description of the methodology, we first provided an overview of the cooperation framework. Then, based on the data collected via the desk research, the interviews, and the online survey, we focused on the trends, tools and methodologies. We also identified some challenges.

Below, after our conclusions, we present some recommendations on technical aspects of the cooperation.

5.1 Conclusions

5.1.1 Trust and Increased Cooperation

Trust appears to be a key issue for both CSIRTs and LEAs when it comes to information exchange.

Trust is a process, not a state, meaning that trust is an ongoing effort that should be always sought and strengthened. Confidence-building measures, collaboration and building of mutual interests between the two communities are key elements of trust. For a good cooperation, trust should be at all levels, from the political to the technical.

From the data collected via the interviews, it is clear that different approaches and levels of cooperation between CSIRTs and LEAs exist. There are different needs and objectives in the collection and dissemination of information between CSIRTs and LEAs. Although CSIRTs representatives and law enforcement agents involved in cybercrime investigation might share a similar background (e.g. they might have a background in IT), there might be differences in cultural aspects of these two communities and this might play a role in the way they cooperate.

Evidence collected suggests that cooperation for the purposes of the information exchange mostly happens in an *ad-hoc* manner and not systematically. Recent national and international incidents (e.g. WannaCry and 'NotPetya') have seen an increase of cooperation and also demonstrate a need for increased collaboration for the purposed of the information exchange.

Secure communication platforms are used by both CSIRTs and LEAs, however as with other issues it is apparent that they use different methods.

Also the frequency of meetings in person and even the physical proximity of offices (e.g. CSIRTs and LEAs offices located in the same building) might help to enhance the cooperation between CSIRTs and LEAs.

An interesting topic for future research could be to see how the focus might move from trust to accountability should cooperation take place between CSIRTs and LEAs from completely different countries, cultures, etc.

5.1.2 Data Processing

Findings from the interviews indicate that CSIRTs produce and use larger sources of information whereas LEAs avoid being overwhelmed with too much data. It is also apparent that there is a difference in how CSIRTs and LEAs collect information: CSIRTs will often process large sets of data and then distribute the relevant information to their constituency, whereas LEAs require very specific information.

A general point regarding information exchange is that organisations have a lack of resources and are concerned to be overwhelmed with information streams and to have difficulties to find the information that is relevant to them.

Processing of big data, automation, deployment of basic filtering to support the data analysis, as well as artificial intelligence for detection and prevention, are all fields that might need to be further explored. An enhanced knowledge of such fields indeed could bring new ideas to consider when discussing present and future cooperation between CSIRTs and LEAs.

5.1.3 Common Taxonomy for CSIRTs and LEAs

A common taxonomy for CSIRTs and LEAs is of help for their cooperation. A common taxonomy for CSIRTs and LEAs (Europol - European Cybercrime Centre) exists and has been developed based on the CERT.PT taxonomy, also in the light of the ENISA report on *Information sharing and common taxonomies between CSIRTs and Law Enforcement* (ENISA, 2015a).

This common taxonomy is expected to be reviewed and updated, if needed, annually.

A joint effort is needed towards a broader adoption and use of this taxonomy.

5.1.4 Open Source In-House Software Tools Versus Commercial Software Tools

A further finding from the interviews is that when it comes to the adoption of tools in general CSIRTs are more inclined to use open source software tools. LEAs seems to look more towards commercial software tools for solutions due to the various possible reasons explained in 4.2.1.3 - Common Tools and in 4.2.1.4 - Encryption.

5.1.5 Different Roles but Strong Synergies

Overall it is clear that CSIRTs and LEAs have different roles and operate in different ways but is also evident that there are strong synergies between both organisations.

5.1.6 Uniqueness of CSIRTs' Role in Mitigating Incidents and in Supporting Cybercrime Investigations

CSIRTs have greater variety of resources that could be used to support LEAs investigating particular types of cybercrime.

5.1.7 Importance of Training and Skills Development

Training, including publicly available online training resources, supports the development of skills within the CSIRTs community - see for instance material available on ENISA's website in the online Training Resources section (ENISA, n.d. c) - and law enforcement community. An example of this is Computer Incident Response Center Luxembourg (CIRCL) which organises MISP training. However, such training is generally targeting either the CSIRTs or the LEAs, more rarely both. Most of the times, indeed, CSIRT and LEA teams do not perform common trainings, thus they do not have the chance to form a common ground and use the same tools and methods.

5.2 Recommendations

Some recommendations are proposed and for each certain categories of stakeholders.

It must be noted that the recommendations below have been developed based on the data and results of this report as well as of the parallel ENISA report on *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (ENISA, 2017).

5.2.1 Build and Maintain a Centralised Repository of Tools, Methodologies, Forms and Procedures, Used for the Cooperation between CSIRTs and LEAs

A centralised repository of tools, methodologies, possibly standardised forms and procedures, used in the EU for the cooperation between CSIRTs and LEAs could help the overall enhancement of the cooperation. The centralised repository of tools and methodologies should be a community effort, not an effort of one or a few organisations only. It could be developed e.g. in the context of CEF (European Commission, n.d. a) and hosted e.g. in a CEF platform - similarly to MeliCERTes facility, which "aims to facilitate swift and effective operational cooperation" for the CSIRTs Network (European Commission, 2017) - or on a community supported platform (e.g. Github).

Recommendation for:

- **ENISA and Europol's EC3:** to collect from the CSIRTs and LEAs the requirements for a centralised repository of tools, methodologies, standardised forms and standardised procedures
- **CSIRTs and LEAs:** to provide the requirements for a centralised repository of tools, methodologies, standardised forms and standardised procedures
- **ENISA and Europol's EC3**: to organise a process to collect in a centralised repository tools, methodologies, standardised forms and standardised procedures, used for the cooperation between CSIRTs and LEAs and to keep the centralised repository updated
- **CSIRTs and LEAs:** to actively participate and share information about tools, methodologies, standardised forms and standardised procedures for more effective cooperation between CSIRTs and LEAs
- **ENISA and Europol's EC3**: to streamline the methodologies used for the cooperation between CSIRTs and LEAs between the Member States
- **ENISA and Europol's EC3**: to facilitate a discussion about defining the strategic tools and their capabilities that should be the standard and baseline ones for cooperation between CSIRTs and LEAs
- **Member States, ENISA and Europol's EC3**: not to build new tools or platforms until there is a sufficient level of common trust reached

5.2.2 Build and Maintain a Centralised Repository of Existing Practices of Cooperation Between CSIRTs and LEAs

Led by both CSIRTs and LEAs, a centralised repository could be beneficial to both communities, as a platform, e.g. developed in the context of CEF (European Commission, n.d. a) - similarly to MeliCERTes facility (European Commission, 2017) - to support various aspects of collaborative working.

Recommendation for:

- **CSIRTs and LEAs**: to actively provide data for the centralised repository, participate and share information, good practices and procedures for more effective cooperation between CSIRTs and LEAs
- **ENISA and Europol's EC3**: to faceplate the setting up of, or possibly build and maintain, a centralised repository of existing practices of cooperation between CSIRTs and LEAs
- **ENISA and Europol's EC3**: to set up mechanisms to validate the information in the central repository
- **ENISA and Europol's EC3**: to define the different levels/tiers of cooperation between CSIRTs and LEAs and the respective cooperation requirements

5.2.3 Maintain an Updated List of LEAs Point of Contacts (PoCs) in Which Whenever Possible Liaison Officers are Indicated as PoCs and Create an Emergency Protocol for Cooperation

LEAs could create and maintain a list of PoCs, possibly with dedicated email address for the communication with CSIRTs (in particular national/governmental), so that CSIRT - and in particular national/governmental CSIRT - can communicate with LEA without relying on individual contacts. In this list, whenever possible liaison officers should be indicated as the PoCs. Also to have an emergency protocol for cooperation to follow especially in case of crisis will be of help.

Recommendation for:

- **LEAs**: to create and maintain a list of PoCs for the communication with the CSIRTs
- **CSIRTs and LEAs**: to create and follow an emergency protocol when the situation where the cooperation takes place requires so

5.2.4 Keep Up-To-Date and Further Enhance If Needed the Common Taxonomy for CSIRTs and LEAs, Promote, Adopt It and Use It

There is a common taxonomy for CSIRTs and LEAs (Europol - European Cybercrime Centre).

Europol and ENISA, together with key stakeholders - CSIRTs and LEAs -, are working together to further enhancing, if needed, and keep-up-to-date this taxonomy. The common taxonomy for CSIRTs and LEAs is expected to be reviewed and updated annually.

This common taxonomy, which has been identified as the most suitable for the cooperation between CSIRTs and LE, should be futher promoted.

It is recommended to be promptly adopted and used both by the CSIRT and LEA communities. This taxonomy should be aligned and maintained within the existing legal framework.

This common taxonomy has been already implemented and imported in MISP (GitHub, n.d. a).

Recommendation for:

- **CSIRTs and LEAs**: to describe how current common taxonomy should be extended/amended
- **CSIRTs and LEAs**: to participate and provide requirements and use cases so that a common taxonomy can be adopted
- **CSIRTs and LEAs**: to adopt and use the common taxonomy
- **ENISA and Europol's EC3**: to jointly work to improve, if needed, the current common taxonomy and keep it up-to-date, and promote - ENISA should act as facilitator for the CSIRT community, while Europol's EC3 for the LEA community
- **ENISA, Europol's EC3, European Commission, Member States**: to consider setting up a group of legal experts to provide assistance to align the common taxonomy to the legal framework and to maintain such alignment

5.2.5 Take Advantage of MISP Capabilities

MISP is already used in other trusted environments, including the military sector (MISP, 2017) (NATO, 2013). Usage of MISP would be beneficial also for the CSIRT and LE cooperation. Some steps could be taken for adopting MISP:

- Use external MISP - prove value
- Build internal MISP - prove value and build processes
- Connect internal MISP to relevant external MISP communities
- Adoption of MISP for collaboration/co-ordination between CSIRTs and LEAs. There is already functionality in MISP that help collaboration and specific sharing groups should be created.
- Implementation of taxonomies in MISP. MISP provides the capability of easily building your custom taxonomy but also used the well know and already provided ones (e.g. TLP. NATO, Europol, etc..). Taxonomy should also support exchange of information related to interference avoidance (e.g. specific fields for sinkholes or monitored resources).

It is worth noting that CIRCL - Computer Incident Response Center Luxembourg organises MISP trainings. Some training material develop in the context of this training is also made available online (CIRCL - Computer Incident Response Center Luxembourg, n.d.).

Recommendation for:

- **CSIRTs and LEAs, possibly with the support of ENISA and Europol's EC3**: to work together towards the adoption of MISP
- **Europol**: to advocate the use of external MISP within LEAs
- **CSIRTs and LEAs**: to support developers of MISP to build start kits for deployment of internal MISPs
- **CSIRTs:** provide MISP trainings explaining practical information sharing in incident response and investigations in LE-CSIRT coordination cases
- **ENISA:** develop collaboration documents and information sharing policy documents to be used by MISP participants and possibly redact the outcome of MISP training and publish them
- **ENISA and Europol's EC3**: to advocate the use of existing taxonomies that can be used in MISP

5.2.6 Identify Use Cases for Threat Intelligence Platform (TIP) and Real-Time Information Sharing

TIP can provide the technology enablement needed for real-time information sharing between CSIRTs and LEAs. There are use cases where usage of a shared TIP would bring value to both CSIRTs and LEAs, e.g. sharing the sinkhole domains as well as the domains/IPs/servers of current investigations so that interference could be avoided.

Recommendation for:

- **CSIRTs and LEAs:** to identify use cases where usage of a shared TIP and real-time information sharing would bring value to both CSIRTs and LEAs and would improve their cooperation.

6 Bibliography/References

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

Bitcoin. (n.d.). Retrieved July 07, 2017, from https://bitcoin.org/en/

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

Blockchain Technologies. (n.d.). *Blockchain Technology Glossary*. Retrieved from http://www.blockchaintechnologies.com: http://www.blockchaintechnologies.com/blockchain-glossary#b

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 Evidence and Computer Crime.*

CERT-EU. (n.d.). *About Us*. Retrieved July 28, 2017, from https://cert.europa.eu/cert/plainedition/en/cert_about.html

CIRCL - Computer Incident Response Center Luxembourg. (n.d.). *MISP - Malware Information Sharing Platform & Threat Sharing - Training Materials*. Retrieved October 10, 2017, from https://www.circl.lu/services/misp-training-materials/#introduction

Collins. (n.d.). *Collins Dictionary*. Retrieved July 28, 2017, from https://www.collinsdictionary.com/dictionary/english/trend

Council of Europe. (2001, November 2001). *Convention on Cybercrime* . Retrieved July 28, 2017, from http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Council of Europe. (n.d.). *Budapest Convention and related standards*. Retrieved 28 July, from http://www.coe.int/en/web/cybercrime/the-budapest-convention

Council of 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. (2017, 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

Council of the European Union. (2017a, May 31). *Note from the General Secretariat of the Council to the Council, Cybersecurity - Information from the Commission, 9621/17.* Retrieved October 8, 2017, from http://data.consilium.europa.eu/doc/document/ST-9621-2017-INIT/en/pdf

Council of the European Union. (2017b, March 13). *Joint paper Eurojust/Europol sent to Delegations on Common challenges in combating cybercrime.* Retrieved September 5, 2017, from http://data.consilium.europa.eu/doc/document/ST-7021-2017-INIT/en/pdf

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

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. (2012). *Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime.* Retrieved July 28, 2017, from https://www.enisa.europa.eu/publications/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime

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). *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. (2015d). *CSIRT Capabilities.* Retrieved July 28, 2017, from https://www.enisa.europa.eu/publications/csirt-capabilities

ENISA. (2015e). *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/cybersecurity-information-sharing

ENISA. (2016c, 12). *ENISA's Opinion Paper on Encryption.* Retrieved August 9, 2017, from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption

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

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

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

ENISA. (n.d.). *Considerations on the Traffic Light Protocol* . Retrieved August 3, 2017, from https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol

ENISA. (n.d. a). *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. b). *ENISA Threat Landscape*. Retrieved August 3, 2017, from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

ENISA. (n.d. c). *Training Resources*. Retrieved August 30, 2017, from https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material

ENISA. (to be published). *Exploring the limitations of current TIPs (tentative title - report currently under finalisation).*

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/HTML/?uri=LEGISSUM:si0016&from=EN.

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

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

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

European Commission. (n.d. b). *EU Survey*. Retrieved July 4, 2017, from https://ec.europa.eu/eusurvey/home/welcome

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

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 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. (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. (2013a, August 12). *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.* Retrieved July 29, 2017, from http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040

European Parliament and Council of the European Union. (2013b, May 21). *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.* Retrieved July 29, 2017, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

European Parliament and Council of the European Union. (2014, April 3). *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal* *matters.* Retrieved August 3, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041

European Parliament and Council of the European Union. (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, and repealing Directive 95/46/EC (General Da.* 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 August 3, 2017, from http://eur-lex.europa.eu/eli/dir/2016/681/oj

European Parliament and Council of the European Union. (2016d, 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 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. (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

Europol. (2017b). *Internet Organised Crime Threat Assessment (IOCTA) 2017*. Retrieved October 23, 2017, from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

Europol and ENISA. (2016, May 20). *On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA joint statement.* Retrieved August 9, 2017, from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

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

Europol. (n.d. b). *SPACE.* Retrieved November 1, 2017, from https://www.europol.europa.eu/sites/default/files/documents/ec3_space_leaflet.pdf

FIRST. (n.d.). *Traffic Light Protocol*. Retrieved August 3, 2017, from https://www.first.org/tlp/

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

GitHub. (n.d. a). *MISP/misp-taxonomies*. Retrieved October 10, 2017, from https://github.com/MISP/misp-taxonomies/blob/master/europol-incident/machinetag.json

GitHub. (n.d. b). *MISP/misp-warninglists*. Retrieved October 9, 2017, from https://github.com/MISP/misp-warninglists

GNU Privacy Guard. (n.d.). Retrieved August 30, 2017, from GnuPG: https://gnupg.org/

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

IETF. (2007). *Request for Comments: 4880 - OpenPGP Message Format.* Retrieved July 07, 2017, from https://tools.ietf.org/html/rfc4880

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

KVM. (n.d.). Retrieved September 24, 2017, from Kernel Virtual Machine: https://www.linux-kvm.org/page/Main_Page

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

MISP. (2017, October 10). *MISP Communities.* Retrieved from http://www.misp-project.org/communities/

MISP Community. (n.d.). *MISP - User Guide - A Threat Sharing Platform.* Retrieved October 9, 2017, from https://www.circl.lu/doc/misp/book.pdf

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

National Cyber Security Centre, Ministry of Security and Justice, The Netherlands. (2013). *Policy for arriving at a practice for Responsible Disclosure.* Retrieved August 30, 2017, from https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/responsible-disclosure-guideline/1/Responsible%2BDisclosure%2BGuideline.pdf

NATO. (2013, December 4). *Sharing malware information to defeat cyber attacks.* Retrieved October 10, 2017, from http://www.nato.int/cps/en/natohq/news_105485.htm?selectedLocale=en

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

NATO. (n.d.). *The NATO Codification System.* Retrieved August 3, 2017, from http://www.nato.int/structur/AC/135/ncs_guide/english/e_1-6-1.htm

No More Ransom. (n.d.). Retrieved July 28, 2017, from https://www.nomoreransom.org/en/about-the-project.html

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.*

STIX™ . (2017, July 28). Retrieved from http://stixproject.github.io/data-model/1.2/campaign/CampaignType/

Annex A: Acronyms

ACRONYM	DESCRIPTION
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
CIO	Chief Information Officer
CIRCL	Computer Incident Response Center Luxembourg
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CTF	Capture the Flag
CSS	Cyber Security Strategy
DAE	Digital Agenda for Europe
DDoS	Distributed Denial-of-Service
DG	Directorate General
DG CONNECT	(European Commission) Directorate General for Communications Networks, Content & Technology
DP	Data Protection
ECI	European Critical Infrastructures
EC3	European Cybercrime Centre
EEA	European Economic Area
EFTA	European Free Trade Association
EMPACT	European Multidisciplinary Platform against Criminal Threats
ENI	European Neighbourhood Instrument
ENISA	European Union Agency for Network and Information Security
EU	European Union
EUCTF	European Union Cybercrime Task Force
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation
GPG or GnuPG	GNU Privacy Guard
IAEA	International Atomic Energy Agency
ICS	Industrial Control Systems
IcSP	Instrument contributing to Stability and Peace
ICT	Information and Communication Technologies
IOCTA	Internet Organised Crime Threat Assessment
IP	Internet Protocol
IPA	Instrument of Pre-accession
ISF	Internal Security Fund
ISP	Internet Service Provider
IT	Information Technology
KVM	Kernel-based Virtual Machine
LE	Law Enforcement
LEA	Law Enforcement Agency
MISP	Malware Information Sharing Platform
MS	Member State
NCI Agency	NATO Communications and Information Agency
NCSC	National Cyber Security Centre
n.d.	No date
NIS	Network and Information Security

NRA	National Regulatory Authority
OSINT	Open Source Intelligence
PNR	Passenger Name Record
RAT	Remote Access Tool
PGP	Pretty Good Privacy
RFC	Request for Comments
SIG	Special Interest Group
SO	Strategic Objective
SOC	Security Operations Centre
SSH	Secure Shell
STIX™	Structured Threat Information eXpression ™
TIP	Threat Intelligence Platform
TF	Task Force
TLP	Traffic Light Protocol
TLS	Transport Layer Security

Annex B: Samples of Questionnaires to Support the Interviews

B.1 Sample Questionnaire to Collect Data from CSIRTs and LEAs for this Report

Questions prepared to support the interviews with CSIRTs and LEAs to collect data for the ENISA guidelines on emerging trends, tools and methodologies to support LEA and CSIRT cooperation in the fight against cybercrime

These guidelines are 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)

These guidelines address technical aspects of the cooperation between CSIRT and LEA. ENISA is carrying out a parallel project aiming at the drafting of a report on further improvement of communication between CSIRT and LEAs (law enforcement agencies). The parallel project addresses legal and organisational aspects of cooperation between CSIRT and LEA in the fight against cybercrime.

Interviewer:
Interviewee name:
Interviewee affiliation:
Interviewee position:
Date of the interview:

QUESTIONS ON TOOLS AND METHODOLOGIES

1. Tools used and main technical challenges in the CSIRT-LEA cooperation to fight cybercrime

- What tools are used for the CSIRT-LEA cooperation to fight cybercrime?
- Which functions or capabilities are outsourced and which are developed in house?
- Which tools are based on open source solution, which on commercial solutions?
- What are the main technical challenges you face in the CSIRT-LEA cooperation?

2. Use of taxonomies

- Have you implemented a taxonomy?
- What were the criteria for choosing that taxonomy?
- Did you implement the CERT.pt taxonomy?

○ If you did, is the CERT.pt taxonomy sufficient for your needs or are there specific domains that should be extended?

- Did you implement another taxonomy?
- Do you use any taxonomy that is implemented in MISP? *(Some more questions on MISP will follow)*
- Have you worked on mapping the synonyms among taxonomies (i.e. on ontology) to ease classification of incidents?
- Do you apply any mechanism of automatic classification of incident?
- Do you produce and report statistics using the aforementioned taxonomy?

3. Use of platforms

- Do you see a need for a coordination between CSIRTs and LEAs in terms of actions and timing for dealing with cybercrime cases? If so, do you think a technical platform would be useful?
- What would be your criteria for using such a technical platform? Would this be based on incident types (if so, would a taxonomy like the CERT.pt be useful) or based on the type of victim?

4. Reporting on trends

- What type of reporting on trends are useful to exchange between CSIRTs to LEAs?

○ Would this reporting be very different from the statistics already (if so) published by your national CSIRT?

○ What timing of the reporting do you think is most beneficial (6 month, bi-weekly, ...)

5. Joint capture the flag or red-team/blue-team exercises

- Would joint capture the flag or red-team/blue-team exercises be beneficial for tool testing/practices?

6. Interference avoidance

- How do you avoid situations in which a CSIRT actions (evidence collection and manipulation, mitigation measures, requests sent to their parties like ISPs) interfere with a LEA investigation?

7. Social engineering against CSIRT/LE?

- What defense mechanisms are in place to prevent social engineering attacks happening towards LEA/CSIRTs?

8. Responsible disclosure

- What would be the input from LEAs and CSIRTs for helping with responsible disclosure?

9. Possible services that CSIRT could offer to LEA

- What are the most benefic services that a CSIRT could offer to LEA (e.g. technical support for evidence acquisition and analysis and vice versa (e.g. support mitigation actions like takedowns)?

QUESTIONS ON INTELLIGENCE SHARING

10. Threat intelligence sharing platform

- Do you think that a threat intelligence and sharing platform would improve the sharing of information between CSIRTs and LEAs?
- Would it help sharing tactical and/or operational and/or strategic intelligence?
- Do you run MISP internally?
- Are you participating in an external MISP?
- What would be the major concern if both LEA and non-LEA organisations are members of a MISP group?
- Are you using any other threat intelligence-sharing platform? Is it a commercial or an in house developed platform?

○ Is the volumes of data/information manageable?

○ Do you actively contribute data/information in the platform?

○ What type of information/intelligence do you or would you be able to share/feed in the platform?

○ Do you consume data from the platform?

○ What type of information/intelligence do you or would you be able to consume?

- What is the level of your engagement with the threat intelligence-sharing platform?

11. What are the main uses and challenges of using this platform?

12. Information classification

- Which classification do you use when it concerns information classification (e.g. “secret”, “confidential” or “restricted”)?
- Have you encountered problems when sharing information between CSIRT – LEAs and how did you overcome these problems?
- If not, do you foresee any problems?
- Have you encountered any technical problems when cooperation between CSIRT and LEA?
- Do you use NATO classification system?
- Do you use NATO admiralty system?

13. Traffic Light Protocol (TLP)

- Do you use the Traffic Light Protocol when exchanging information between CSIRTs and LEA (and vice-versa)?

14. Encryption of information

- What is the preferred way of encrypting information when exchanging documents (not the transport protocol but encrypting the document itself)?
- Which way of encryption do you use for the exchange of information CSIRT-law enforcement?
- Do you use secured email for the exchange of information CSIRT-law enforcement? If so, which standard (PGP, smime, other product open) do you use? And which implementation?
- Do you use mobile devices for exchanging information? If yes, do you use specific apps (e.g. Signal, etc.)?

15. Sensors, honeypots and sinkholes

- Do you use honeypot data from other sources e.g. Shadowserver, SISSDEN, etc.
- What types of sensor data would you be interested in (e.g. DDoS, IoT?)
- Is there joint work-in-progress between CSIRTs and LEAs to setup passive network sensors (with rules from a threat intelligence platform) or honeypots?
- What type of tooling and processes are lacking for CSIRTs and LEAs to setup a sinkhole?

QUESTIONS ON TRENDS

16. Which are the trends in the CSIRT-LE collaboration? Are you aware of changes that have recently occurred or changes that may occur in the collaboration between CSIRT and LEA?

17. Are you aware of the reasons for these changes (e.g. a rise of the terror levels in different countries)

18. Monitoring Darknet and social media

- Do you make use of monitoring tools for keeping an eye what is going on the Darknet or social media?
- Is there an exchange (either formal or informal) process between CSIRTs and LEAs?
- Do you make use of the AIL-Framework?
- Do you use open source tools for monitoring these sources? Are these in-house developed tools or commercial tools?
- What are the pros and cons of the tools that you use for monitoring these sources?
- What tools do you use to correlate/analyse the vast amount of data you collect from the aforementioned tools?
- What tools do you use to visualise the aforementioned data?

19. Wannacry

Which things went well and which could have gone better in the CSIRT-LEA cooperation?

- Without going into details, how would we be able to prevent a thing like the take down of a sinkhole server?
- Did the Wannacry decryption solutions came from infosec individuals or was it a LEA coordinated effort?

QUESTIONS ON LEGAL AND ORGANISATIONAL/POLICY CHALLENGES

20. Legal challenges

- What main legal challenges do you see that affects the information sharing and cooperation between CSIRTs and LEAs?

21. Organisational/policy challenges

- What main organizational/policy (internal procedures) challenges do you see that affects the information sharing and cooperation between CSIRTs and LEAs?

B.2 Sample Questionnaire to Collect Data from CSIRTs for this Report and for the Report on Further Improvement of Communication between CSIRTs and LEAs

Questions prepared to support the interviews with CSIRTs to collect data for both following ENISA's projects:

1) **Report on further improvement of communication between CSIRTs and LEAs, which focuses on legal and organizational aspects**
2) **Guidelines on emerging trends, tools and methodologies to support LEA and CSIRT cooperation in the fight against cybercrime, which focuses on technical aspects of their cooperation.**

Both these Report and Guidelines are 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)

Interviewer(s):

Interviewee(s):

Date of the interview:

Expected duration of the interview: 1,5 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?

7.

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?

8.

a. Which kind of cooperation does your organisation have with the LE (tick relevant the boxes)

- □ *reply to LE requests in the context of criminal investigations*
- □ *witnesses in court*
- □ *forensic experts*
- □ *sharing reporting on trends*
- □ *joint training/common trainings, including joint capture the flag or red-team/blue-team exercises*

- □ *regular meetings*
- □ *any other type of bilateral trust-building events*
- □ *other (Please specify)*

b. Exchange reporting on trends,

i. What type of reporting on trends are useful to exchange between CSIRTs to LEAs?

ii. Would this reporting be very different from the statistics already (if so) published by you/your national CSIRT (if you are not the national CERT)?

iii. What timing of the reporting do you think is most beneficial

- □ *every year*
- □ *every 6 months*
- □ *every month*
- □ *every two weeks*
- □ *every week*
- □ *other (please specify)*

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

a. Do you exchange vulnerability information?

b. Do you exchange incident information from CERT to LE based on predefined parameters (for example incidents towards specific network) or incident categories (ref. taxonomy)?

c. If you exchange information, is it a manual process or an automatic process

d. If you exchange incident information, to what level is the information anonimized?

10. How do you avoid interferences, i.e. situations in which a CSIRT actions (evidence collection and manipulation, mitigation measures, requests sent to their parties like ISPs) interfere with a LEA investigation?

11.

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?

12.

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

[Yes/No]

b. If yes,

i. Does your organisation have a formalized way (e.g. clear steps to take, deadlines, tec.) of *receiving* requests from the LE?

[Yes/No]

Does your organisation have a formalized way of accepting/rejecting requests from the LE?

[Yes/No]

Does your organisation have a formalized way of processing of and replying to requests from the LE?

[Yes/No]

13. What type of communication channels has your organisation established with the LE of your country or of other countries? (Please tick relevant boxes)

- □ *face-to-face meetings*
- □ *secured email*
- □ *online platform*
- □ *other (please specify)*

14.

a. Do you think that a threat intelligence and sharing platform would improve the sharing of information between CSIRTs and LEAs?

[Yes/No]

b. Would it help sharing tactical and/or operational and/or strategic intelligence?

[Yes/No]

c. Do you run MISP internally?

[Yes/No]

d. Are you participating in an external MISP?

[Yes/No]

e. What would be the major concern if both LEA and non-LEA organizations are member of a MISP group?

f. Do you actively contribute data/information in the platforms you are part of?

[Yes/No]

g. What type of information/intelligence do you or would you be able to share/feed in the platform?

- □ *add TTPs used by adversaries*
- □ *submit data (C2s, dropped filenames …) in analyzed malware*
- □ *submit data (C2s, dropped filenames …) in malware analyzed by others*
- □ *information (email characteristics) on phishing campaigns*
- □ *sightings of IOCs that are already in the platform*
- □ *vulnerability information that is not yet published by vendor*
- □ *publications or documents by industry experts on attack campaigns*

h. Do you consume data from the platform?

[Yes/No]

i. What are the main challenges to use a platform together with LE?

- □ *technical*
- □ *legal*
- □ *organizational*
- □ *other (please specify)*

j. Are these challenges different compared to using the same platform with only CSIRTs? If so, what challenges are different?

- □ *technical*
- □ *legal*
- □ *organizational*
- □ *other (please specify)*

15. Which ways of encryption do you use for the exchange of information CSIRT-law enforcement?

- □ *secured email for the exchange of information CSIRT-law enforcement (PGP, smime, other product open, etc.)*
- □ *encrypting the document itself (for example encrypting a document and then attaching it to an unencrypted email, using password protected Office documents)*
- □ *mobile devices with specific applications (e.g. Signal, etc.)?*
- □ *other (specify)*

16. Which classification do you use when it concerns information classification (e.g. “secret”, “confidential” or “restricted”)?

17. Do you use the Traffic Light Protocol when exchanging information between CSIRTs and LEA (and vice-versa)?

[Yes/No]

18. 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]

19.

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?

20. Use of taxonomies

a. Have you implemented a taxonomy?

[Yes/No]

b. If yes, which taxonomy did you implement?

c. What were the criteria for choosing that taxonomy?

d. Is the taxonomy that you implemented sufficient for your needs or are there specific domains that should be extended?

[Yes/No]

e. Do you use any taxonomy that is implemented in MISP?

f. Have you worked on mapping the synonyms among taxonomies (i.e. on ontology) to ease classification of incidents?

[Yes/No]

g. Do you apply any mechanism of automatic classification of incident?

[Yes/No]

h. Do you produce and report statistics using the aforementioned taxonomy?

[Yes/No]

i. Do you use the taxonomy when exchanging information with LE (keep the classification)?

[Yes/No]

j. Do you use the taxonomy to define what information to share with LE?

[Yes/No]

21.

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]

22.

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

[Yes/No]

b. If yes, what type of challenges?

- □ *technical*
- □ *legal*
- □ *organizational*
- □ *other (please specify)*

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

23. 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]

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

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

[Yes/No]

26.

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?

[Yes/No]

d. On other grounds? Which grounds?

27.

a. Does your organisation request data from LE?

[Yes/No]

b. Are these requests generally fulfilled?

[Yes/No]

c. If not, on which grounds?

- □ *technical*
- □ *legal*
- □ *organizational*
- □ *other (please specify)*

28.

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.)?

29.

a. Which areas of law are relevant when your organisation cooperate with LE to fight cybercrime

- □ *data protection*
- □ *data retention*
- □ *criminal law and criminal procedure*
- □ *contract law and confidentiality obligations*
- □ *intellectual property rights*
- □ *legal grounds of the CSIRT*
- □ *NIS Directive*
- □ *other (please specify)*

30.

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 counseling?

[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?

31. 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]

32.

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

[Yes/No]

b. Do you have an appointed liaison officer within your organization to talk to LE?

[Yes/No]

c. Do these contact points regularly meet? If yes, how often?

[Yes/No]

33.

a. Do you have an obligation to report to the LE when you come across possible crimes? [Yes/No]

b. Can you do the reporting anonimized, leaving out the victim details? [Yes/No]

34. 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]

35.

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?

c. How do you deal with differences in the legal systems within different European countries?

36.

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]

37.

a.

i. Which are the trends in the CSIRT-LE collaboration?

ii. Are you aware of changes that have recently occurred or changes that may occur in the collaboration between CSIRT and LEA?

iii. Which could be possible reasons for these changes in CSIRT-LE cooperation (e.g. a rise of the terror levels in different countries)?

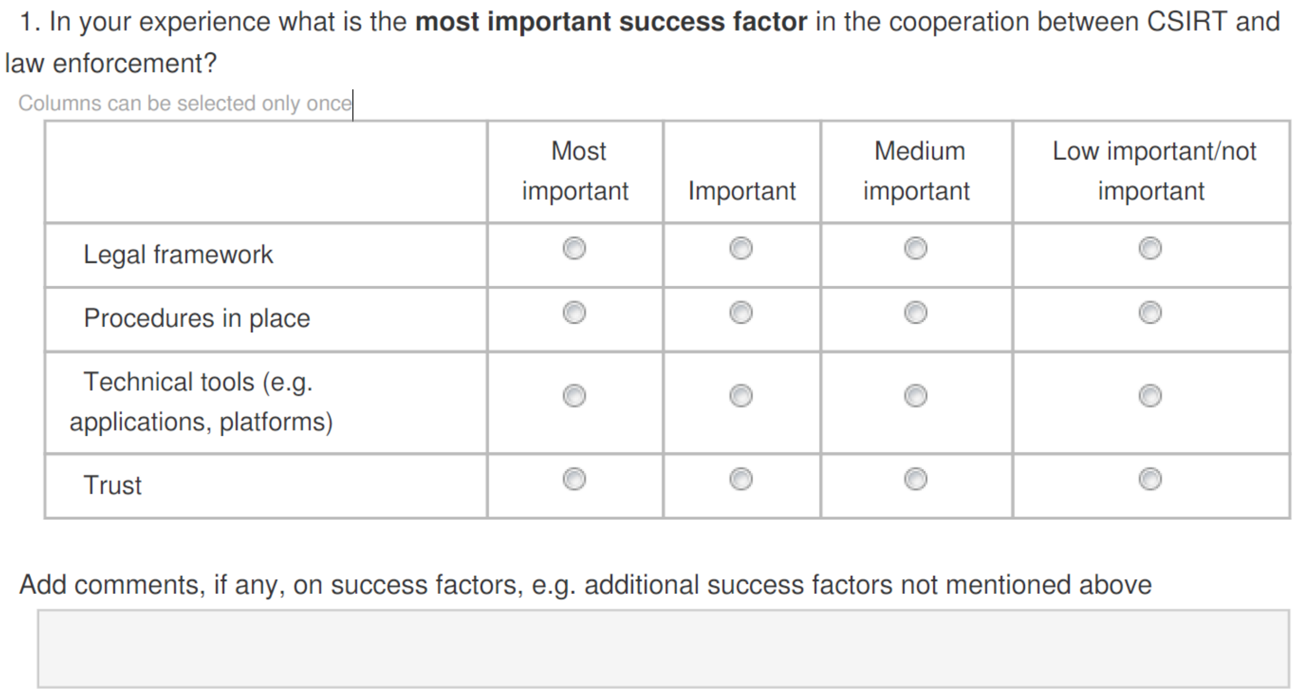
38. WannaCry ransomware attack: what went well and what could have gone better in the CSIRTs-LEA cooperation?

39.

a. Do you run your own sinkholes or honeypots?
[Yes/No]

b. Do you share information from the sinkhole or honeypot with LE?
[Yes/No]

Annex C: Questions from the Online Survey

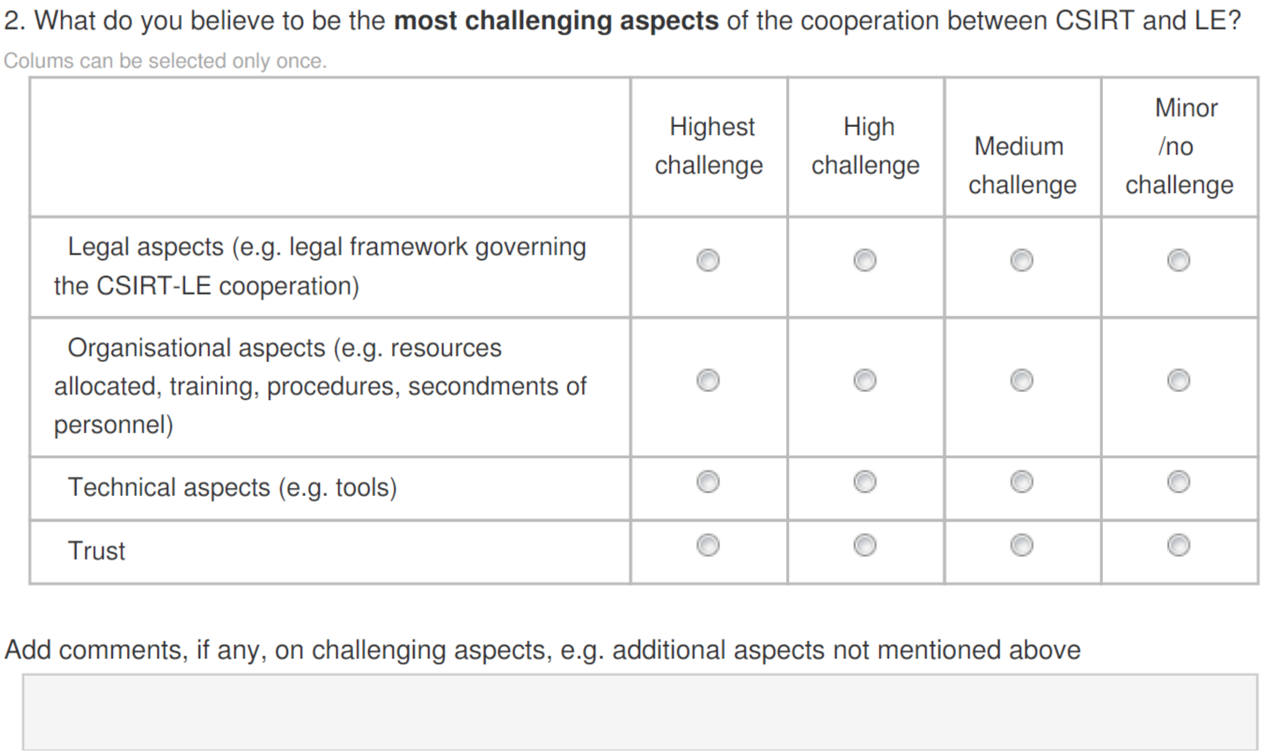


1. In your experience what is the **most important success factor** in the cooperation between CSIRT and law enforcement?

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

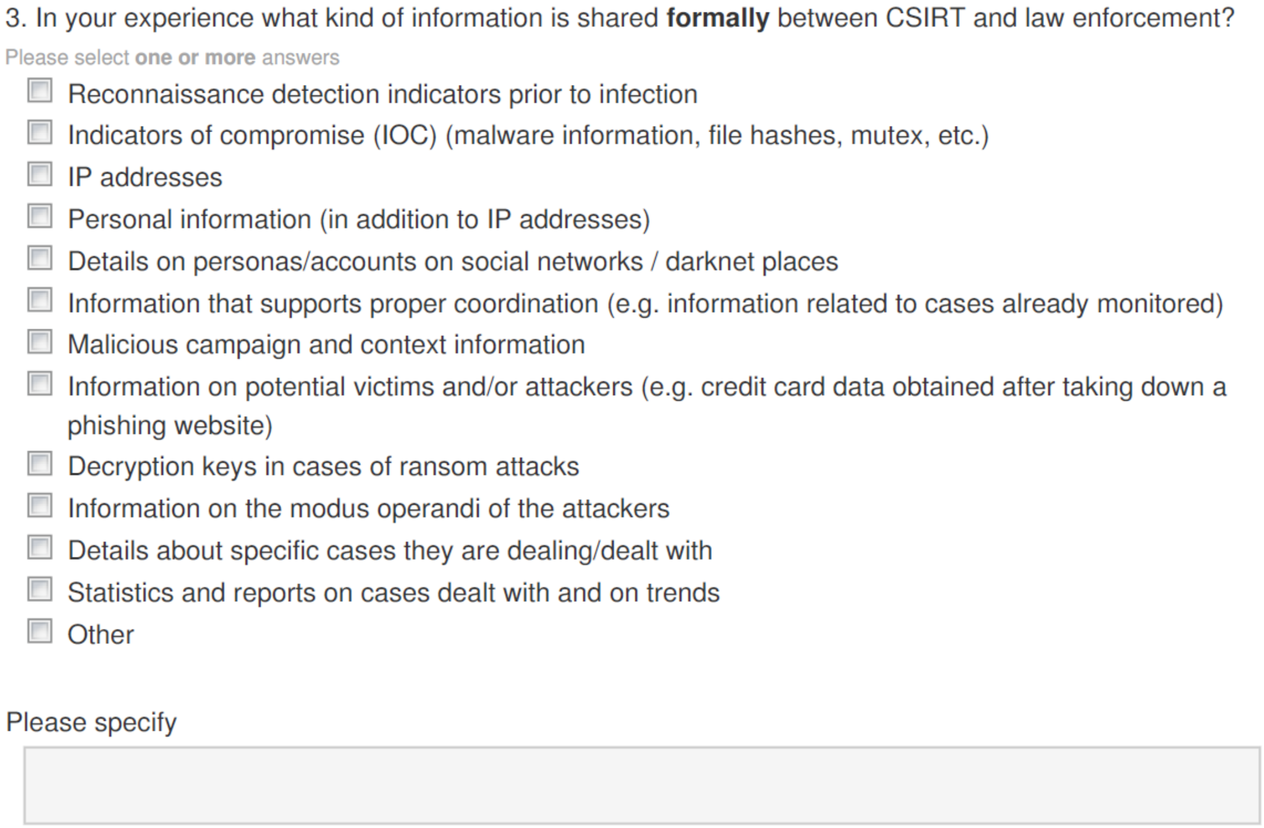


2. What do you believe to be the **most challenging aspects** of the cooperation between CSIRT and LE?

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

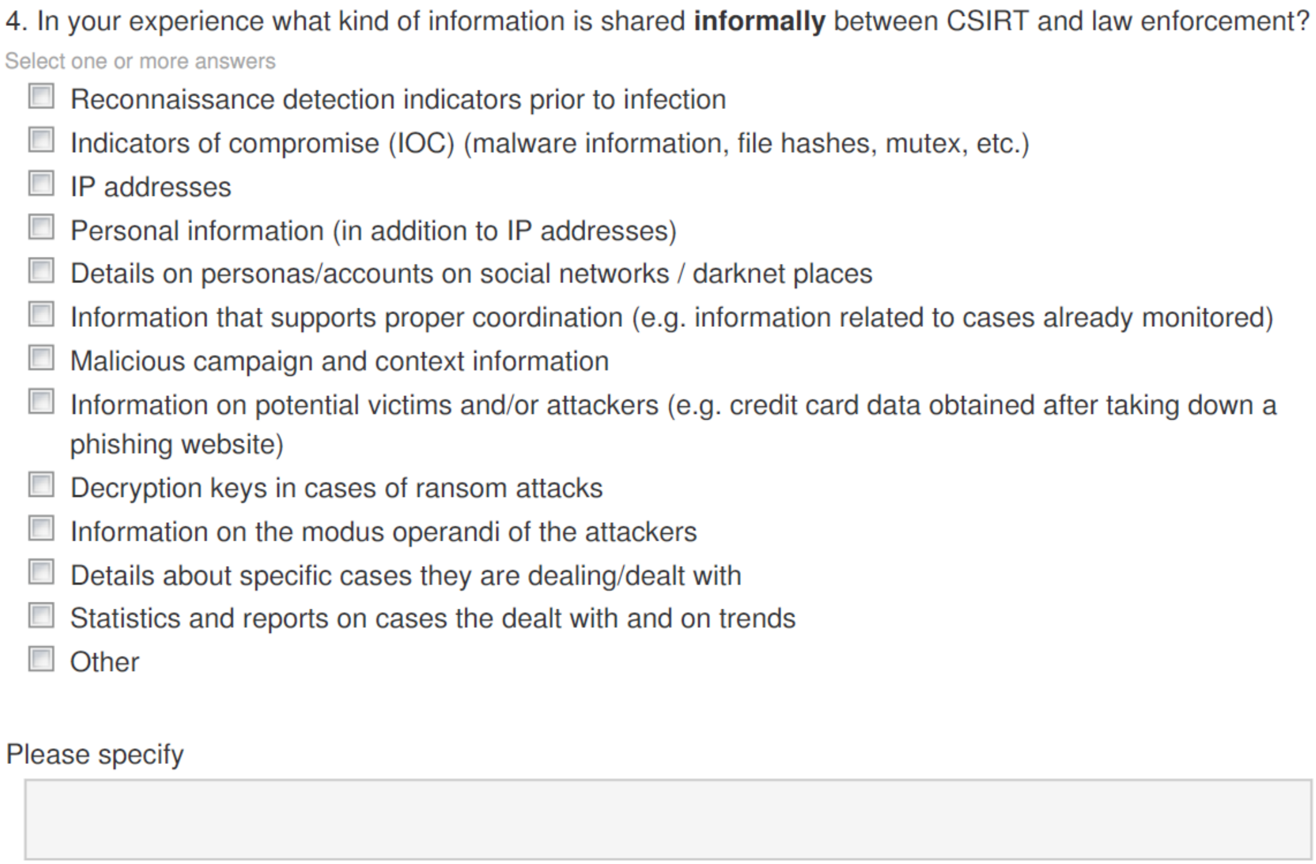


3. In your experience what kind of information is shared **formally** between CSIRT and law enforcement?

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

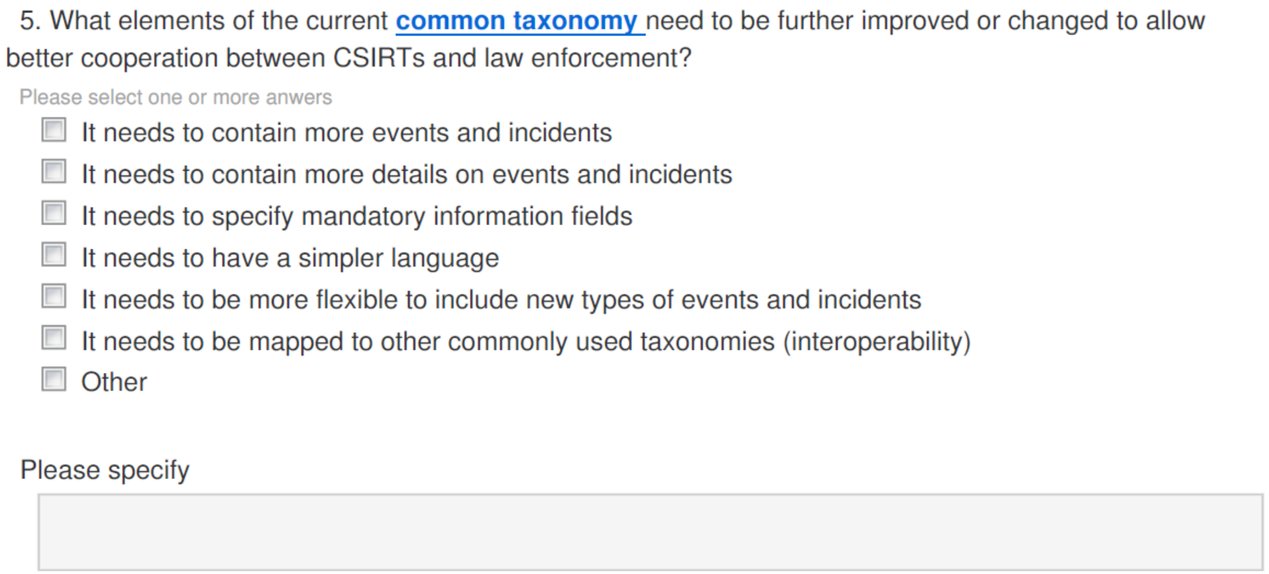


4. In your experience what kind of information is shared **informally** between CSIRT and law enforcement?

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

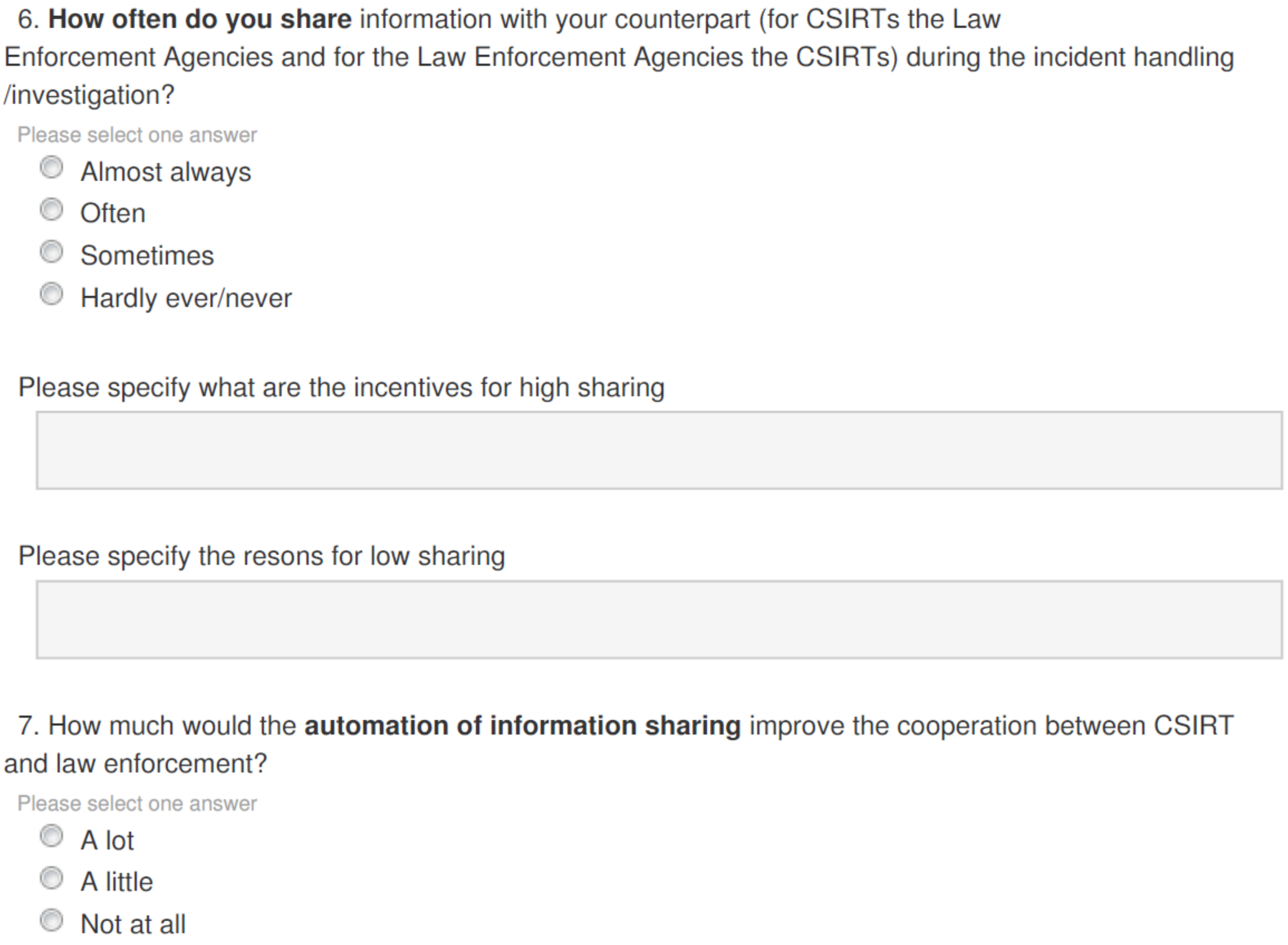


5. What elements of the current **common taxonomy** need to be further improved or changed to allow better cooperation between CSIRTs and law enforcement?

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

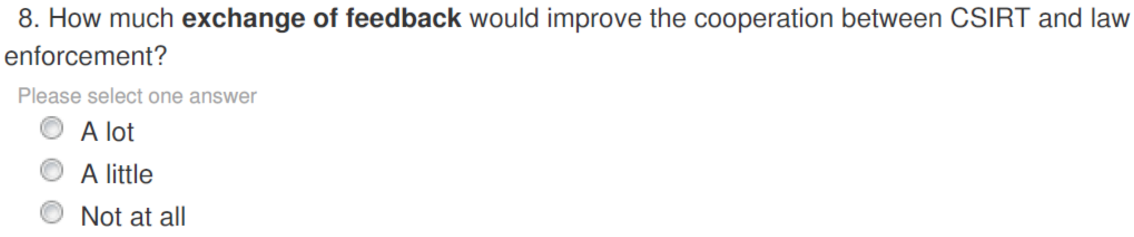
Please specify what are the incentives for high sharing

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

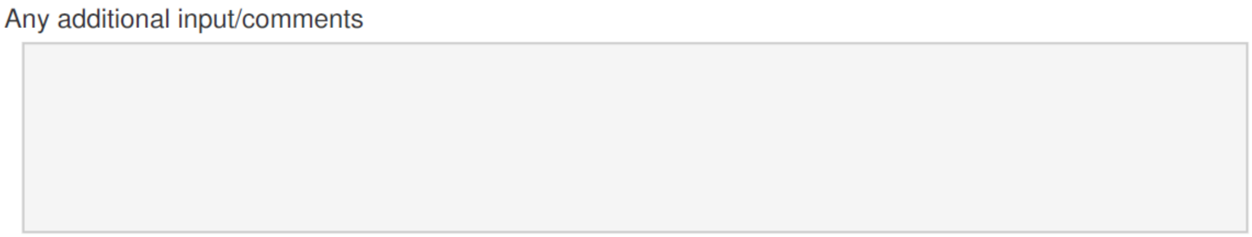
- ○ A lot
- ○ A little
- ○ Not at all



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: Examples of Sources and Material Collected During the Desk Research but Not Included in the Bibliography/References

- RFC2350
  - https://www.ietf.org/rfc/rfc2350.txt
- Europol documents that indicate the need to collaborate on dark net monitoring and public social media channels and *fora*
  - https://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe
  - https://www.europol.europa.eu/newsroom/news/darknet-dealer-of-drugs-and-arms-arrested-slovak-authorities
  - https://www.europol.europa.eu/newsroom/news/europol-coordinates-eu-wide-hit-against-online-terrorist-propaganda
  - https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2016.pdf
  - https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime
- Mandiant / FireEye Report M-Trends 2016
  - https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016-NEW.pdf
- IGF - Best Practices Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRTs) for Internet Security (2015)
  - https://www.first.org/global/governance/bpf-csirt-2015-report.pdf
- Disclosure of information to law enforcement
  - https://www.jisc.ac.uk/guides/networking-computers-and-the-law/disclosure-of-information-to-law-enforcement
- Tools and methods used in cybercrime
  - https://www.slideshare.net/patelripal99/tools-and-methods-used-in-cybercrime

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-05-17-116-EN-N

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

ISBN: 978-92-9204-230-1
DOI: 10.2824/177198