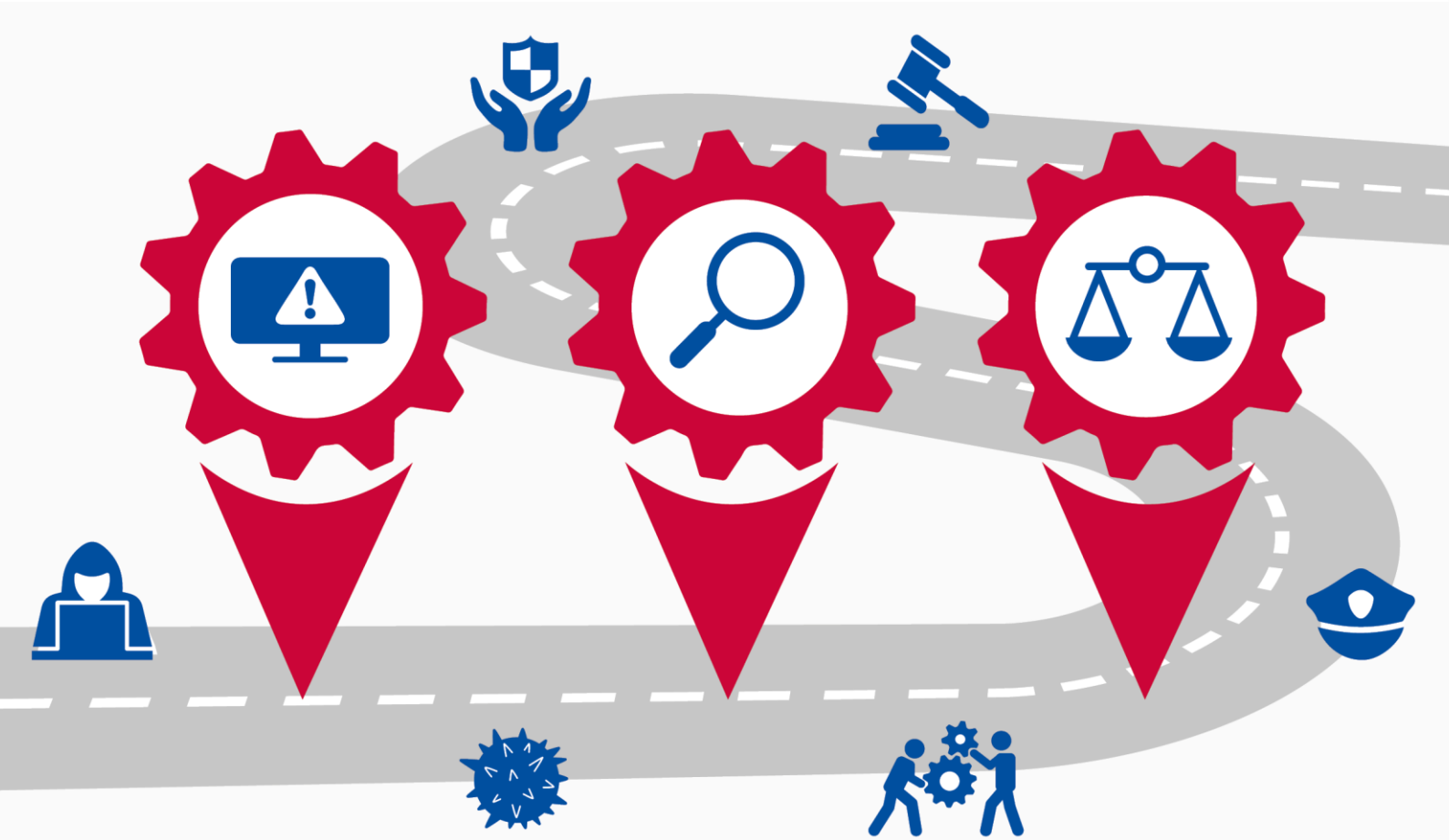
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



ROADMAP ON THE COOPERATION BETWEEN CSIRTS AND LE

DECEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

To contact the authors please use CSIRT-LE-cooperation@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Alexandra Michota (ENISA), Andreas Mitrakas (ENISA), Andreas Sfakianakis, Catalin Patrascu, François Beauvois, Koen Van Impe, Silvia Signorato, Smaragda Karkala (ENISA), Václav Stupka.

ACKNOWLEDGEMENTS

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

- The subject-matter experts, selected from the list of network and information security (NIS) experts compiled following the ENISA call for expression of interest (CEI) (Ref. ENISA M-CEI-17-C01), who on an individual basis provided valuable input to the report.
- The subject-matter experts/organisations who took the time to be interviewed and who provided valuable data for this report, including but not limited to:
  - Andreas Iacovou, National CSIRT.CY, Cyprus
  - Antti Kurittu, National Cyber Security Center, Finnish Transport and Communications Agency Traficom, Finland
  - Catalin Zetu, General Inspectorate of Romanian Police, Romania
  - Cybercrime Division, Hellenic Police, Greece
  - Danish National Police, Denmark
  - Federal Office for Information Security (BSI) – CERT-Bund, Germany
  - Francisco Losada, INCIBE-CERT, Spain
  - Giorgos Karkas, Office for Combating Cybercrime and Digital Forensic Laboratory, Cyprus Police, Cyprus
  - Jo De Muynck, CERT.be, Belgium
  - Luca Guerrieri, Italian State Police, Postal and Communications Police, Italy
  - Marco Brusegan, Public Prosecutor, Italy
  - Marco Lavernaro and Diego Marson, CSIRT, Yarix, Italy
  - NASK, CERT PL, Poland
  - National Bureau of Investigation, Hungary
  - Nelu Munteanu, Romanian National Computer Security Incident Response Team, CERT-RO, Romania
  - Øystein Andreassen, National Criminal Investigation Service (NCIS), Norway
  - Rogério Gil Raposo, National Cyber Security centre – CERT Portugal, Portugal
  - Steinarr Kristján Ómarsson, Reykjavik Metropolitan Police, Iceland
  - Timmothy Zammit, Cybercrime Unit, Malta Police, Malta

- All CSIRTs, law enforcement and judiciary respondents to the online survey conducted to collect data for this report as well as the European Union Agency for Law Enforcement Cooperation (Europol) European Cybercrime Centre (EC3) colleagues for their support in distributing the survey via their networks.
- The ENISA colleagues who contributed with their input to this study. Special thanks go to Silvia Portesi.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-331-5, DOI: 10.2824/40199

CONTENTS

EXECUTIVE SUMMARY

The purpose of this roadmap is to further explore the cooperation across computer security incident response teams (CSIRTs) – in particular with national and governmental – law enforcement (LE) and the judiciary (prosecutors and judges).

This roadmap follows the reports that ENISA has published throughout 2017 and 2018 on this subject-matter*: Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary* (ENISA, 2018), which focused on the aspects of the cooperation across the three communities; *Review of Behavioural Sciences Research in the Field of Cybersecurity* (ENISA, 2018a), which focused on human aspects of cybersecurity; *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement* (ENISA, 2017), which focused on technical aspects; and *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (ENISA, 2017a), which focused on the legal and organisational issues of cooperation. All these reports are available on the ENISA website.

When these entities – CSIRTs, LE and the judiciary – cooperate, they face challenges that have been categorised as being technical, legal, organisational and/or human behaviour as they associate with organisational culture. Understanding these challenges is essential to tackle them, further enhance the cooperation and thus better fight against cybercrime. This roadmap aims to support the cooperation between CSIRTs and LE, as well as their interaction with the judiciary in their fight against cybercrime, by providing information on the aforementioned cooperation aspects and by identifying current shortcomings and making recommendations to further enhance cooperation. The geographical coverage of this roadmap is mainly limited to the EU and European Free Trade Association (EFTA) countries.

The data for this roadmap was collected via desk research, interviews with subject-matter experts and an online survey. The data collected has demonstrated that CSIRTs, LE and the judiciary mainly face a range of cooperation challenges. The legal framework is one of the most frequently mentioned ones that acts as impeding data exchange; discrepancies in technical or legal knowledge is another one, as it may make communication challenging; the chain of custody in evidence collection might also be an issue when using methods that might make evidence likely inadmissible to a criminal trial. Incident notifications and cybercrime reporting differ from one Member State to another as different legal obligations might have been set by their national laws.

The core recommendations identified to improve cooperation between CSIRTs and LE and their interaction with the judiciary are as follows.

ENISA:

- to promote the use of ‘Segregation of duties’ matrix for avoiding conflicting roles throughout the cybercrime investigation lifecycle
- to provide guidance for building a competency framework for cybersecurity workforce
- to promote knowledge of digital forensics rules
- to promote interoperability of cooperation tools deployed and conceived considering future technologies
- to assess the suitability of cybersecurity certification for common tools and processes

Member States:

- to define and implement a national framework for cooperation having all the communities involved
- to use the 'Segregation of duties' matrix for assigning roles and responsibilities throughout the cybercrime investigation lifecycle aiming to get all communities involved
- to develop national competency framework and education and training policies
- to promote joint trainings, common inter-community technical and table-top exercises carried out by competent people
- to take into account interoperability requirements when conceiving tools

1. INTRODUCTION

1.1 PURPOSE

Collecting information on current cooperation between CSIRTs and LE communities is a key step to enhance it. In 2018, the ENISA report on CSIRT and LE cooperation aimed to present aspects of cooperation between the two communities by adding the important dimension of their interaction with the judiciary (prosecutors and judges); the purpose of this roadmap is to allow to better apprehend subtle aspects of the cooperation and challenges lying ahead.

This roadmap analyses the practices used by various countries when cooperating in order to better manage the cybersecurity incidents, identifies the key hindrances that prevent or limit effective cooperation, and looks for examples of good practices through which cooperation can be strengthened and further enhanced.

Importantly, ENISA aims at using this roadmap as guidance to plan its policy support activities in the forthcoming period of its multiannual work programme planning.

1.2 BACKGROUND OF THE REPORT

In 2018, ENISA published a report addressing aspects of the cooperation between CSIRTs and LE to fight against cybercrime, along with their interaction with the judiciary. The 2018 ENISA report on *Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary* (ENISA, 2018) confirmed that CSIRTs interact much more with LE than with the prosecutors and that they interact very rarely with the judiciary; cultural limitations set additional hindrances to this cooperation. There are legal provisions concerning CSIRTs and LE cooperation and their interaction with the judiciary; it is broadly accepted that the use of common tools to facilitate cooperation and interaction seems to be one of the key success factors for effectively fighting cybercrime.

As highlighted in the 7th ENISA/EC3 workshop for national and governmental CSIRTs and their LE counterparts (ENISA, 2018c), the theme of interaction across CSIRTs, LE and the judiciary is extremely important. In the context of the fight against cybercrime, it was also highlighted that there is a need to leverage on joint trainings to bring these communities closer together in terms of cooperating.

The *ENISA programming document 2019-2021* includes 'Objective 4.2. CSIRT and other NIS community building'. Under this objective, 'Output O.4.2.2 – Support the fight against cybercrime and collaboration between CSIRTs and LE has the goal to build upon the progress ENISA has made in supporting different operational communities (e.g. CSIRTs, LE, European [Financial Institutes – Information Sharing and Analysis Centre] FI-ISAC) to enhance mutually satisfactory ways to collaborate and support exchange of good practices among different stakeholders in operational communities in Europe (ENISA, 2018b, p. 53).

This roadmap follows up on previous ENISA work and it contributes to the implementation of the *ENISA programming document 2019-2021*, Output O.4.2.2, in particular to what is planned for as 'A roadmap of further activities on CSIRT/LE cooperation along with their interaction with the judiciary'.

While this roadmap was initially conceived as a document not for publication (to be shared with selected stakeholders only), because of the more general interest that this document might have, the decision was taken to publish it.

1.3 ROADMAP OBJECTIVES AND SCOPE

1.3.1 Roadmap objectives

The main objectives of this roadmap are as follows:

- To gather further information and discuss the current cooperation across CSIRTs, LE and the judiciary as far as it concerns their fight against cybercrime.
- To provide information on the technical, legal, organisational and cultural aspects of their cooperation and interaction.
- To formulate and propose recommendations to further enhance the cooperation across CSIRTs, LE and the judiciary.

1.3.2 Roadmap scope

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

The geographical coverage is limited to the EU (European Union, 2019) and EFTA (EFTA, n.d.) ([1]) countries. (See also (ENISA, 2015a)). This does not mean however that all these countries are covered in the roadmap and that no reference to other countries outside the EU and EFTA is made. Comparison between the EU and EFTA, or between the EU and the United States, or the EU and Asia (e.g. ASEAN), also fall outside the scope of this report.

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

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

This roadmap does not aim to present an exhaustive set of instances of cooperation across CSIRTs, LE and the judiciary, rather it seeks to facilitate the drawing of meaningful conclusions and recommendations for further enhancing their cooperation and interaction.

1.4 TARGET AUDIENCE

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

For the purposes of this roadmap, the definition of each community is listed below:

- **Computer security incident response team (CSIRT) or computer emergency response team (CERT)** is ‘an organisation that studies computer and network security to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and […] offer other information to help improve computer

([1]) 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.

and network security'. At present, 'both terms (CERT and CSIRT) are used in a synonymous manner, with CSIRT being the more precise term' (ENISA, 2015a, p. 7) (ENISA, 2015, p. 12) (ENISA, 2016a, p. 10). Governmental CSIRTs (Council, 2016a) are teams whose constituency are the public administration networks (ENISA, 2017);

- **Law enforcement (LE), law-enforcement agencies (LEAs), police and police agencies police and police agencies** are terms used in this report, and are synonymous, and used to refer to police and police agencies, also used as synonymous. LE is 'any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' *(Official Journal of the European Union*, 2016);
- **Judiciary** refers both to prosecutors and judges (a similar approach taken in (Council of the European Union, 2017). Prosecutor refers to 'a legal official who accuses someone of committing a crime, especially in a [criminal] law court' (Cambridge Dictionary, n.d.). Judge refers to a person who is in charge of a court of law and who makes final decisions.

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

2. METHODOLOGY

2.1 INFORMATION COLLECTION INSTRUMENTS USED

The methodology chosen for creating this roadmap is largely inspired by the methodology used in previous ENISA reports (ENISA, 2017), (ENISA, 2017a), (ENISA, 2018). This approach represents a tested practice that is suitable for the purpose of data collection and analysis for policy support in cybersecurity. Data for this roadmap was collected through desk research, interviews with subject-matter experts and via an online survey. A qualitative methodological approach has mainly been used due to the rather new field addressed; however, some quantitative data were also collected: an online survey was carried out to validate and complement the findings from the desk research and the interviews.

2.1.1 Desk research

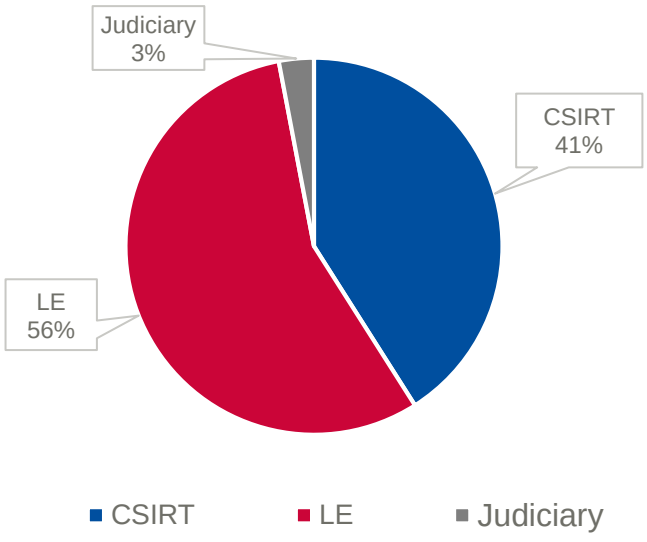
Initial desk research was carried out based on publicly available information sources, including ENISA publications. The findings from this desk research were particularly useful for the scoping of the report and for drafting the questionnaire to support the interviews.

Supplementary desk research was conducted to address certain specific topics that the project team deemed appropriate to examine in more depth following the analysis of the data collected via the interviews.

2.1.2 Interviews and written replies to the questionnaire

A total of 31 subject-matter experts from 22 Member States replied to the questionnaire either via structured interviews or with written replies. Of the respondents, 12 were experts from the CSIRT community (mainly but not exclusively from national/governmental CSIRTs), 18 from the LE community (mainly national police but also one from a local police force), and one from the judiciary community.

Figure 1: Overview of communities of respondents to the interview



A questionnaire (see Annex C – Questionnaire to support the subject-matter expert interviews) was prepared to support the interviews. Most questions were open. For all questions, including yes/no questions, interviewees could add comments and additional information.

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

The interviews were carried out from June to mid-July 2019. They were conducted either face to face or via phone and they lasted around 1 hour each. Interviewees received the questions in advance and in most cases they had the opportunity to review the notes taken by the interviewers (ENISA project team) with their replies and validate them.

Two out of 31 respondents opted to submit written replies only. Some interviewees completed also the online survey.

The questionnaire developed to collect data for this 2019 roadmap that addresses the issue of cooperation across CSIRTs, LE and the judiciary and aims to collect more in-depth information on technical, legal, organisational and cultural aspects of their cooperation.

The interview questions started with a set of common questions for all participants to answer, followed by three sets of specific questions for CSIRTs, LE or judiciary to answer respectively.

2.1.3 Online survey

An online survey was carried out to collect additional data to validate and further substantiate some findings. It was comprised of 25 questions (see Annex D – Questions in the online survey), most of them with closed answers and some with the possibility to add additional comments and provide more details related to the answers.

The survey was developed using EUSurvey ([2]), a survey tool which is 'supported by the European Commission's ISA programme, which promotes interoperability solutions for European public administrations'.

The invitation to complete the survey was disseminated via:

- a closed ENISA mailing list of European national and governmental CSIRTs;
- a Europol mailing list of the European Union cybercrime task force (EUCTF ([3])), 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 June 2019 and was open for around 2 weeks. The data collected via the online survey was used to validate the data collected through the desk research and the interviews and used to produce some statistical graphs.

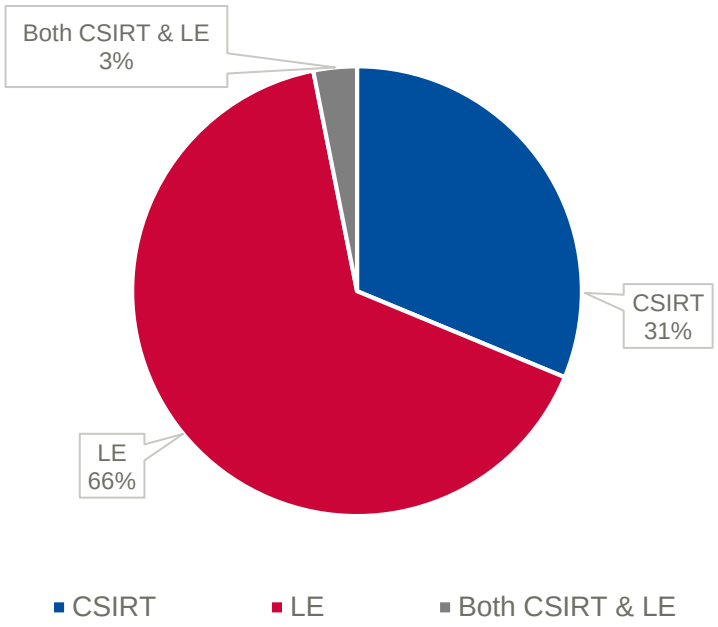
A total of 33 replies ([4]) were received. Of these ([5]), 24 were from EU Member States and EFTA countries (EFTA, n.d.) and one from a non-EU/non-EFTA country. It must be noted that the reply from non-EU/non-EFTA country was somewhat in line with the other replies received and has been used to formulate general considerations; however, the graphs in this roadmap were

([2]) https://ec.europa.eu/eusurvey/home/welcome
([3]) In execution of the JHA Council conclusions of 27-28 November 2008 and of the 26 April 2010, Europol, together with the European Commission and the EU Member States, have set up the European Union cybercrime task force (EUCTF) composed of the Heads of the designated national cybercrime units throughout the EU Member States and Europol. The EUCTF is an interagency group formed to allow the Heads of Cybercrime Units, Europol, the European Commission and Eurojust to discuss the strategic and operational issues related to cybercrime investigations and prosecutions within the EU and beyond.
([4]) ENISA is not privy of the exact number of recipients of the Europol list. The ENISA mailing list is approximately 63.
([5]) More than one community of each MS participated in the online survey.

developed based only on the 24 replies from EU and EFTA respondents, to ensure full consistency with the geographical scope of the report.

In total, 11 respondents out of 33 in the EU and EFTA, were from the CSIRT community, 21 from the LE community and one belonged to both of these communities; no replies were received from the judiciary. An overview of the composition of the EU and EFTA respondents, based on the community they belong to, is presented hereinafter in Figure 2.

Figure 2: Overview of communities of respondents to the online survey



2.2 DATA USED TO DEVELOP THE RECOMMENDATIONS

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

2.3 SELECTION AND CLASSIFICATION OF THE STAKEHOLDERS

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

- CSIRTs/LE/judiciary community
- geographical location
- size of country (population)
- level of maturity in CSIRT-LE cooperation
- level of CSIRT maturity ([6])
- size of the CSIRT
- relevant jurisdiction

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

2.4 CONTRIBUTION BY SUBJECT-MATTER EXPERTS

ENISA selected six external subject-matter experts from the list of NIS experts compiled following the ENISA CEI ([7]) (Ref. ENISA M-CEI-17-T01) (ENISA, n.d.).

Four of them contributed to this roadmap by supporting the data collection and the drafting while two were reviewers. The two CEI experts contributing as reviewers reviewed this roadmap in several rounds including the first draft in May 2019, an intermediate draft in June 2019, the semi-final and the final draft in July 2019.

All six experts contributed *ad personam*.

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

([7]) The ENISA CEI list comprises of experts in various NIS subject-matters that have been selected according to a procedure in line with the ENISA financial regulation; these experts are called upon by ENISA from time to time to support the Agency in carrying out its operational duties.

3. CSIRTS, LE AND THE JUDICIARY: STATE OF PLAY

This chapter presents the state of play for the cooperation across the three communities. This chapter also discusses cases that lack cooperation; examples for cybercrime cases that cooperation is required are also presented.

3.1 LACK OF COOPERATION

The extent to which cooperation and information sharing among the three communities is taking place varies considerably across Member States due to various reasons. As seen in Figure 3, in some countries, cooperation is universally accepted as a necessary measure, required by law, implemented in guidelines and internal policies and supported by implementation of technical, organisational and procedural measures; while in others, the cooperation is limited to providing information (in the form of evidence or witness testimony) when requested by the LE or the judiciary. Figure 4 depicts that all three communities agree that cooperation across CSIRTs, LE and the judiciary should be mainly regulated by national legislation.

Figure 3: Replies to question 22 of the online survey conducted for this roadmap

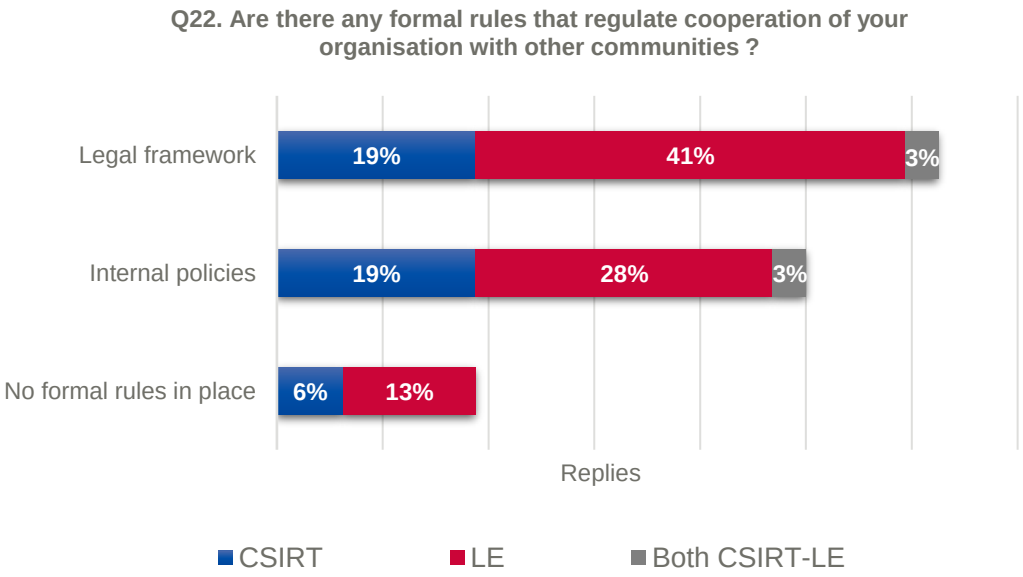
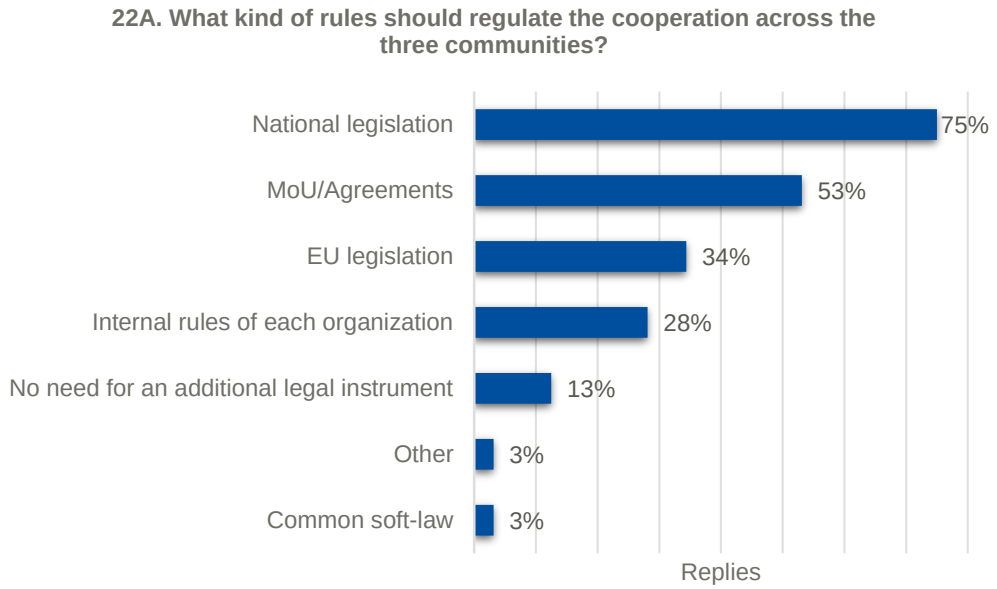


Figure 4: Replies to question 22A of the online survey conducted for this roadmap



As both desk research and interviews showed, all three communities agree that effective collaboration and information sharing can streamline their work. By working closely together the communities may achieve increased effectivity of mitigation of cybersecurity incidents as well as of cybercrime investigations, better quality of electronic evidence, greater availability of expertise and specialised technical tools, improved availability of information about relevant vulnerabilities and threats, increased effectivity of response to the large-scale attacks on national infrastructure, and ultimately therefore, greater security in society.

Following chapters of this roadmap examine the possible reasons for the lack of cooperation across CSIRTs, LE and the judiciary is highlighted and present the tools and mechanisms through which this cooperation can be promoted at EU and national level.

Not all cyber incidents are cybercrimes (so LE do not need to be informed) and not all cybercrimes are considered cyber incidents (so CSIRTs do not need to be informed). This means that LE and CSIRTs do not always have the same interest in incidents or investigations, which also affects the way they further handle each case. Since cybercrime crosses borders, cooperation among countries is often crucial in the fight against it. In this regard, at least three difficulties are identified:

1. **Political difficulties**. Some Member States are reluctant to cooperate because they prefer to achieve the investigative results on their own. Sometimes this is linked to a political vision that considers collaboration across operational communities as erosion of sovereign state powers as cybersecurity has entered the diplomatic realm (European Commission, 2018a). In particular, it seems that diplomacy encounters difficulties to promote EU values, interests and principles in the cyber domain. Moreover, there are some issues in supporting aimed at strengthening capacities of partner countries and organisations in the field of cybercrime (EU Council, 2016), (Moret E., Pawlak P., 2017).
2. **Legal difficulties**. At European level, there are different regulations related to the cybercrime depending on the state. This makes the interaction for CSIRT, LE and the judiciary more difficult.

3. **Difficulties related to different mindset approaches**. CSIRT, LE and the judiciary have different approaches or mindsets, which also derives from the different educational and scientific backgrounds. In particular, CSIRTs have a 'technical mentality' while the judiciary has a 'legal mentality'. The LE have partly a 'legal mentality' and partly a 'technical mentality' that is entrenched in how society operates in the area of crime. The different mentalities make communication among these three entities not always easy. This can also lead to limitations of cooperation or at least a slowdown in cooperation.

Despite these three obstacles, there are some improvements in cooperation among CSIRTs, LE and the judiciary at the European Union level. This derives from a set of factors. For instance, European Union acts aimed at encouraging cooperation; big complex transnational cases (see Petya (EC3, 2017), NotPetya (Europol, 2019), WannaCry (ENISA, 2017b), etc.) have changed the perception of the need for cooperation; and training and education needs in the area of cooperation have also been highlighted through reports (ENISA, 2017a); (ENISA, 2018).

National legal framework and CSIRT type are some of the major differentiators when it comes to frequency and level of cooperation across CSIRTs, LE and the judiciary. National and governmental CSIRTs are usually more involved in this type of cooperation, especially those that are functioning under a National Cyber Security Centre (NCSC) type organisation. Obviously, operating under the same governmental umbrella, or even working at the same facilities, enables organisations to better know each other and to benefit from a higher mutual trust both organisationally and personally. Another important aspect of this setup is that it poses less legal challenges for cooperation and information sharing (e.g. CSIRT is not considered an external organisation). Background check of the CSIRT staff is just one example of things that increase the level of trust from the LE perspective.

Interviews show a strong trend regarding cooperation obstacles, the majority of those being attributed to procedural difficulties and legal issues. Cultural and organisational difficulties, may be seen as a major issue; however, interviewees have identified those cooperation challenges as less aggravating. (See Figures 5, 6).

Figure 5: Replies to question 1 of the online survey

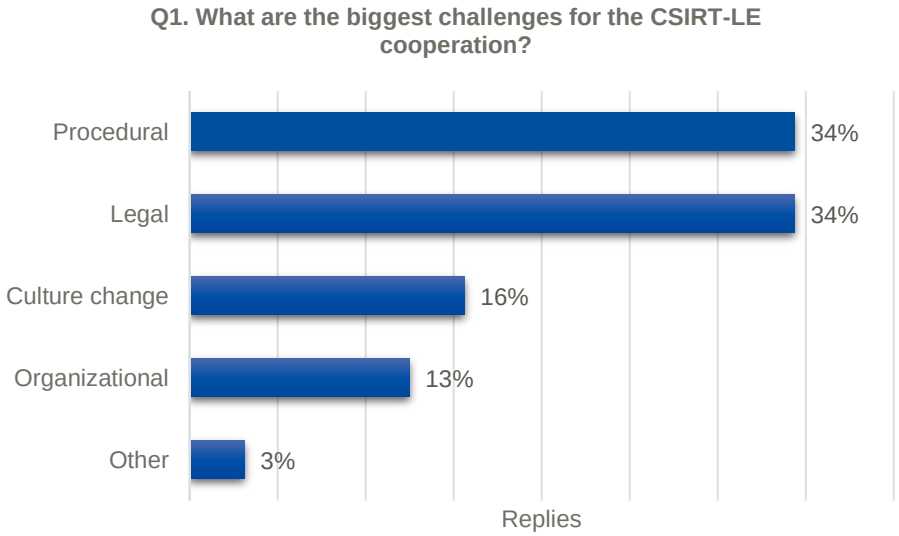
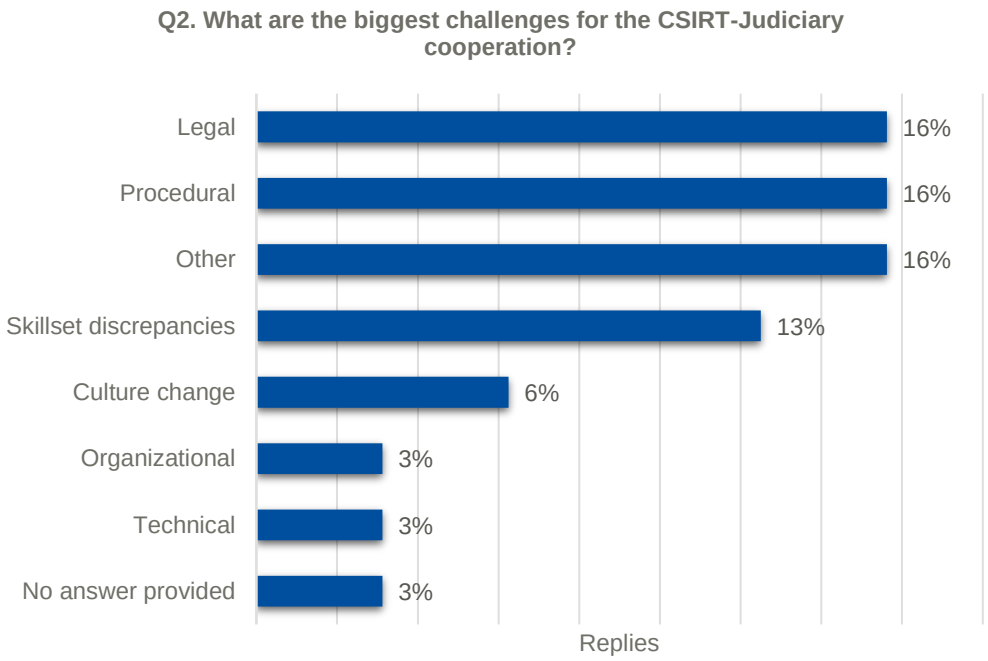


Figure 6: Replies to question 2 of the online survey



3.2 EXAMPLES OF CYBERCRIME CASES WHERE COOPERATION IS REQUIRED

When cooperating in a cybercrime investigation case, each entity shares its expertise to move the case forward. LE conducts the investigation following the instructions of the magistrate/prosecutor who determines the strategic options. The magistrate usually decides whether to use coercion or not (seize, searches, interception) while LE conduct investigations on field. Coercion-based acts as well as open sources investigation provide a lot of data that need to be analysed and processed. In this phase, CSIRT expertise might be needed, having required internal skills and tools.

Some big complex transnational cases are presented below:

- Altran was one of the most important European IT consulting companies. At the beginning of 2019, it was struck by a ransomware attack a few weeks before markets financial publication. Stocks took a hit and a few month later, Altran was bought out by Capgemini (Capgemini, 2019). Cooperation between CSIRT and LE took place immediately: Altran was in contact with several critical infrastructures. As such, national CSIRT was first responder on site. They collected evidence and then provided it to LE for investigation.
- Sytech leak (Abrams, 2019): on 18 July, 0v1ru$, a so far-unknown hacking group, published allegedly leaked Russian Federal Security Service's (FSB) data. Screenshots published on twitter showed interface of internal network as well as a massive (7 Terabytes or 7 000 gigabytes) amount of leaked data. Most of these data were concerning FSB Unit 71330 spying and surveillance projects. Among them, a Tor de-anonymisation project which had been previously suspected by researchers. Data were then passed to Digital Revolution group who put it at journalists' disposal.
- NotPetya attack (Andy Greenberg, 2018): this attack was conducted through the Ukraine main tax-paying application which infected entire parts of the country's economy as well as other big foreign companies (A.P. Moller-Maersk, Saint-Gobain S.A., Merck KGaA).

Looking more of a wiper than a ransomware, because lacking decrypting capabilities, NotPetya was an attack, seemingly, against a country. Because of the very complex technical architecture used by attacker and extensive planning they seem to have conducted, investigations showed to be very heavy and technical. CSIRT provided its technical expertise.

- Botnet takedown (usually requires a close and efficient cooperation and coordination among CSIRTs, LE and the judiciary from different countries. The Avalanche botnet dismantling (Eurojust, 2016) was a 4 years operation which implied a strong CSIRT-LE cooperation. German BKA, criminal police, and BSI, national CSIRT, worked together for 4 years to takedown the infrastructure.

4. COOPERATION ASPECTS

4.1 ORGANISATIONAL ASPECTS

4.1.1 Organisational structure

4.1.1.1 Segregation of duties per community

Each community has its own discreet set of responsibilities, duties, expertise, powers and technical and procedural tools. Sometimes, however, duties and responsibilities overlap, and this might lead to undesirable interference to each other's activities. Therefore, it is important for the communities to understand each other's duties.

For this purpose, the segregation of duties matrix (SoD) developed in the 2018 ENISA report on *Cooperation between CSIRTs and LE: interaction with the Judiciary* (ENISA, 2018) could be used in order to highlight conflicting or overlapping duties performed by one community or more. Not only does this matrix identify the key responsibilities for each community but it also links them with the skills required to fulfil these duties by presenting appropriate training topics that should be provided ([8]).

When using the SoD matrix, it is necessary to identify the key roles of individual communities. CSIRTs are responsible to ensure the confidentiality, availability and integrity of systems within their constituency. LE aims to trace offenders and gather evidence that describes the course of the offence and show offenders' guilt. On the basis of the results of the work of the law enforcement authorities, the judiciary assesses the factual and legal conclusions resulting from the evidence obtained and decides on guilt and punishment.

The CSIRTs' role is to prevent incidents from happening by implementing appropriate security measures or suggesting such measures to their constituency. And in the event of an incident, their aim is to detect and analyse the incident and apply appropriate measures, remedy the damage and subsequently secure the exploited vulnerabilities, or other existing threats. As first responders, however, they could be also responsible for advising their constituency to report the incident to LE (or in some cases they might have themselves a duty to report), expected to share the information with other sectors or targeted industries, and required to provide necessary assistance to other communities and collect evidence.

LE is dedicated to investigate cybercrimes and investigate possible culprits. They have legal power to mandate entities to cooperate in the investigation and disclose information or to contribute to the investigation in different ways: seizes, searches, and interceptions. LE responsibility is to collect evidence in a lawful way, even if it may challenge remediation or business continuity. Of course, they seek to avoid further consequences to the victims, but sometimes, evidence collection can postpone remediation or return to normal.

The roles of the judicial authorities vary, as public prosecutors or investigative judges/magistrates usually direct the course of an investigation, to authorise some investigative actions, to analyse and interpret collected evidence and provide legal assistance to the LE. The court judges have the authority to authorise some investigative measures, to admit and assess the evidence provided by LE and prosecutors, and ultimately decide who the victim is, who the

([8]) ENISA does not keep track of whether and, if so, who adopted and implemented the SoD matrix in practice, so it is not known what its use looks like in practice and for what purposes and to what extent it is actually used.

offender is, what the crime was and how the offender should be punished. In addition, the judicial authorities should act in such a way as to ensure that fundamental rights are respected during the investigations as well as during the trial. Examples of fundamental rights are the Right to a fair trial and Right to an effective remedy (Council of Europe, 1950), Article 6 and Article 13 and (EU Parliament, EU Charter of Fundamental Rights, 2012) Article 47, Right to respect for private and family life ((Council of Europe, 1950), Article 8 and (European Union, 2012) Article 7), Right to no punishment without law ((Council of Europe, 1950) Article 7 and (EU Parliament, EU Charter of Fundamental Rights, 2012) Article 49), Prohibition of discrimination ((Council of Europe, 1950) Article 14 and (EU Parliament, EU Charter of Fundamental Rights, 2012) Article 21).

The role, the powers and responsibilities however vary greatly in individual states. There are significant differences also at European level. More in-depth information on the role of all of the communities can be found in 2018 ENISA report *Cooperation between CSIRTs and LE: interaction with the Judiciary* (ENISA, 2018).

4.1.1.2 Indicative example of Segregation of duties matrix

Figure 7 depicts a very indicative example of a SoD matrix. It is not based on a specific legal system. Depending on the country and its legal system this duty matrix might be different and show different segregation of duties.

As seen in the matrix, the activities of crime have been categorised based on the timeline of a crime; in particular, we have activities prior to an incident/crime, during the incident/crime and post incident/crime activities.

The following SoD matrix presents, with all its limitations due to abstraction and generalisation, how individual duties and responsibilities may be assigned among the three communities. As seen in Table 1 there might be overlapping duties performed by more than one communities. Once there is lack of coordination, this can lead to interference with each other's activities, which can have a negative impact on the efficiency and effectiveness of their work. It is therefore appropriate in these cases that the relevant communities agree on rules for the segregation of duties in order to prevent these negative effects.

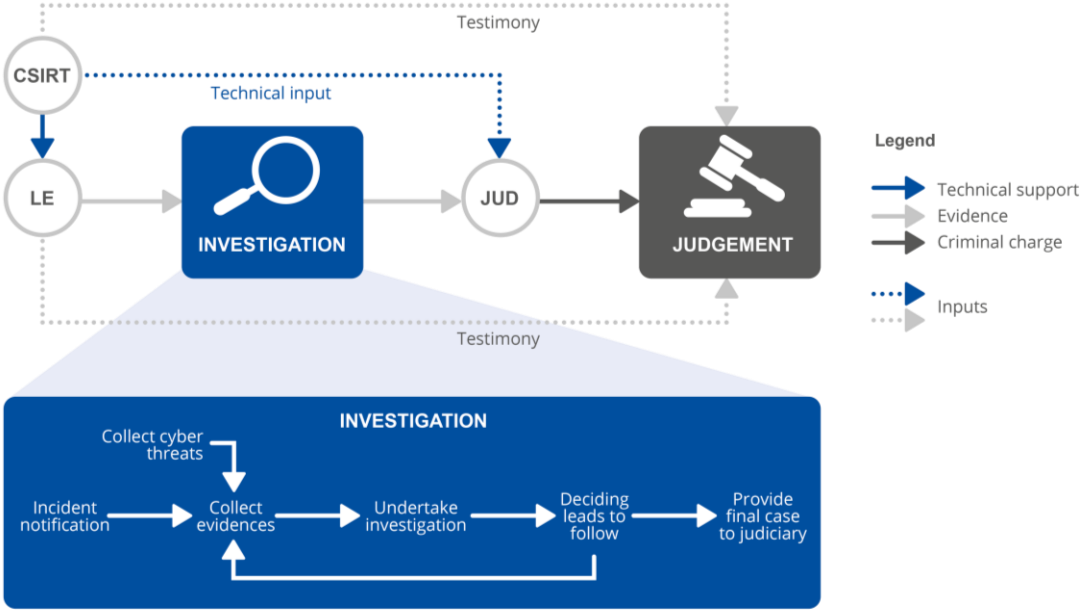
Table 1: SoD Matrix – Indicative example

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training	✓	✓	✓	✓	Problem-solving and critical thinking skills
Collecting cyber threat intelligence	✓	✓		✓	Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats	✓	✓		✓	Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats	✓				Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime	✓	✓			Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cyber security incident/crime	✓	✓			Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cyber security incident/crime	✓	✓		✓	Incident and crime classification and identification
Identify the type and severity of the compromise	✓	✓		✓	Knowledge of cyber threats and incident response procedures
Evidence collection	✓	✓		✓	Knowledge of what kind of data to collect; organisation skills
Providing technical expertise	✓				Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial	✓	✓		✓	Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)	✓			✓	Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime	✓	✓		✓	Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)	✓				Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling	✓				Communication skills; communication channels
Mitigation of an incident	✓				Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation		✓		✓	Knowledge of the legal framework; decision-making skills
Leading the criminal investigation			✓	✓	Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation			✓	✓	Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE		✓	✓	✓	Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution	✓	✓	✓	✓	Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery	✓				Technical skills
Protecting the constituency	✓				Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view	✓				Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence		✓	✓	✓	Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE			✓	✓	Testimonies in a criminal trial
Admitting and assessing the evidence			✓	✓	Evidence in a criminal trial
Judging who committed a crime			✓		Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost	✓	✓	✓	✓	Evaluation skills
Reviewing the response and update policies and procedures	✓				Knowledge how to draft an incident response and procedures

4.1.1.3 Interaction flowchart

A graphic representation of the interaction flow is presented in Figure 7, based on an abstraction and generalisation of the data collected for this roadmap (especially the responses from the online survey). This flowchart is a continuation of last year's information flowchart focusing on the investigation phase of a cybercrime (ENISA, 2018, p. 40). This graphical representation, with all the limitations due to abstraction and generalisation, presents actions taken during the investigation phase; although criminal investigation seems to be under LE duties, it is worthwhile to mention that CSIRTs' technical expertise and judicial authorities' viewpoint are needed in order the investigation to be completed.

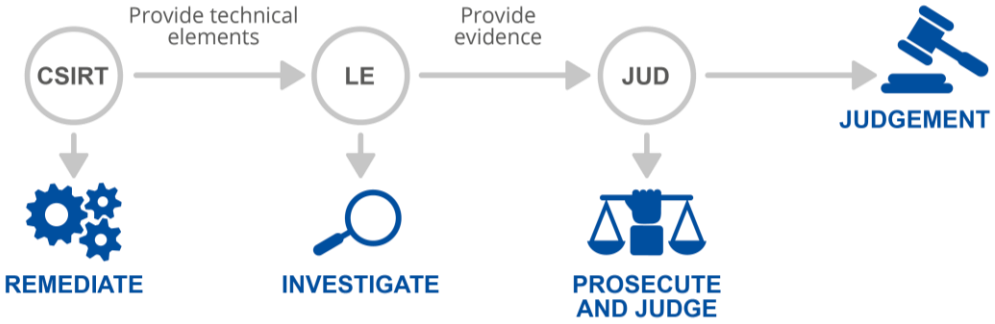
Figure 7: Graphical representation of the flow of information across CSIRTs, LE and the judiciary: Analysis of the investigation phase



4.1.1.4 Complementarity of duties

Each community's duty is part of a process which lead to identifying cybercrime perpetrator(s) and building a safer internet. CSIRTs focus on remediation and business continuity while LE objective is to identify the perpetrator and then the judiciary will guarantee the legal prosecution so the culprit can be charged and brought before the competent court. Figure 8 depicts the roles and duties of each community are illustrated in the graph below.

Figure 8: Roles and duties per community



Even though each community has different goals, means, powers and duties, their responsibilities are complementary. The key goal of the CSIRTs is to ensure availability, integrity and confidentiality of networks and systems within their constituency; however, when the security is threatened by external attackers, they would need law enforcement to identify the attacker and prevent him from further attacks. On the other hand, to successfully identify and prosecute the attacker, law enforcement might need information, data, expertise or equipment that in some cases might be available exclusively to the CSIRTs. Finally, in order for the judiciary to be able to convict and punish the attacker, they need actionable electronic evidence so as to understand how the attacker operates and what the electronic evidence suggests.

Therefore, the activities of each individual community must be coordinated. In some cases, there are internal security policies of each organisation, or common policy for both communities that govern the information sharing between certain CSIRTs and LE. Such internal security policies can improve cooperation between CSIRTs and LE by allowing-the CSIRTs to acquire a greater knowledge of e-evidence collection requirements and develop compliant operational practices.

4.1.1.5 Discrepancies in finalities: investigation vs remediation

Evidence collection

- **Investigation: needs for evidence collection**
  Evidence must be collected in a lawful manner. If a specific law, applying to all involved communities, outlines detailed standards to handle an investigation, it must be applied and interpreted within the scope and in the meaning of other legal instruments, national and possibly international, that are aimed at protecting fundamental rights ([9]).

  Forensic evidence collection must guarantee evidence data have not been altered or tampered with. To do so, investigators must for instance use write blockers ([10]). Should a member of LE staff not do this, the lawyer of the defendant could argue that there had been evidence alteration by the police.

  Each step of evidence collection is bordered, whether in a technical manner, by imposing use of vetted tools, or controlled by a magistrate. In case of interception, some specific operations can only be carried out by using tools vetted by a dedicated commission.

([9]) For more on differences between common and civil law systems please see subchapter 4.4.1.4. below.
([10]) A writing blocker is a system aimed at avoiding any alteration of the target device during copy. It is mandatory to guarantee proof relevance in trial.

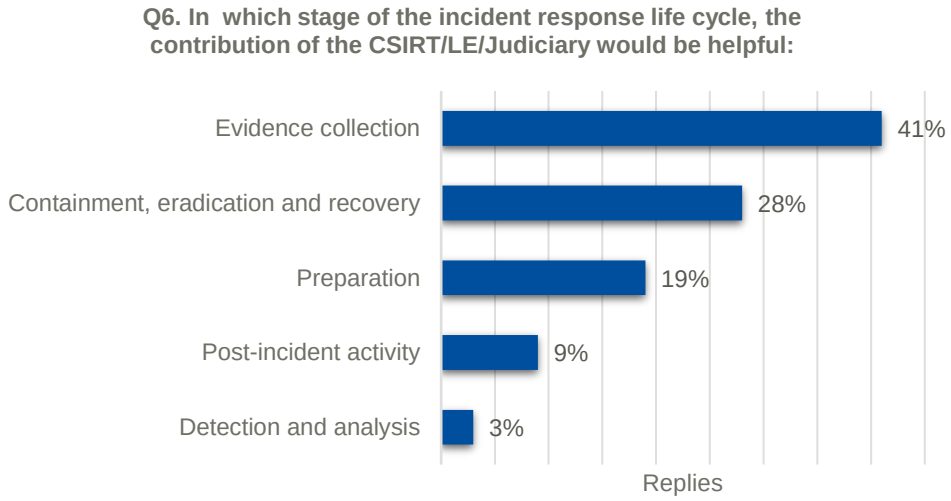
- **Remediation: may destroy evidence**
  Depending on the IT infrastructure affected as well as the processes and procedures used for backup and logging, remediation without proper evidence preservation could actually destroy evidence and may complicate investigations further.

  For instance, re-imaging of an infected workstation can delete information about a malware family. This can be prevented by firstly collecting volatile data (live data, before shutting down the machine: network connections, running apps/processes, paging file, memory dump, etc.) and then taking a full disk image. In virtualised environments, such activities can be done by simply taking a virtual machine snapshot before the re-image.

  The functioning of CSIRTs is not as strictly regulated as in the case of LE, and therefore they are more flexible to choose appropriate measures to deal with an incident. However, if CSIRT members are not familiar with the law enforcement processes, the handling of the electronic evidence and the legal requirements for evidence admissibility, their activities may render the digital evidence inadmissible and therefore useless for criminal prosecution.

Based on the online survey results (see Figure 9), the most critical phase where cooperation is of great importance is the evidence collection phase. During this phase, LE may request CSIRT experts for support in order to lead complex technical activities; LE may have limited internal resources for the technical analysis.

Figure 9: Replies to question Q6 of the online survey



Timing:

Timing of operations constitutes one of several discrepancies in the CSIRT/LE way of intervention. An investigation often needs LE to access private data. As such, access to this data is authorised mainly under a magistrate's control and strictly ruled by law. This guarantees civil liberties but the several layers of controls may introduce a lot of uncompressible delay. Data access is usually managed by several tracking procedures which eventually generate red tape. As an example, setup of an interception can take more than 1 week. Transnational cooperation, especially outside the EU, is subject to an even more demanding set of requirements and formalities.

CSIRTs have as a main task to respond to and mitigate cyber incidents. When the cyber incident has a cybercrime component the remediation part might interfere with the LE investigation if proper cooperation and a remediation procedure has not been set in place. For example host disinfection or reimage might erase the necessary evidence/traces for investigations.

Because of the strict requirements that apply, LE timing is usually longer than that of CSIRTs. While CSIRTs have to provide fast, sometimes immediate, response to incident, LE's investigations take longer to pursue. If first LE responders' actions are quick to preserve evidence, further investigation timeframes require time due to legal constraints. Investigations imply evidence search and collection, warrants and request issues, analysis of new evidence and so on. To be efficient, evidence analysis (malware samples, logs files, compromised hard drive or memory dump) must be thorough and extensive. Evidence and IOCs extracted will then trigger new research such as server seize, interception of IP, identification of an email or an ISP account (Facebook account, Google account, etc.). Each of these steps may have to be vetted by a magistrate which extends investigation duration. Furthermore, when European or international cooperation is implied, MLATs (international warrants) use can take several months to occur.

Another key factor that can delay the investigation is the innovative nature of cybercrime. It comes with challenging legal questions that the current legal framework has not been conceived for. For example, how to seize a bitcoin wallet outside the investigating police force's country? Cybercrime investigations trigger legal questioning which often fuel law modification. No matter how long it takes, each legal question must be carefully discussed among all actors (LE, magistrate, even Europol and Eurojust) and can postpone even more next investigation steps.

During the remediation phase, there is limited time frame for action as systems need to be recovered as soon as possible. Sometimes proper evidence collection or preservation would increase significantly the remediation time which might have a negative impact from a business perspective. That is why there are situations when the victim needs to decide on the priorities: remediation vs investigation. CSIRTs need to be prepared to offer this consultancy to the victims.

Taxonomy:

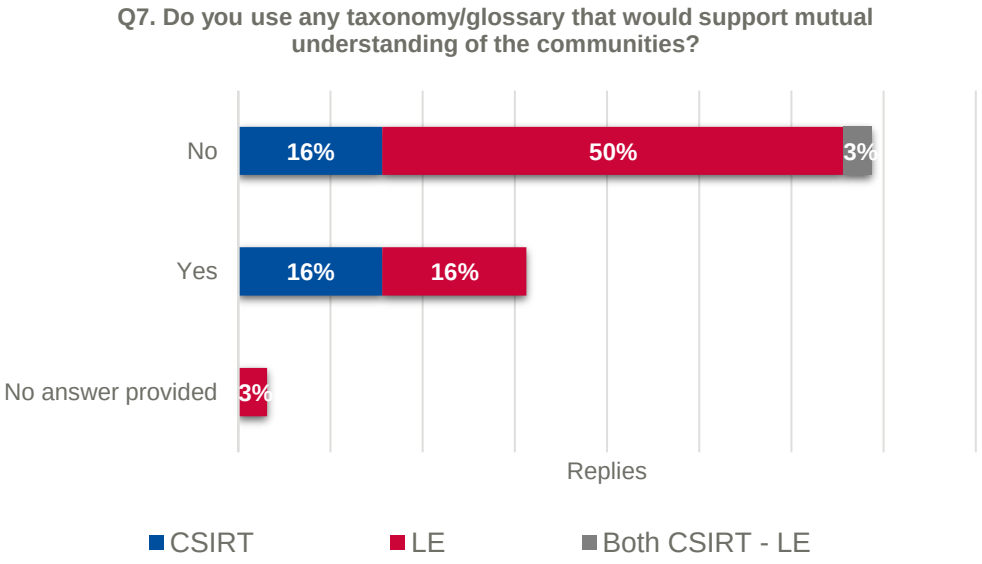
The vast majority of the CSIRTs use at least one taxonomy and that is because they usually publish periodic reports on incidents handled and also because they process and share data automatically. ENISA promoted the use of taxonomies in the CSIRT community as part of the best practices sharing. (ENISA, 2016)

LE use taxonomies too but more often refer to legal definitions of crimes foreseen in the criminal law framework, namely in the articles of the criminal code. In the criminal code each crime/infringement is described in general terms. The main difference is those descriptions are results-based: intrusion in a system is the act of unlawfully accessing someone else's system. Objectives are different: cybersecurity taxonomy defines how things have been done to be able to identify vulnerabilities, correct them and reach a more secure situation after the incident than before. The criminal law aims at having perpetrators punished and stopping the commission of crimes. But the same issue can happen the next day from another perpetrator. Since the criminal law is the base ground for any investigation work, LE often refer to legal definitions of crimes. It is changing slowly because of the needed interactions with cybersecurity ecosystem and, for investigations purposes, to be technically more efficient.

There is however clear motivation to share a common language among the communities since their cooperation is necessary. There are some common taxonomies available that can be used to achieve mutual understanding. The common taxonomy developed by ENISA and Europol lists and categorises most common cybersecurity incidents and links these incidents to relevant offenses defined in the Directive on attacks against information systems (EU Council, 2013) and CoE Convention on Cybercrime (Council of Europe, 2001). Some countries also decided to further develop their taxonomies – some included links to national criminal codes, definition of incidents from CSIRTs' perspective, or suggestions on how to proceed with incident mitigation, report identified offences or collect evidence. In some cases, a glossary of terms, which defines the meaning of certain terms used by individual communities, may also be appropriate in order to further enhance mutual cooperation and understanding. Such a glossary could be especially useful for the judiciary, since judges and public prosecutors have legal education and very technical language may represent a challenge for them. An example of such a glossary that also facilitates cross-border cooperation, as it contains definitions in the national language and in English, can be the Cyber Security Glossary developed by the authorities of the Czech Republic (Gov CERT CZ, 2015).

Figure 10 highlights that 45 % of LE respondents stated that they do not use any taxonomy or glossary that would support mutual understanding of the communities.

Figure 10: Replies to question Q7 of the online survey



The judiciary tasks are based on the criminal law using in particular the criminal code that applies to each national legal system; this is used as a basis to qualify the criminal offences. However, adopting a common language is necessary in order to improve the cooperation with the CSIRT and LE communities as there is lack of common understanding. The judiciary usually have a legal background and might face challenges with technical language and technical problems.

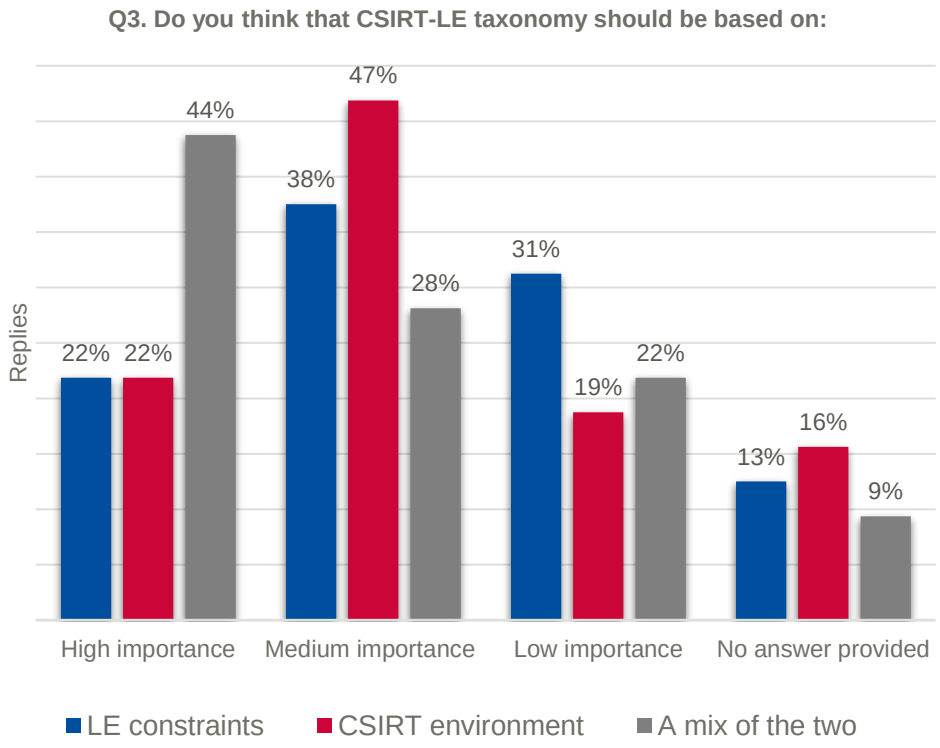
Currently, in criminal trials, the Court may ask for CSIRTs' technical expertise in order to explain technical concepts, such as IP addresses. This is because the judiciary are not always familiar with technical terminology. It would be of great importance for the judiciary

to receive more and more technical training that would help when dealing with cybercrime cases.

The judiciary evaluate cybercrime through the criminal law (mainly but necessarily limited to the criminal code) that determines which crimes and offences are punishable. As a form of taxonomy, it is more results-oriented without focusing on how a crime has been committed. As such, this would probably be very different from a standard taxonomy; as long as systems have been hacked, details such as vulnerability exploitation, scam or human errors could only be examined as aggravating factors when assessing the sentence imposed. What the judiciary need to know is that the perpetrator is responsible for infringing the system.

Based on the online survey results, what is of high importance is the CSIRT-LE taxonomy to be based both on LE constraints and CSIRT environment (See Figure 11).

Figure 11: Replies to question Q3 of the online survey



4.1.2 Governance framework and compliance

4.1.2.1 Management practices

Management practices usually refer to the approaches that are followed by managers aiming to make their organisation more efficient. Differences are highlighted in the management practices used by each community and are presented below.

- **CSIRT approach:** CSIRTs are usually small organisations with simple hierarchy (flat organisations) and this is a key factor in the fast decision-making process. Another aspect is that CSIRTs tend to have more operationally involved managers (or at least informal leaders) to be able to make quick decisions for initiating the CSIRT's key activity, i.e. the

incident response. Some CSIRT may organise a form of polyvalence where a person can be assigned to different tasks each week.

- **LE approach:** At operational level, LE use a hierarchical organisational structure based on ranks to ensure information flow and decision-making at the desired level. One of the key challenges in cybercrime relates to the method applied in either LE or CSIRTs, with CSIRTs generally taking a more technical approach on incident analysis.

  Information flow and reporting seem to be a cultural matter as LE usually have a fairly strong set of processes for information flowing. It allows decision-makers, operational or even politicians, to be provided with the most possibly relevant information. This type of organisation proves to be very efficient in cases of emergency or a crisis. Staff of any hierarchical level know their roles of intervention and any legal requirement about information sharing between LE and their counterparts. Thus, in the EU cooperation field, this pyramidal organisation with Europol acting as coordinator has proved to be very efficient.

- **Judiciary approach:** The judicial authority is a functional authority for LE and an adjudicator in terms of applying the law. Compared to the LE, the judiciary usually have the powers to take measures against a criminal action and control investigative acts.

  In most constitutional systems, the judiciary are independent from other authorities in a Member State. However, the level of their independence varies from country to country, as well as the scope of each authority and its organisational structure. It is generally accepted that the judicial authorities have a hierarchical organisational structure and in some countries dedicated units are dealing with certain types of crime. This hierarchical structure is met in both the courts and the prosecutor's offices. From the perspective of cybercrime investigation, it is crucial to determine to what extent the judicial authorities are specialised in a type of crime. In some countries, there are specialised units in courts or prosecutors' offices dedicated to cybercrime that have staff with technical expertise. However, in other countries, this is not possible because of the organisational structure of courts and prosecutor's offices and relevant legislation; it is then up to the individual judges and prosecutors to decide whether or not to specialise and voluntarily educate themselves.

  Another important aspect is that the judiciary has institutional authority over the law enforcement. As a rule, the course of the investigation is supervised by a prosecutor or an investigative judge whose authorisation or cooperation is often required to carry out certain procedural measures. The evidence and information collected during the investigation must have the quality of admissible evidence and be onwards provided to the judge in a comprehensible way, for the latter one to decide on its relevance and assess the weight of evidence.

4.1.2.2 Internal security policies permitting and supporting information sharing with CSIRT/LE counterpart

Each CSIRT/LE is capable of sharing information when working with its own community but both communities might face have difficulties in sharing with each other due to legal and operational restrictions. Usually LE have more restrictions on exchanging information with CSIRTs given the confidential nature of the investigations and for that reason, in certain cases we observe a one-way data flow: from CSIRTs to LE. This also depends a lot on the CSIRT national mandate and setup.

Another problem is the remediation-investigation dichotomy which impedes information sharing. LE have a specific proven legal framework to share intelligence with LE in other Member

States. Sharing with another community outside the LE field poses two challenges, one operational and one legal.

On the operational side, sharing investigation information can impede or even jeopardise the identification of perpetrators. Also, LE tend to avoid disclosing information by fear of compromising several months or years of work. An LE agency could share an IOC of an IP address of a C² server. However, intelligence sharing may generate a takedown by a CSIRT partner, while LE intended to seize or intercept the C² server. From a legal standpoint, the prosecutor decides whether to communicate, or not, any case-related information. Therefore, before sharing data, LE need to explain the necessity and seek prosecutor's permission first.

4.1.2.3 Practices and procedures: sharing the same organisational procedures

Sharing common organisational procedures may still be a challenge as each community has been established to meet its specific mission's objectives while respecting a set of different rules.

4.1.2.4 Degree of procedures' formalisation

CSIRTs, being relatively new organisations, have yet to crystallise their working methods in a way that aligns with the scientific and forensics method applied in LE which is over a century and a half old. While LE's work is considerably formalised due to legal requirements, forensic cybercrime investigation procedures have overall not reached the same level of detail within the CSIRT community. Remediation takes place within the (usually) controlled environment of a constituency's system. CSIRT have developed a fairly good grip on it and can take stances on almost all aspects of this environment. On the contrary, not all steps of a specific LE investigation process can be anticipated, as the process has to address the human factors that are related to each victim and each perpetrator and may significantly affect the handling of a cybercrime case. The most challenging part would be to analyse the victim's device, detect and collect the IOCs.

4.1.2.5 Incident report protocol

CSIRT may face challenges when reporting incidents to preserve partners' trust. CSIRT usually do not have a formalised process to report incidents to LE but have very good and documented ways for incident reports collection.
LE are notified through victims' complaints instead of incident reports. The key challenge for the investigation is unknown incidents. Even if no complaint is lodged, once an incident is detected, an investigation could be initiated; in some MS jurisdictions, LE may be required ex officio to launch the procedure, regardless of the victim's interest in pursuing an investigation that may go on for years. This can be a challenge for LE units being overwhelmed by cases of compromised IP addresses.

4.1.2.6 How to improve the performance of national CSIRTs in terms of procedural compliance

Effective supervision of the national CSIRTs' constituency should also include a check on the training of their staff regarding the collection of e-evidence to be used in a criminal trial.

When using procedural tools for evidence collection purposes, CSIRTs have to comply with the requirements mandated by LE. In order for the evidence obtained to be admissible in court, the procedural rules defined in the code of criminal procedure must be followed. However, CSIRT staff usually do not have a legal or in-house expertise or experience with criminal investigations, so compliance management issues are challenging for them.

For this reason, it is advisable, on the one hand, to provide CSIRTs with relevant information on how to proceed in accordance with the law and, on the other hand, for CSIRTs to be supervised when they are performing the requested activities.

The transmission of information can take various forms; in some countries, CSIRTs and LE carry out joint workshops, conferences or other regular meetings where information and experience are being shared. A very effective tool is the implementation of joint exercises, where law enforcement authorities verify their ability to cooperate effectively with CSIRTs, and CSIRTs in turn verify their ability to comply with requests received from LE.

For the purposes of supporting CSIRT operations, in some countries, LE liaison officers are appointed to work closely with CSIRTs as consultants, to provide advice on how to act in accordance with the law and how to cooperate effectively with law enforcement authorities. This mechanism can also work vice versa; a CSIRT representative may also play the role of a liaison officer and get involved in activities of law enforcement authorities and provide them with information on how to work effectively with CISRTs.

4.1.2.7 How to ensure compliance with judiciary procedures – a concern for CSIRTs

The identification of the author of an information security incident is necessary when investigating it as a crime. The author can be convicted in a criminal trial only if his sentence is based on valid evidence. For this reason, it is very important to collect evidence that meets the requirements for being admissible in criminal proceedings.

As explained in section 4.1.1.5, some of the actions taken by CSIRTs when dealing with an incident may render the digital evidence inadmissible. Such evidence cannot be used in court and it is therefore worthless for criminal proceedings. Hence, CSIRT team members should be familiar with the procedures of preserving and securing admissible evidence for criminal proceedings and be encouraged to implement such procedures in practice.

In order to avoid to destroy evidence and potentially interact or even compromise further LE investigation, CSIRT should aim to align their incident response and especially remediation procedures with LE and judiciary procedures and requirements.

Moreover, there is a certain complementarity between CSIRT, LE and the judiciary responsibilities and attributions, but the success of a cybercrime investigation might depend on how well their procedures and processes are adapted to each other and integrated to form a national/European framework.

One possible solution is for the CSIRTs to have accredited experts that could handle and examine evidence and even testify in court. However, this depends on the national legislation. Furthermore, it would be necessary for CSIRTs to receive specific legal training in the field of evidence collection, best practices, and criminal trials. An optimal measure would be to implement evidence collection standards along with LE and the judiciary to preserve the integrity of further investigations.

4.1.2.8 Does compliance with judiciary procedures need to be audited?

Depending on the legal framework, procedures may be questioned during a trial to guarantee the admissibility of evidence.

To be admissible in court, each piece of evidence must meet several admissibility requirements. These requirement vary depending on the national legal framework. For

instance, honeypots ([11]) that are deployed to better identify attackers' techniques used in cybercrime cases create challenges in terms of evidence admissibility. In some Member States, the use of a honeypot is considered incitement, rendering thus the evidence collected inadmissible in court. In other Member States, where the legal framework has different principles, this method is considered admissible.

If CSIRTs are asked to testify in court, their evidence collection methodology is likely to be questioned by the judges, the prosecution and/or the defence attorneys.

An evaluation and feedback exchange should follow between the judiciary and CSIRT constituency; in every cybercrime cooperation case, the judiciary should provide feedback on evidence provided by CSIRTs and may issue recommendations for further improvement.

In addition, a typical audit conducted by the judiciary should also examine the written CSIRT standard operational procedures to assess whether adequate measures are applied for evidence collection.

4.1.3 Training needs

4.1.3.1 Policy initiatives to promote cooperation across the three communities

Since the adoption of the EU Cybersecurity Strategy in 2013 (EU Commission, 2013), the European Commission has made great efforts to ensure the online protection of European citizens, companies and institutions. The EU has supported cooperation as part of the EU Cybersecurity Strategy. Currently, the Commission has added cybersecurity to its core policy priorities. ENISA has a fundamental role in developing policy initiatives to promote cooperation across CSIRTs, LE, and the judiciary. The cooperation across the three communities could also be enhanced by providing training.

4.1.3.2 How to overcome the skills gap across CSIRTs, LE and judiciary

Each stakeholder, i.e. CSIRT, LE and the judiciary, has a very specific skillset. A skills gap presents obstacles to cooperation as there is no common understanding and also creates difficulties in perceiving all necessary information. To overcome this challenge, the gap could be addressed through joint training. In particular:

- **CSIRTs** can provide technical training. CSIRTs have developed technical skills and can deliver to the other communities investigation-oriented technical training, e.g. on network investigations, and advanced systems.
- **LE** can provide legal and investigation training. Usually, this is a field in which CSIRT staff, lacking a legal background, have more limited knowledge. International LE cooperation is a distinct field, based on specific international legal instruments and requires operational experience in order to be mastered. LE usually provide to the judiciary, training on the cyber investigation field more than technical training. The key is not to explain how to analyse, for example, a log file, but to provide magistrates with an understanding of cyber-attack mechanics, cybercriminals' modus operandi and legal implications of any coercive action taken. These training sessions should provide magistrates with technical knowledge and give them strategic investigation directions.
- **Judiciary** can provide both CSIRT and LE with legal training. In particular, they should focus on the exclusionary rules of evidence. Representatives of the judiciary can provide the other two communities with detailed information on the legal rules

([11]) A honeypot is a system left opened on the internet with vulnerabilities known by its owner, with the intention of attracting hackers and thus collecting information.

applicable to criminal proceedings, the handling of electronic evidence, the evaluation and admissibility of evidence, and the procedures for reporting a crime. Similarly, they can provide information guidelines derived from practice and case law on how electronic evidence should be handled properly or how it should be presented and evaluated in court. On the other hand, judges and public prosecutors, via technical training, might increase their technical knowledge needed to understand some of the specificities of cybercrime such as the nature and weight of certain types of electronic evidence.

These cross-training efforts between CSIRTs and LE are very good opportunities for sharing and building a common cultural ground.

TF-CSIRT and FIRST material are a good starting point for LE to understand the CSIRT's world. ENISA has also published material (ENISA, 2019) covering a broad set of technical topics, including a recent course on Digital Forensics (ENISA, 2019a).

Other training initiatives in this field originate for instance from joint initiatives of the European Union and the Council of Europe (see e.g. GLACY ([12]) and GLACY+ projects ([13])) and from UNODC (see e.g. University Module Series on Cybercrime (UNODC, n.d.) in which there are modules specifically focused on cooperation.

4.1.3.3 Prototype organisational behaviour

Organisational behaviour aims at answering several questions impeding cooperation. The following questions and possible answers provide some guidance for improving cooperation.

- How to avoid duplicated efforts?
  - (a) Communicate once the incident handling has initiated
  - (b) Send observers on site
  - (c) It is necessary to trust others.

- To achieve this, however, it is necessary for CSIRTs to acquire more legal knowledge about e-evidence:
  - (a) Use segregation of duties matrix
  - (b) Come up with policies or rules on when and how to cooperate
  - (c) Conduct training

- How to handle incidents in order to prevent evidence loss or alteration?
  - (a) Design and implement a common standard for data collection
  - (b) Implement taxonomies
  - (c) Define best practices for most common types of incidents
  - (d) Develop practical guides
  - (e) Receive joint training
  - (f) Provide legal training

- How to efficiently share intelligence?
  - (a) By using MISP
  - (b) By using common taxonomy
  - (c) By having English language skills allowing CSIRTs, LEs and the judiciary to communicate easily
  - (d) By holding regular meetings and building trust

([12]) https://www.coe.int/en/web/cybercrime/glacy
([13]) https://www.coe.int/en/web/cybercrime/glacyplus

- How to efficiently mutually provide expertise and tools:
    (a) Through joint training
    (b) By maintaining some basic communication tools

4.1.3.4 Case study – Czech Republic

The Czech Republic's strong focus on cybersecurity led to the adoption of the Cyber Security Act (Czech Republic, 2014) and showed that one of the fundamental challenges for successful protection and defence of national cyberspace is the ability of the competent public and private institutions to cooperate against the rise of cybersecurity incidents. An appropriate way to strengthen this cooperation is to implement joint exercises to verify and develop the technical, legal and organisational capabilities of competent institutions and personnel. Cyber exercises seem to be a great opportunity to get technically skilled professionals, government representatives and other stakeholders to interact, confront each other and exchange their different perspectives on and approaches to problem solving.

Exercises conducted in the Czech Republic are organised by the National Cyber and Information Security Authority (NCISA), a central body of state administration for cybersecurity, operating government CERT. Its constituency includes systems of critical information infrastructure, important information systems and operators of essential services. Exercises organised by NCISA are of two types – technical, primarily focused on testing the technical readiness of security engineers, CSIRT members and other ICT experts of relevant institutions; and non-technical, table-top exercises that focus on organisational readiness and cooperation capability.

The Cyber Czech technical exercise has been developed and implemented every year since 2015 in cooperation with Masaryk University, using the infrastructure of the cyber range KYPO (KYPO by CSIRT MU, n.d.) developed by Masaryk University as a part of their security research. The exercise is based on the Red team–Blue team principle, with the red team consisting of cybersecurity experts from governmental CERT, Masaryk University and other partner institutions. During the exercise the red team launches cyber-attacks on infrastructures managed by the Blue team, and the Blue team's task is to protect their critical systems from these attacks.

However, this technical exercise also includes an organisational and legal component as it also simulates the role of the police, the DPA, regular internet users and journalists. Besides defending their network, and communicating with regular users and media, Blue team members must also be able for instance to detect whether an offence has been committed, know how to identify it and report it to the police, and how to respond to requests for operational information or evidence. In some runs of this exercise actual investigators from the National Centre for Combatting Organized Crime, responsible for investigating serious cybercrimes, are also involved.

While technical exercises are designed for practicing primarily technical skills and capabilities, NCISA also organises discussion-based, table-top exercises that are used for testing procedures, crisis management processes, institutional arrangements and agreements. A specific exercise of this type was also organised with a focus on cooperation between CSIRTs and the LE; in particular the focus of this exercise was to investigate the processes related to the investigation of the incident and the initiation of criminal proceedings, coordination, cooperation and information sharing between communities (LE, CSIRTs, other security entities and victims) and cross-border cooperation capabilities. As part of this exercise, participants are provided with the scenario and are required to decide, in their capacity, what actions to take in order to mitigate and investigate the incident. The team of organisers then moderates possible discussions, mediates the transfer of information and informs team members about new

developments in scenarios and assigned tasks. The aim then is for both communities to understand how the incident is approached from a different perspective, to recognise the implications of the security team's incident handling activities in the context of criminal proceedings, to identify white spots in cooperation and coordination during incident management, investigation, and beyond.

Both types of exercises proved to be a suitable tool for enhancing the understanding of the mutual roles of individual communities in managing cybersecurity incidents, for sharing experience with incident management and cybercrime investigations and for identifying and setting up appropriate procedures and tools for mutual cooperation and coordination.

4.2 TECHNICAL ASPECTS

4.2.1 Use of (common) tools to facilitate cooperation and interaction

One of the key recommendations of the 2018 ENISA report was the use of common tools in order to facilitate cooperation and interaction across the three communities. Based on the data collected through the interviews the most common used tool remains email but there is a recent tendency to adopt Pretty Good Privacy (PGP)[14] protocol for encryption of the communication and MISP for threat intelligence sharing.

While CSIRTs have started to offer technical support to LE for adopting MISP, some MSs are already using or building national tools for instant messaging communication and information sharing. In the last case, LE are usually included by default while CSIRTs may also be invited depending on their role in the national setup (usually national and/or governmental CSIRTs).

- **Common IT network**

  Analysis of the data collected through the interviews conducted showed that segregated networks were another obstacle to cooperation. This creates day-to-day difficulties that hinder LE and CSIRT staff cooperation and delay any exchange due to the laborious procedures. When possible, sharing a common IT infrastructure is a first and mandatory step to enhance the cooperation.

- **MISP**

  Malware information sharing platform (MISP) ([15]) is an application designed by Luxembourg CSIRT (Computer Incident Response Centre Luxembourg – CIRCL). It was designed to store and exchange information on indicators of compromise. Being an open-source software tool and heavily supported both by CIRCL and the community, it has been considered to be a standard tool in the cybersecurity field. MISP is an efficient way to store data and unique for its sharing factions.

  MISP is widely used around the world, with 6 000 instances being already deployed (MISP Project, n.d.).

  MISP facilitates cooperation between CSIRT and LE. For instance, it is used by Luxembourg to share IOCs (indicators of compromise) between Luxembourg CSIRT, and other partner agencies, especially LE.

- **Instant messaging**

  Instant messaging tool is essential as it facilitates immediate communication. It provides quick and direct message exchange which is very crucial during the cybercrime investigation phase.

([14]) https://www.openpgp.org/
([15]) https://www.circl.lu/services/misp-malware-information-sharing-platform/

- **Encryption**

  PGP is the most commonly used method for encryption of communication across the communities; it is an open source solution internationally recognised as a secure protocol. PGP has already been adopted by most of the CSIRT teams in Europe, including national and governmental ones. Moreover, some of the CSIRTs have started to use it in their communication with LE counterparts.

- **File sharing system**

  File sharing is another essential tool to be included in the CSIRT-LE cooperation toolset. Part of the technical cooperation is also the regular file exchange. To do this, setting up a secure and user-friendly environment is fundamental in order to:
  - facilitate cooperation;
  - avoid shadow IT, where personnel relies on inappropriate ways to perform the required tasks (clouds, third-party holstering application/infrastructure, etc.).

- **Coordination platform**

  In case of major cyber crisis, CSIRTs and LE should strongly cooperate. This can easily be achieved only if some tools for supporting their technical cooperation have already been set up.

4.2.2 Tools and their key functionalities

Each community uses tools for their day-to-day activities. By using the same toolset, CSIRTs, LE and the judiciary could further enhance their cooperation. Such tools are needed for: information sharing, evidence collection, coordination and secure communications.

- **Information sharing**

  The use of information-sharing tools is dependent on the organisation's culture: while CSIRT are familiar with these tools, LE seem usually to rely on the most commonly used (i.e. email, file sharing, Europol mailing system SIENA (16)). Information-sharing tools usually include:
  - A database system for storing information;
  - One or several taxonomies;
  - A sharing system, either centralised or peer-to-peer.

  More advanced tools can provide other functionalities, such as:
  - Data visualisation (charts, graphs);
  - Data quality assessment;
  - Data management system (based on categories of data or other criteria).

- **Evidence collection**

  The tools used by CSIRTs and LE for evidence collection vary. While LE tend to use commercial tools (e.g. EnCase ([17]), FTK ([18]), etc.) and specific hardware (e.g. write blockers used to avoid any writing on a drive while copying it to avoid tampering), CSIRTs are more familiarised with open source and free available tools (DD ([19]), Clonezilla ([20]), DumpIT ([21]), etc.). Moreover, LE are more focused on legally sound data collection while CSIRTs look for technical accuracy.

([16]) https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena
([17]) https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r
([18]) https://accessdata.com/products-services/forensic-toolkit-ftk
([19]) https://www.linuxjournal.com/article/1320
([20]) https://clonezilla.org
([21]) https://blog.comae.io/your-favorite-memory-toolkit-is-back-f97072d33d5c

- **Coordination**

  While some of the already existing and used tools (e.g. MISP, email, instant messaging) can be used for coordination between communities, the need for automation in terms of quickly marking certain types of resources as being under investigation has been highlighted (e.g. national CSIRT to be able to quickly crosscheck if certain IPs or URLs are investigated by LE, and if so, to avoid any interference with that investigation).

- **Secure communication**

  Secure communication is provided through exchange of encrypted emails or messages. GPG is widely used for encryption and it is supported by several mail service providers. Military affiliated agencies may use other encryption algorithms.

  Instant messaging applications like Mattermost (Mattermost, n.d.) allow encryption too. But what is of great importance is for each organisation to select and use tools fitting into its ecosystem and its partnerships.

4.2.3 How the investigations are carried out – forensic methods?

Based on the replies received from the interviews and the online survey results, cybercrime investigations are carried out by using the following forensic methods:

- **Computer forensics:**

  The main purpose of an evidence collection tool is to allow the user to extract information from a system without modifying it. To do this, the main device to use is a write blocker ([22]). LE operate easy-to-use forensic tools such as EnCase ([23]) or X-Ways ([24]).

  These tools allow staff with basic forensics knowledge to efficiently conduct investigations. Another advantage is that these tools are usually very efficient to handle and display a lot of items simultaneously. This feature is necessary when going through several hundred thousands of files.

- **Network forensics:**

  Network forensics are executed to find traces of suspicious activity or previously flagged items (IOCs). A tool that is widely used for this purpose is Wireshark (25); it allows its users to search through all protocols for pieces of data.

  Interception/sniffing in pcap can generate huge volumes of data that can be analysed with Moloch (26).

  Netflow data is smaller in size (and can be sampled); DNS logs are text and manageable in size; Netflow and DNS logs are most often not analysed within Moloch but separately (nfdump, ELK, manually).

([22]) This tool is placed between the analysing computer and the target device. Write blocker blocks all write commands, making sure the target is not altered.
([23]) https://www.guidancesoftware.com/encase-forensic
([24]) https://www.x-ways.net
([25]) https://www.wireshark.org
([26]) https://molo.ch

- **Mobile devices forensics:**

  Mobile devices forensics refer to the tools and technologies of digital forensics utilised for the recovery of evidence from a mobile device; multiple methods have been developed to address evidence collection from a variety of mobile devices. For instance, Jtag (27) mobile forensics rely on jtag connection analysis for artefacts recovery; while 'Chip off' (28) is a technique that implies chip removal and analysis of chip data.

- **Memory forensics:**

  Live memory acquisition can be a challenge from an organisational perspective. What is needed is qualified personnel, having the appropriate skills and the right tools for acquisition. However, it is hard to collect evidence when a network or a hard drive are encrypted; memory becomes one of the last place where evidence can be found.

  The main tool for memory forensics is Volatility (29). It loads numerous plugins for finding malware and has become a standard. It is an open source tool that requires training to use it.

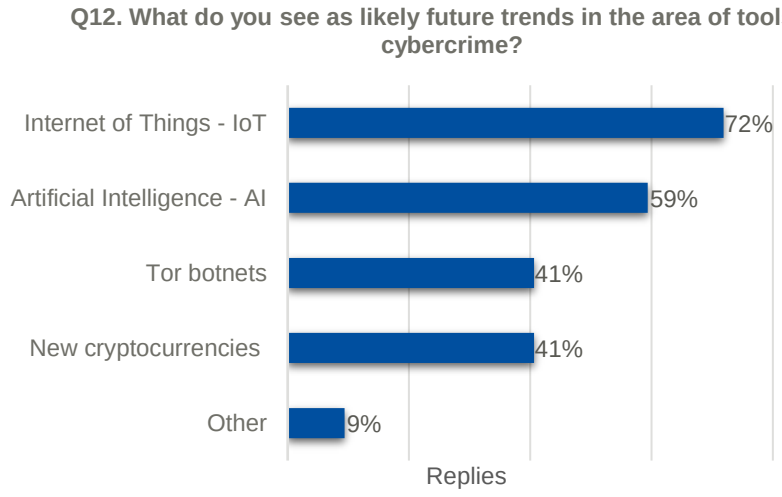
- **Live forensics:**

  Sometimes the data acquisition must be done while the device is powered on. A common use case is with VPS providers that are running multiple VMs or containers on the same physical server; in this case, the data collection needs to be done without powering down the physical server. Acquisition of containers (Docker (30)) is just an indicative example.

4.2.4 Future technology and cybercrime attribution (Carrier Grade NAT (CGN), AI, IoT)

Although future technologies seem to create challenges for the investigation teams, they could also provide cooperation opportunities. Figure 12 shows how the respondents to the online survey replied to the question on likely future trends in the area of tools for cybercrime.

Figure 12: Replies to question 12 of the online survey



(27) https://forensicswiki.org/wiki/JTAG_Forensics
(28) https://www.digitalforensics.com/blog/chip-off-technique-in-mobile-forensics
(29) https://www.volatilityfoundation.org
(30) https://www.docker.com

4.2.4.1 IoT

IoT use will create challenges when investigating a cybercrime as applications are based on proprietary codes and infrastructures. Although IoT devices also contain some private data, such as connection data, sometimes those have to be analysed for investigation purposes. They usually use specific technologies, both software and hardware. An example of investigation is the Mirai case (Krebs, 2019). A Mirai botnet used CCTV devices to launch DDoS against DNS service. Analysis of CCTV allowed the perpetrator to be identified.

4.2.4.2 Artificial intelligence

AI could be used by a cybercriminal for vulnerability scanning. IPs are scanned for any fingerprint they may provide. AI could deduce from appropriate datasets information not only for an attack vector, but also for the kind of internal vulnerabilities that could potentially be exploited for moving laterally in the system. AI tools could also enable an attacker to optimise botnet resources, for example to have DDoS attacks switching between machines, making detection and mitigation more difficult. Botnets are currently layered through to avoid detection. One usual setup is to have one layer of a peer-to-peer network of zombie-machines and above that several layers that transmit instructions and channel stolen information to the attackers' last node.

Nevertheless, AI technologies could be utilised to counter cybercrime attacks as well. For instance, improve botnet management by using AI tools to detect patterns and anticipate attacks based on identified vulnerabilities.

4.2.4.3 Publicly available mass market encryption

Latest developments, projects and initiatives from the open source community, researchers, but also from big technology companies are pushing for the availability of strong encryption products for end users, including end-to-end encryption.

Mylar project is one example of a practical system that can compute on encrypted data (Popa R.A., 2016). This system might be used by LE to query encrypted databases or capture traffic for specific words or strings and results without decrypting the content.

4.2.4.4 Carrier Grid NAT

On the internet, every connected device needs an IP address. However, the number of IP addresses (Internet Protocol Version 4) is limited and insufficient to meet the exploding demand for new addresses for connected devices including connected objects and smart phones. A new version of IP address (IPv6) which provides an unlimited number of IP addresses is available but the transition from IPv4 to IPv6 requires internet access providers and internet content providers (websites, social media, webmail services, etc.) to update software and hardware.

As a supposed-to-be temporary solution to address the problem of shortage of IP addresses, internet access providers adopted CGN ([31]) technologies which allow sharing of IPv4 addresses with multiple internet users (several thousands). CGN technologies are used by internet service providers to share one single IP address among multiple subscribers at the same time.

This has an impact on criminal investigations as an IP address is often the only information that can link a crime to an individual. It might mean that individuals cannot be distinguished by their IP addresses anymore, which may lead to innocent individuals being wrongly investigated by law enforcement because they share their IP address with several thousand others – potentially including criminals.

([31]) https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online

As said, this was supposed to be a temporary solution until the transition to IPv6 was completed. For some operators however it has become a substitute for the IPv6 transition. Despite IPv6 being available for more than 5 years the internet access industry increasingly uses CGN technologies (90 % for mobile internet and up to 38 % for fixed line internet access providers while 12 % were expected to deploy it in the coming months) instead of adopting the new standard (Europol, 2017).

4.2.5 Technical knowledge used by the judiciary

The judiciary need to broadly understand technical information behind investigation techniques. What is of great importance is to precisely understand what is at stake, such as private information and liberties infringements.

For example, if LE want to execute a sinkhole ([32]) of a malware, the judiciary will need to understand how this will be done and what kind of data should be collected. Depending on national laws, executing a sinkhole of a malware, may or may not be authorised, mostly for privacy and data protection reasons.

4.3 HUMAN ASPECTS ASSOCIATED WITH ORGANISATIONAL CULTURE

4.3.1 Mind-set differences

One of the differences of individual communities that may prevent or restrict cooperation and information sharing are differences in personalities or social roles. This situation may result in one community not understanding the constraints that apply to the other, or its role and mandate. Some indicative examples are presented below:

There is no common understanding of what data types can be used as evidence. For CSIRTs, any data or information related to the source of a security incident can be evidence. The way that attribution of cybercrime is being done may result in making evidence inadmissible in a trial. Sometimes CSIRTs seem not to understand that the requirements of the quality of evidence in the concept of criminal law are significantly high; evidence must be obtained according to the applicable law and handled in a specific way.

There is limited common understanding of the objectives related to the fight against cybercrime; CSIRTs aim to achieve the fastest possible mitigation of incidents and ensure the confidentiality, integrity, availability (CIA) triad of systems of their constituency. But reckless pursuit of these goals can lead, for example, to destruction of valuable evidence or even expose the monitoring activities to the attacker.

Hence, mind-set differences could hinder the cooperation at the stage of evidence collection, in case the competent CSIRT community is not appropriately prepared to address relevant scenarios as well as when there is difficulty in determining what data may constitute evidence or not. Understanding what can be used as solid, admissible evidence in a court of law is a challenge for CSIRTs. This requires time as CSIRTs would need to receive training on what kind of elements they should look for when collecting evidence. Indeed LE and CSIRTs usually operate under different time-frames. LE officers are emergency specialists who work in legal-based timeframes, such as for example temporary detention, which are generally too short for exhaustive analysis. On the contrary, CSIRTs often deal with espionage cases and are trained to lead a thorough and exhaustive analysis.

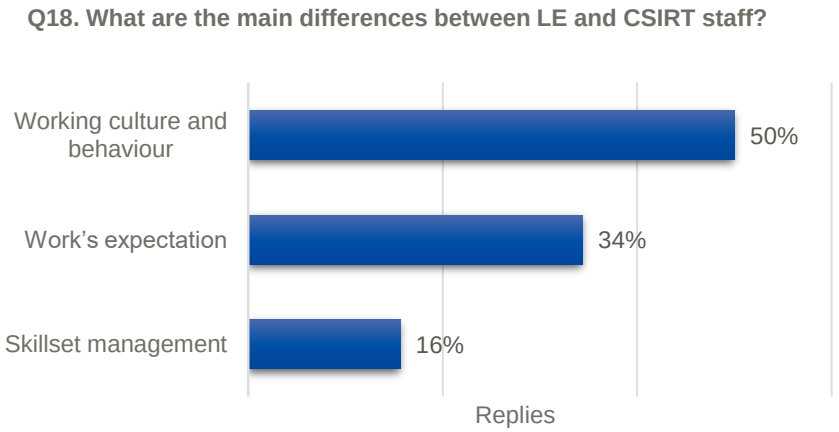
([32]) Operation consisting of buying a domain name used by a malware to transmit stolen data. The interest for LE is to identify victims.

Ultimately, these communities bear a different perspective. LE operate under an offence- based system. In an optimal scenario of a cybercrime case, the case is closed, with the perpetrators identified and brought to justice. CSIRTs are accustomed to handling intelligence, collecting, storing and then analysing the relevant data. Legal constraints may arise when processing personal data and this could impact the progress of the investigation. Lastly, the judiciary has mainly a legal perspective and often lacks a technical background or knowledge. The objective of the judiciary is to determine whether the suspect is the offender and proceed to the conviction in accordance with the law and while respecting the fundamental rights of the suspect.

4.3.2 Assessing personnel skills and qualities

Assessing personnel skills and qualities for each community will be a necessary step to enhance their cooperation. Each community has its own professional context, motivations and constraints.

Figure 13: Replies to question 18 of the online survey



Differences between the communities are observed in multiple levels. More particularly, provided the nature of the respective community, work expectations vary, with LE prioritising achieving higher ranking and being recognised as experts who have more time to practice. While CSIRTs identify as their work expectations the improvement of skills or the development of multiple skills. Secondly, relating to the upkeep of their skills and their training necessities, some LE noted that there are few in-house training possibilities available and an inadequate budget for that purpose. In contrast, some CSIRTs indicated that there are many internal resources and usually adequate budget for that purpose. Both communities agreed that training courses must be carried out by truly competent people. Referring to personal KPIs, LE identified as such the number of cases handled and the reaction time. The number of cases handled is also a personal KPI for CSIRTs, in addition to their skillset. Finally, when examining the impact on cooperation, the communities determined that the difficulties are due to the technical level discrepancies and the CSRITs' lack of legal knowledge.

4.3.3 Competency-based framework

Some countries have concluded that a systematic approach is needed to effectively build a human workforce basis capable of addressing cybersecurity challenges. This is the reason why some countries are developing competency frameworks that specify what type of employees are needed in the cybersecurity field, what qualifications these employees should have, what training programmes, exercises and materials to acquire such qualifications are available and how to cover any identified gaps.

An example of such a framework is the US NICE framework (National Institute of Standards and Technology, 2017) ([33]), which includes a taxonomy of qualifications. For each qualification, is then identified what kinds of competences, skills and knowledge are required.

Such a framework can be used in several ways. On this basis, scales for assessing the competencies of applicants for individual positions in cybersecurity could be defined. This framework could also be used to analyse the current state of the labour market, assessing what qualifications are missing from cybersecurity professionals. Another use could be to present the availability of courses, training programmes and other education and training opportunities that could help applicants to be better qualified.

Outcomes of such analyses then could be used to develop policies, initiatives and regulation focused on promoting cybersecurity education and building a cyber-workforce.

4.4 LEGAL AND POLICY ASPECTS

4.4.1 Legal framework in EU

The legal framework establishes and shapes the process of cooperation between CSIRTs and LE as well as their interaction with the judiciary in the context of fighting against cybercrime. Information on the legal and policy framework can also be found in the 2017 and 2018 ENISA reports on CSIRTs and LE cooperation (ENISA, 2017a), (ENISA, 2018).

The legal framework in this area is presented at three levels: international level, EU level, national level.

4.4.1.1 International level

The first and the most relevant international treaty on cybercrime and electronic evidence is the Council of Europe Convention on Cybercrime ((Council of Europe, 2001) ([34])). This convention is also called the ‘Budapest Convention’. On the one hand, this aims at providing guidelines for any country for the development of a comprehensive national legislation against cybercrime. On the other hand, this convention is a framework for international cooperation between the signatory states. The Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Council of Europe, 2003) complements the Budapest Convention. The Cybercrime Convention Committee (T-CY) is also preparing a draft version of the 2nd Additional Protocol (Council of Europe, 2019) to the Convention on Cybercrime (Council of Europe, 2001) to submit to the Committee of Ministers in the light of its adoption. This draft and an Explanatory Report is expected to be finalised by December 2019 ([35]). The 2nd Additional Protocol is ‘designed to provide solutions for a more efficient criminal justice response to cybercrime and other crime involving electronic evidence in accordance with data protection and other safeguards’ (Council of Europe, 2019, p. 4).

([33]) https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
([34]) https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185
([35]) The 2nd Additional Protocol is prepared taking into account among others: Article 46.1.c Budapest Convention on Cybercrime; the decision adopted by the Cybercrime Convention Committee (T-CY) at its 17th Plenary (June 2017); Parliamentary Assembly Recommendation 2077 (2015) on ‘Increasing cooperation against cyberterrorism and other large-scale attacks on the Internet’ and the response of the Committee of Ministers of 27 April 2016; the Programme and Budget of the Council of Europe for 2016/2017 as adopted by the Committee of Ministers on 24/25 November 2015 referring to follow up to be given to the work of the TCY on access to evidence in the cloud; agreement in principle by the TCY at its 16th Plenary (November 2016) on the need for an additional Protocol, and drawing from the Final Report and Recommendations of the T-CY Cloud Evidence Group and, in particular section 4.5 with possible elements of a Protocol.

4.4.1.2 EU level

The European Union can legislate through several types of legal acts. The acts that the European Union can issue are the following:

(a) **Regulations**. A regulation is a binding legislative act which must be applied in its entirety throughout the EU, without exception.

(b) **Directives**. A directive is a legislative act that establishes a common goal that must be achieved by all EU countries. However, it is the prerogative of each Member State to define its own laws aimed at achieving these objectives.

(c) **Decisions**. A decision is a directly applicable legal instrument which is binding upon those individuals to which it is addressed (the individual can be e.g. an EU country or an individual company).

(d) **Recommendations**. A 'recommendation' allows the EU institutions to publish their views and suggest guidelines without, however, imposing any legal obligation on those to whom it is addressed. Clearly, a recommendation is not binding.

(e) **Opinions**. An 'opinion' is a legal instrument that allows EU institutions to make a non-binding statement.

4.4.1.3 National level

This level concerns the rules issued by various Member States. The international and European legal frameworks are a reference point for national legal frameworks. Nevertheless, it is sometimes possible to find different legal frameworks in various Member States. This diversity has consequences for the cooperation between CSIRTs and LE and their interaction with the judiciary.

4.4.1.4 Differences in legal systems and evidence admissibility

In a criminal trial, it is important that e-evidence is integral and qualitatively reliable. To achieve this result, data integrity must be ensured in all the life stages of e-evidence management, namely: identification, collection, acquisition and preservation. In particular, as stated by Mitrakas and Zaich 'The chain of custody through appropriate policy frameworks can be used in order to assess the quality of the collected data. Chain of custody investigations may also help in establishing the hierarchical structure that prevailed at the time that the acts under investigations were committed' (Mitrakas, 2009, p. 164 and 173). Depending on the Member State, the verification of the chain of custody can have different legal consequences. In some Member States, this verification is relevant only for the purposes of evaluation of evidence. In other Member States for the admissibility of evidence. The grounds of inadmissibility of evidence are defined by the national laws of each Member State. Each piece of evidence has to be legally obtained, according to the competent jurisdiction.

The national judicial systems are characterised by differences that could also have an impact on the cooperation and interaction across CSIRTs, LE and the judiciary. The judicial systems could be categorised into: common law systems and civil law systems.

(a) The judicial systems of common law are also called adversarial systems (or adversary systems). In such a system, a criminal trial is conceived as a conflict or dispute, where each of the parties supports a contrary position. The oral evidence is of fundamental importance; such evidence is acquired by means of the so-called cross-examination. The judicial precedent is very important in a common law system. This means that a decision of a court can be used as a source for future decisions, also known as precedents; precedents are authoritative and binding and must be followed. This is the principle of *stare decisis* ('let the decision stand').

(b) The civil law systems are non-adversarial systems. The judge sometimes has a more active role in the collection of evidence and can also interview the witnesses by himself. The principle of *stare decisis* does not apply to this case.

From a juridical point of view, the 'nature' of e-evidence may create issues regarding its admissibility in a criminal trial. For this reason, in some Member States there are specific requirements regarding the collection of e-evidence in order to be admissible in courts. In addition, related research and evaluation carried out by the Council of the European Union on the prevention and combating of cybercrime has concluded 'that in most Member States, procedural laws are technology-neutral, which means that general rules and principles on gathering of evidence are applied and that procedural systems do not contain any formal rules on admissibility and assessment of e-evidence' (Council of the European Union, 2017, p. 11) . More information about the topic of e-evidence in court can be found also in the 2018 ENISA report on CSIRT and LE cooperation (ENISA, 2018).

4.4.1.5 Discrepancies

Although meaningful progress has been made at European level to strengthen the cooperation and interaction across CSIRT, LE and the judiciary, discrepancies which may partly hinder this progress, still remain.

It is important to point out that there are significant differences in purpose of responding to information security incidents between CSIRTs and LE investigators. A CSIRT aims to mitigate an incident, which may also be a crime, as soon as possible and restrict the negative impact it may have. When performing such tasks, a CSIRT is often not adequately concerned about preserving the evidence that could be used to identify the author of the incident. On the contrary, an LE investigator aims to identify the author of this incident, which is determined to be a crime, for the purpose of prosecuting the criminal offences. For this reason, it is very important for LE investigators that CSIRTs do not to delete evidence, but preserve it properly ([36]).

In addition to that, fundamental differences in each entity's posture and structure, both within and between them, may further impede cooperation and interaction among CSIRT, LE and the judiciary. For example, as some interviews have shown, the hierarchical structure of LE and the judiciary may cause delay in cooperation, especially with the CSIRTs of other Member States. Moreover, disconnection may also result from the different mind-sets these entities have.

At national as well as at European level, there are a plurality of non-legislative acts (memoranda, public–public and public–private agreements, and industry standards) concerning CSIRT, LE and the judiciary. Such acts have often contributed to the improvement of cooperation and interaction between CSIRT, LE and the judiciary. However, the multiplicity and diversity of content of the various acts causes discrepancies between situations that are similar but regulated by different acts.

Regarding 'judicial confidentiality', Member States' legislation often differs. Consequently, the types and categories of information that can be shared can vary from one Member State to another.

4.4.1.6 Jurisdiction issues

- **EU law defining only framework**
  Since cybercrimes do not stop at the borders of Member States and may concern various Member States, what is often observed is authorities of several Member

([36]) For more on this please see subchapter 4.3.1. on Mind-set differences.

States investigating the same crime. This fact may create conflicts of exercise of jurisdiction. At European level, Council framework decision 2009/948/JHA (EU Council, 2009) ([37]) establishes the rules for prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings.
Moreover, 'Electronic evidence has become relevant in a large majority of criminal investigations and increasingly often, judicial authorities need to make a request in another jurisdiction in order to obtain necessary evidence from service providers. Making it easier and quicker to obtain this evidence across borders is therefore of crucial importance for investigating and prosecuting crime, including terrorism or cybercrime' (EU Commission, 2018), II.1, p. 1). At present, this purpose is pursued by means of: mutual legal assistance (MLAT) instruments; European Investigation Order; and voluntary cooperation in those cases where it is legally possible.

In view of the particular needs of speed and technicality in the collection of e-evidence, the European Commission has prepared two proposals with the aim of improving the investigative cooperation between Member States. These proposals are:

- Proposal ([38]) for a regulation on European production and preservation orders for e-evidence in criminal matters (EU Commission, 2018); and
- Proposal ([39]) for a directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (EU Commission, 2018).

These legislative initiatives will address the jurisdictional issues related to cross-border cooperation/information sharing.

Some important points that still need to be addressed are:

- How quickly data useful for the investigation can be provided;
- Inability to provide certain types of data, in particular data that are subject to 'judicial confidentiality';
- Inability to provide data due to differences in data retention rules;
- Poor quality of data transmitted by CSIRTs to LE;
- Admissibility of digital evidence.

4.4.2 Admissibility of digital evidence

4.4.2.1 Categories and classification

This section presents the categorisation and classification of digital evidence:

- Categorisation of digital evidence: data stored on a device can be divided into two categories, namely volatile data and non-volatile data.

  (a) **Volatile**
  Volatile data usually refers to live memory data. When a computer is running, it loads in live memory all data needed to work. This data types are precious and sensitive for analysis for two reasons. First, all live data is unencrypted for the computer to work on it. Encrypted data such as communication application data is unencrypted in live memory.

([37]) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:328:0042:0047:EN:PDF
([38]) http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-jd-cross-border-access-to-e-evidence-production-and-preservation-orders
([39]) http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-jd-cross-border-access-to-e-evidence-appointment-of-legal-representatives

Second, live memory contains a lot of information like registry or configuration data the computer needs to run. If the attacker erased his tracks, useful data can still remain in live memory.

(b) **Non-volatile data**
Non-volatile data refers to any data that can be retrieved even after computer has been cycled on or reset. This data can usually be found either on hard drive or on USB key, SIM card, chip, or any other type of so-called 'dead storage'. These locations are where system stores all data needs to run on next start.

Among non-volatile data, deleted files are also included. When a file is deleted from a computer, it simply removes its internal reference to it in hard-drive master file table (MFT). MFT is equivalent to a map or a summary listing of all available data and their location on the drive. Unless explicitly ordered by user, data is not actually erased and can be recovered by forensic analysis.

- Types of digital evidence (based upon their source) – see also forensic methods.

- Outside data: all data not produced within the system.

(a) **Internet data**
Internet data is the data related to the internet; this data must be stored by service providers for the purposes of the prevention, investigation, detection or prosecution of criminal offences (see 4.4.1)

(b) **Malware sample**
Malware sample includes malicious files usually found on the victim's system as long as the attackers have not erased it. This file, namely **payload** operates on the system to execute illegitimate instructions, such as data theft, file encrypting, DDoS triggering. Compared to traditional crimes, it is the 'weapon' used to commit it. Investigators look for malware sample in the first place because it may contain a lot of information on culprit infrastructure and help them to identify the attacker.

- Internal data: data locally produced by the system.

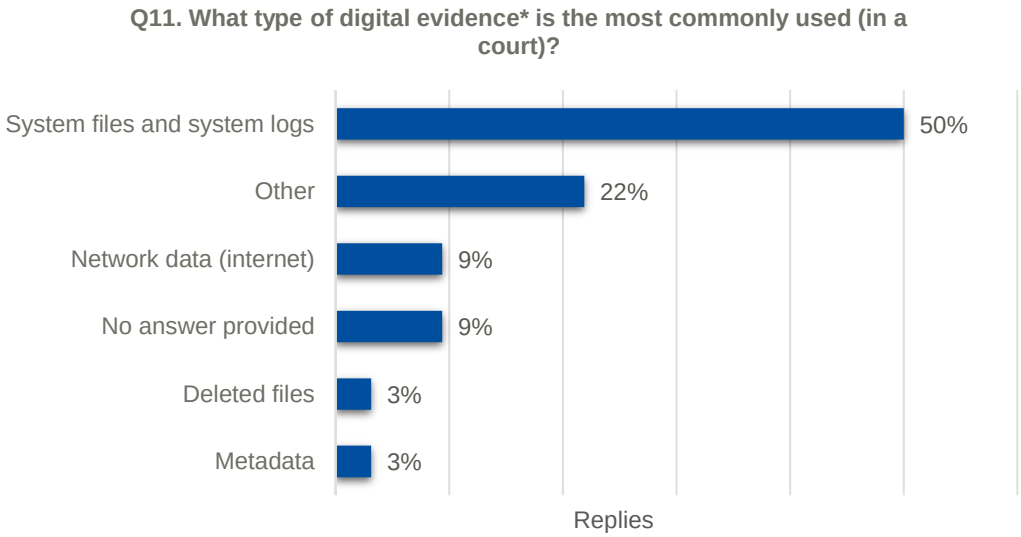
(a) **System files and system logs**
According to Article 3 No 6 Directive (EU) 2016/680 (EU Council, 2016b) and Article 4 No 6 Regulation (EU) 2016/679) (EU Council, 2016), 'Filing system' is defined as any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. The logs contain a record of the operating system (OS) events, being system logs, user logs or application logs. Consequently, logs can be very useful for investigation purposes because they provide data related to processes executed on the computer at the time of the attack. In system logs, tampering, fraudulent operation and any illegitimate action will appear, unless attackers manage to erase them.

(b) **Internal network data**
Internal network data such as net flow, DNS data and pcap files are data transiting into the system. Numerous pieces of evidence can be collected from these data types as activities run on a computer have been logged, e.g.: when malware tried to communicate with their servers for stolen data recovery, when

a hacker pivoted from one machine to another, and any other hacker's operation into the system.

Figure 14 presents the various types of digital evidence most commonly used in a court of law, based upon their source (volatile and non-volatile data). System files and system logs are the data types most commonly used, as indicated by 50 % of the online survey respondents.

Figure 14 – Replies to question 11 of the online survey



* Types of digital evidence based upon their source - volatile and non-volatile.

4.4.2.2 ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence

The International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) have proposed international standards for evidence gathering. In particular, a careful chain of custody is strongly recommended.

Although the ISO/IEC recommendations are not legally binding, there are common standards that should be observed by investigators all around the world in order to allow an effective circulation of criminal evidence between the countries.

Several ISO/IEC recommendations can have an impact on a criminal trial. Among these ISO recommendations, ISO/IEC 27037:2012 appears particularly important because it provides specific rules on digital evidence for the various phases concerning e-evidence, namely identification, collection, acquisition and preservation.

Such rules are provided for various devices such as:

- Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions; digital still cameras and video cameras (including CCTV); electronic devices (PEDs), memory cards; mobile phones, personal digital assistants (PDAs), personal mobile navigation systems, standard computer with network connections, networks based on TCP/IP and other digital protocols, and devices with similar functions as above.

ISO/IEC standards that could be used during the cybercrime investigation phase are presented in the following table.

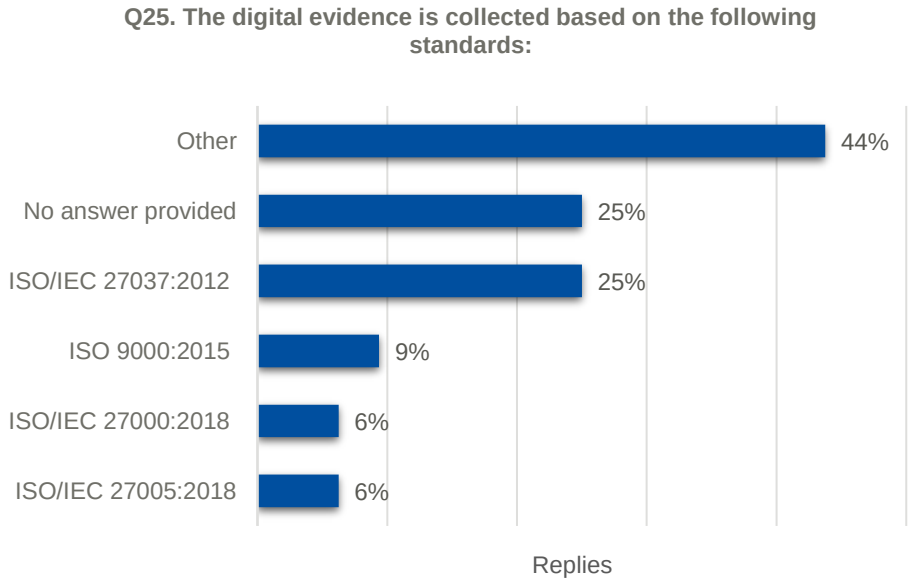
Table 2: ISO/IEC standards for the cybercrime investigation phase

ISO/IEC standard	Title
ISO/IEC 27050-2:2018	Information technology – Electronic discovery – Part 2: Guidance for governance and management of electronic discovery
ISO/IEC 27050-3:2017	Information technology – Security techniques – Electronic discovery – Part 3: Code of practice for electronic discovery
ISO: 27050-1:2016	Information technology – Security techniques – Electronic discovery – Part 1: Overview and concepts
ISO/IEC 30121:2015	Information technology – Governance of digital forensic risk framework
ISO/IEC 27043:2015	Information technology – Security techniques – Incident investigation principles and processes
ISO/IEC 27042:2015	Information technology – Security techniques – Guidelines for the analysis and Interpretation of digital evidence
ISO/IEC 27041:2015	Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method
ISO/IEC 17020:2012	Conformity assessment – Requirements for the operation of various types of bodies performing inspection

Figure 15 depicts the free-text replies provided in the online survey (Question 25). Some of the respondents replied that:

- No ISO standards are followed during the evidence collection; digital evidence is collected based on the framework defined by national laws. Any method or tool (like FTK, EnCase), scientifically documented, can also be accepted.
- Internal national manual based on the parameters that are set in different standards are used for evidence collection.
- Efforts for implementing ISO standards are made.
- Evidence is collected based on national legal requirements.

Figure 15: Replies to question 25 of the online survey



4.4.2.3 EU cybersecurity certification

One of the tools that could provide security assurance for sharing of information and data between communities could be cybersecurity certification. For example, tools for secure exchange of information useful as evidence in criminal proceedings could be certified through specific certification schemes. Currently, cybersecurity certification is only implemented at national level and broader EU level involvement is expected following the adoption of the Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (EU Council, 2019). This regulation, besides other provisions, creates the mandate for an EU-wide cybersecurity certification framework. The purpose of the EU cybersecurity certification framework under Regulation (EU) 2019/881 is to establish and maintain the trust and security on cybersecurity products, services and processes. This could help users and service providers to determine the level of security assurance of the products they use or provide. EU cybersecurity certification schemes aim to define specific requirements and criteria for assessing the level of adherence of specific products against these requirements. Specific products, services and processes will then be assessed by conformity assessment bodies at national level, an issued certificate will then be valid throughout the EU.

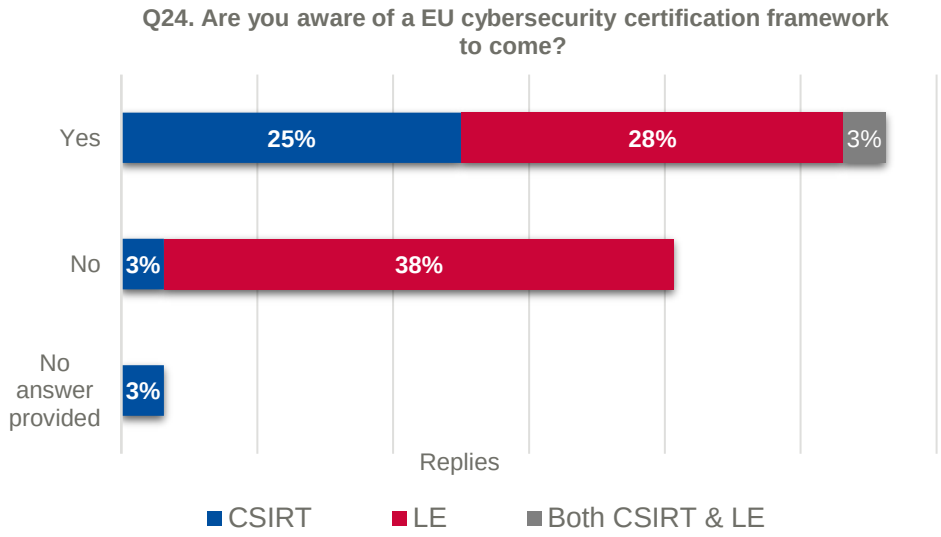
Such mechanisms could be used also to certify the level of security assurance of products and processes used to collect and share information and data among the communities; this could help to build trust and mutual understanding among CSIRTs, LEs and the judiciary. Also, quality and validity of evidence collected and produced by such certified products and services could be considered high and decrease the likelihood of inadmissible evidence in criminal proceedings.

Interviews conducted clearly show that only half of the respondents are aware of the existence of the Cybersecurity Act and its content, as illustrated in Figure 16 below. Those who know about this legislation and are familiar with the proposed certification mechanism can be divided into two groups:

- Respondents who do not consider EU certification to be relevant to cooperation or information sharing, or do not expect this legislation to have a positive impact on it.

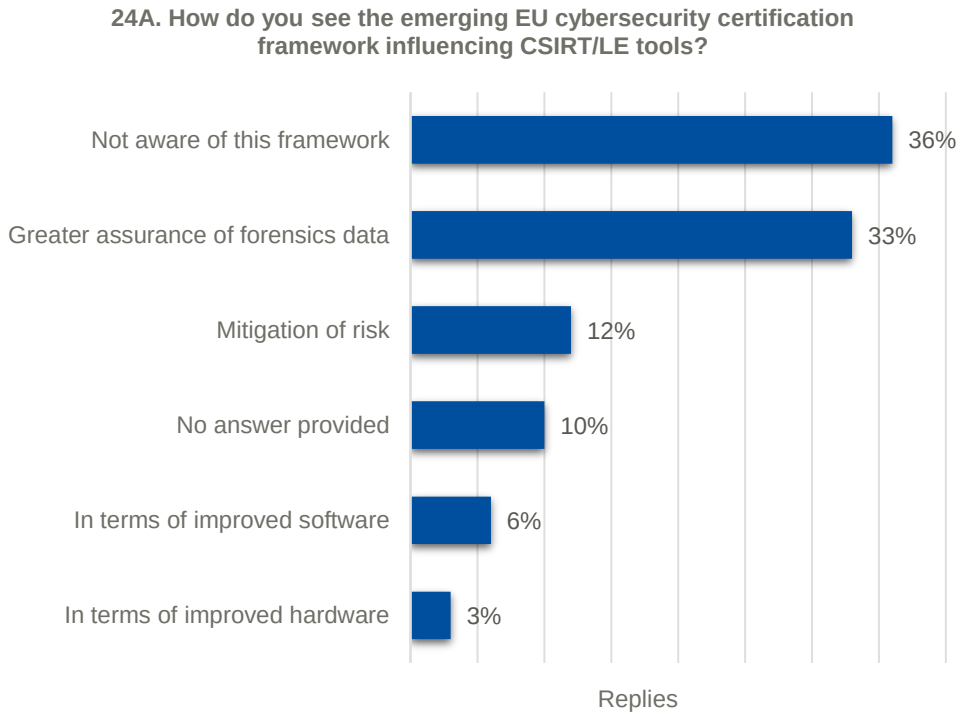
- Respondents who believe that successful implementation of EU-wide certification could produce two effects:
    - First, to build trust between communities by allowing the use of secure and certified tools to collect and transfer information and data and by verifying the security and efficiency of the mechanisms and procedures applied;
    - Second, to specify procedural duties and responsibilities of individual communities in cooperation.

Figure 16: Replies to question 24 of the online survey



In Figure 17, those aware of the emerging EU cybersecurity certification framework believe that technical cooperation between CSIRT and LE could be enhanced as certified CSIRT/LE tools can increase the level of assurance of forensic data acquired and mitigate the risks encountered.

Figure 17: Replies to question 24A of the online survey



4.4.3 Major cross-border cyber-attacks

For CSIRT and LE, preparedness against large-scale cyber-attacks, EU Blueprint and LE ERP serve as tools to support the communities in effectively detecting, investigating, disrupting and deterring large-scale cyber incidents of a suspected criminal nature.

4.4.3.1 EU Blueprint

On September 2017, under the Estonian presidency, the European Commission validated a blueprint (EU Commission, 2017) regarding an LE major cross-border cyber crisis emergency protocol. Two major cyber crises, namely WannaCry and NotPetya, highlighted the great need for a coordinated response in case of large-scale incidents that are hard to handle at national level.

Also, in 2017, the Council of the European Union adopted a Framework for joint EU Diplomatic Response to Malicious Cyber Activities (EU Council, 2018). This framework makes full use of measures within the EU common foreign and security policy, including restrictive measures.

In 2018, Council Conclusions on EU Coordinated Response to Large-Scale Incidents and Crisis was aimed at making operational the Blueprint, along with the development of a European Cybersecurity Crisis Cooperation Framework. This led to the LE Emergency Response Protocol (LE ERP).

4.4.3.2 LE ERP

The ERP is a protocol to support LE in providing immediate response to major cross-border cyber-attacks through:

- Rapid assessment;
- Secure and timely sharing of critical information;
- Effective coordination of international aspects of investigations.

ERP is split among several parts:

- Procedures, roles and responsibilities;
- Secure channel of communication;
- Contact points for exchange of critical information;
- Coordination and de-confliction mechanism.

ERP steps unfold as follows:

1. **Early detection of incident**: OSINT monitoring, Europol operational centre, LE, CSIRT network, partners (ENISA, UNODC, OSCE), private sector partners, other (academia, research institutes);
2. **Threat assessment**: Incident's relevance is assessed through a matrix taking into account target's nature and scope (geographical, number of services affected, type of victims affected, number of victims affected) and impact (damage potential, recoverability, reproducibility, tangible losses);
3. **Decision**: Based on previous assessment, decision to enter protocol and proceed through ERP steps or revert to normal operation is taken;
4. **Establishing coordination centre and activate information-sharing tool**;
5. **Early warning notification (EWN)**: Europol produces the EWN and shares that with stakeholders;
6. **Emergency operational action plan (EOAP)**: Europol and stakeholders coordinate and produce the EOAP in order to streamline operational actions in response to the crisis;
7. **Investigations and multilayer analysis**: Member State and Europol lead investigation, through OSINT or on site, while exchanging information in real time;
8. **Situational assessment**: Depending on last situational assessment, decision is made to repeat previous steps of the protocol OR close protocol;
9. **Closure of ERP**: Once incident is contained, ERP is closed. Notices are sent to all stakeholders and debriefing is organised.

4.4.3.3 Impact on CSIRT/LE cooperation

ERP is a LE coordination mechanism aimed at preserving evidence and taking advantage of LE reaction capacities and manpower.

CSIRT play an important role into ERP as stakeholders and primary information source.

First, National CSIRTs are usually in charge of crisis management. At step 2 (threat assessment), they state whether or not a crisis is ongoing.

Second, CSIRTs are a privileged source of qualified information. Based on their tools, expertise and broad ecosystem (system probes, industrial partnerships), they have access to relevant intelligence that would otherwise not reach LE.

ERP is a LE/judiciary protocol for emergency response that includes CSIRT as a full partner; this is an example of cooperation among three communities.

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

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

- Working together (in the same building/office), or at least having liaison officers, is recognised as being the most efficient way of ensuring very good cooperation and information sharing between CSIRT and LE. This model is successfully implemented at least by the Nordic countries.
- There is a very low interaction between the judiciary and the CSIRTs.
- Cultural differences between CSIRT and LE are seen as the most important obstacle to cooperation and information sharing.
- Recent EU legislation on personal data protection (including GDPR) makes the cooperation between CSIRTs and LE harder as it sets stricter compliance requirements for the data processors and applies visibility restrictions even to data that were public in the past (e.g. WHOIS issue).
- LE often rely on CSIRTs' technical support and expertise as well as on sharing data about incidents.

Multi-stakeholder cooperation and information sharing are the key activities for ensuring cybersecurity. However, as can be seen from the online survey carried out and the interviews conducted, in all countries there is space for improvement of this cooperation, depending on the maturity level of each community and the restrictions that are being set by their national legal framework. Improvements can be made in organisational, technical, cultural and legal aspects of this cooperation:

- **Organisational challenges:** There are no formal rules in place for cooperation among the communities to set the ground for sharing experience, knowledge and getting acquainted with each other's practices.
- **Technical challenges:** There is a lack of effective tools for secure sharing of information and data as well as for evidence collection.
- **Cultural challenges:** There is lack of trust among the communities and this results in sharing a limited amount of information. The staff of each community are either not encouraged or conversely required by law or policies to provide assistance or cooperation to other communities.
- **Legal challenges:** Poor implementation or wrong interpretation of the EU legislation for the protection of personal data sometimes may lead to lack of information sharing; liability issues in data breach cases seem to be a challenge for the staff who are acting as data processors or controllers.

5.1.1 The importance of cooperation

An information security incident can be either a minor security incident or can also be a cybercrime. If the incident is also a crime, it is necessary to identify the perpetrators. To achieve this goal, cooperation and interaction among CSIRTs, LE and the judiciary are of fundamental importance; therefore, the cooperation challenges highlighted through the interviews should be eliminated.

5.1.2 Effectiveness of cooperation

Effective cooperation is based both on the knowledge of the legal framework and on some factual aspects. In particular:

(a) The legal framework on the subject is articulated. Even if the acts of the European Union contribute to progressively eliminating the diversities in legislation of the various Member States, significant differences are still highlighted across them. Interviewees from the LE community pointed out that in some cases the communities might not have a thorough knowledge of some key EU legal instruments, such as the European Investigation Order (EIO) ([40]) that can play an important role in the investigation of cybercrime.
(b) CSIRT, LE, and the judiciary have different mind-sets due to their different educational and scientific backgrounds. This type of difference can set obstacles to the effectiveness of an investigation as they make communication among these three communities harder. Moreover, the different objectives set by the CSIRTs, LE, and judiciary sometimes make CSIRTs ignore the legal requirements for the data validity that could influence the admissibility of the data collected as evidence in a criminal trial.

5.1.3 Strengthening of cooperation

Despite the significant advances in the field of cooperation, the analysis of the collected data shows that it is necessary to further strengthen it. In order to achieve this goal it is necessary to act on a series of factors such as:

(a) To simplify the communication mechanisms between CSIRT, LE, and the judiciary;
(b) To speed up the time needed to obtain authorisation from their hierarchy by LE and the judiciary;
(c) To deliver technical and legal training dedicated to cooperation and interaction across CSIRT, LE and the judiciary;
(d) To improve the knowledge of the English language of everyone involved.

5.2 Recommendations

The recommendations presented in this roadmap have been categorised into organisational, technical, cultural and legal, based on the aforementioned cooperation challenges.

5.2.1 Organisational

It is evident that CSIRT, LE and judiciary communities have complementary roles when fighting against cybercrime; it is important to have clarity in duties and responsibilities of each actor and measures in place to ensure coordination in order to avoid duplication of effort and increase the effectiveness of combatting cybercrime. The segregation of duties matrix (for an example see section 4.1.1.1.), once customised for each country, could help to give clarity of responsibilities of each community and identify overlaps that may cause mutual interference in their activities.

([40]) http://www.eurojust.europa.eu/Practitioners/operational/EIO/Pages/EIO.aspx

Defining an explicit cooperation framework among the various actors would also facilitate interaction across the three communities. By setting up internal procedures for information sharing and best practices exchange, LE and CSIRTs can automate the cooperation process and make it more tangible, embedded into day-to-day activities.

These rules can be implemented in various forms. Depending on each EU MS's maturity level on law adoption, such a cooperation framework could be a legal instrument (regulating the functioning of CSIRTs, handling cybersecurity incidents, investigating cybercrime, etc.), national policy documents, inter-community memoranda of understanding, or their mutually compatible internal guidelines.

The interviews also showed that appointing liaison officers in the partner community can significantly enhance mutual trust and the effectiveness of cooperation. LE liaison officers involved in CSIRT activities may provide assistance in identifying and qualifying offences, collecting evidence properly, identifying offenders, or providing assistance to LE. CSIRT liaison officers involved in LE activities can in turn provide their own expertise and experience with specific technologies, where appropriate, provide access to information and data available to CSIRTs or contacts with experts and partners. Beyond liaison officers, staff of each community could also be assigned in other communities for adequate posting. CSIRT personnel could spend some time as technical experts in an LE unit while an LE officer could work in crisis management within a CSIRT community.

Some Member States have put CSIRT and LE to work together in the same building. Building a common culture and ecosystem has proved efficient for their cooperation. This is a way also to improve cooperation conditions among the communities, making the information exchange easier; by doing this, Member States could build a team comprising different actors able to work together during investigations.

Staff exchange and liaison officers could facilitate the mutual understanding across the communities and voluntary information sharing on specific topics/cases. These opportunities will create mixed culture personnel and thus strengthen cooperation.

Based on the data collected for this report, the main recommendations related to the organisational aspects of the cooperation are:

- **Member States with the support of ENISA, Europol and possibly Eurojust**: To reach a better understanding and spread across the communities the knowledge of roles and responsibilities of CSIRTs, LE and the judiciary throughout the cybercrime lifecycle phases, possibly by using 'Segregation of duties' matrix;
- **Member States with the support of ENISA and Europol**: To promote staff exchange between CSIRTs and LE and appoint liaison officers;
- **ENISA and Europol**: To support the Member States to identify key information flow paths to strengthen the cooperation across CSIRTs, LE and the judiciary.

5.2.2 Technical

Using a common taxonomy (section 4.1.1.5.) solves the common problem of different classification and description of individual types of cybersecurity incidents and their links to criminal offences. Taxonomies can be extended to community best practices, definitions, references to relevant legislation, or division of responsibilities in individual cases.

Also using common tools could help the communities' coordination. For instance, data collection tools used by CSIRTs often do not store data in a format that can also be used operatively by law enforcement authorities and judiciary. When the usage of the same tools is not feasible, at least interoperability of tools could help cooperation and mitigate possible operational challenges in information exchange. Thus, it is of great importance for CSIRTs, LE and the judiciary to take into account interoperability requirements when conceiving tools, to make sure that each tool can export data in a standard format that can be functional for all communities.

Based on the data collected for this report, the main recommendations related to the technical aspects of the cooperation are:

- **ENISA, Europol's EC3, and Member States**: To promote the use of common taxonomy;
- **ENISA, Europol's EC3, and Member States**: To promote usage of common tools or at least interoperability of tools deployed and conceived considering future technologies ([41]).

5.2.3 Cultural

Setting up regular synchronous and asynchronous meetings as well as physical meetings allows the communities to share information about the current security situation, risks, vulnerabilities and experiences. In particular, this helps to raise their awareness of current threat landscape and foster mutual trust across the communities. This can be achieved:

- Through joint exercises (section 4.1.3.), not only are individual skills tested, but also individual communities are familiarised with practices of their counterparts; shared exercise could also help the communities to identify inappropriate procedural rules and build personal ties between the members of each community.
- Through workshops (section 4.1.2.6.), individual communities can share experiences and knowledge. This event type is particularly suitable for exchanging information on legal rules, appropriate procedural procedures or specific technical procedures in specific cases.
- Best practices exchange (section 4.1.3.3.) creates opportunities for the staff to debate and share practices on each community's field of expertise.
- Regular joint meetings give the communities the chance to cooperate and this seems to be a good tool not only for sharing experience, information on threats and vulnerabilities, trends and other important news, but also for building trust based on personal connections between members of such communities.
- Experience sharing (section 4.1.3.2.) gives the staff the opportunity to identify what worked well and what can be improved through their professional experience.

Cybersecurity/legal glossaries can also improve mutual understanding by clearly defining terms that might be understood differently across the three communities. Publishing internal guides (section 4.1.3.3.) provides the communities with internal-use-only material on how cooperation is developed at operational level as an everyday duty.

When assessing the qualifications of members of individual communities, the requirement for their ability to interact with other relevant communities is often not taken into account. Creating an appropriate qualifications framework that defines the roles of employees within the communities, the experience and knowledge expected by them, could probably eliminate this

([41]) For further detail also refer to section 4.2.4.

deficiency. A competency framework that could provide specific requirements for these roles could encourage educational institutions to include in their curriculum appropriate courses and training focused on cooperation, while employers would also take these requirements into account when selecting employees.

In previous ENISA reports, the importance of joint training for CSIRTs, LE and the judiciary was highlighted. However, the interviews conducted to prepare this roadmap showed that training organised is often criticised for its inadequacy, its usefulness and most of the time it is even considered as a waste of time.

It is therefore necessary to promote high-level training useful for the CSIRTs, LE and the judiciary that could be appealing to them. In order to do this, well-prepared trainers are needed. They should have appropriate theoretical and practical knowledge, as well as the ability to communicate their knowledge effectively.

The interviews showed that the communities' knowledge of digital forensics rules related to the criminal trial can be further improved. Measures and actions operated by CSIRTs when handling a security incident could delete evidence or compromise the LE investigation (section 4.1.2.7). This has a direct impact on the evidence admissibility and the outcome of the investigation, hence it must not be neglected.

Both joint exercises focused on technical cooperation and table-top exercises focused on management cooperation could be very effective tools. Through these we can evaluate the appropriateness of having set internal procedures, the ability of individual communities to cooperate and also provide practical experience of cooperation, helping thus the communities to build mutual trust. Creating specific exercises focused on specific aspects of cooperation between specific communities and entities is effective, however often very costly. Interested communities could participate in already existing national and international exercises to test their cooperation in practice.

Interdisciplinary training covering not only the technical aspects but also the legal aspects should be provided. For example, the lack of knowledge of the relevant legislation and of the established procedural practices are key challenges that the communities are faced with. In particular, CSIRTs might lack knowledge of the law governing the practice of obtaining electronic evidence and procedures applied in criminal proceedings. On the other hand the law enforcement and the judicial authorities might not have a thorough knowledge of the functioning of the CSIRTs and the potential in terms of support that might have from CSIRTs in collecting evidence.

Based on the data collected for this report, the main recommendations related to the cultural aspects of the cooperation are:

- **Member States, possibly with the support of ENISA**: To analyse composition and size of available workforce and develop national competency frameworks;
- **ENISA, possibly with and Europol's EC3, CEPOL and Eurojust:** To help CSIRTs, LE, and the judiciary to identify joint training possibilities on digital forensics where technical and legal aspects are both examined; to promote a culture of training, both for technical and legal matters; to prepare training material on CSIRTs, LE and the judiciary cooperation targeting the three communities;
- **Member States:** To allow and encourage CSIRTs, LE and the judiciary (staff from all hierarchical levels) to participate in the trainings and exercises.

5.2.4 Legal

To avoid duplication of efforts, undesired interference and to assure an efficient utilisation of the resources and expertise, Member States should define and implement cooperation frameworks among CSIRTs, LE and the judiciary by taking into account the responsibilities and capabilities of these communities as well as their complementarity.

Agreements and memoranda of understanding are instruments where the rules of cooperation and requirements related to evidence handling are defined; these types of cooperation agreements can help CSIRT, LE and the judiciary representatives work together against cybercrime and can significantly increase the effectiveness of their cooperation.

When designing and developing tools for communities, specific requirements defined by each of them are taken into account. Security and privacy standards of the tools utilised may vary from one community to another; a certification scheme that might provide a certain level of security assurance for the tools used during the cybercrime investigation would further enhance the cooperation among the three communities. Additionally, applying security standards on the identification, collection, acquisition and preservation of e-evidence, may assist the communities in ensuring the admissibility of e-evidence in a criminal proceeding and hence promote successful cross-sectoral and international cooperation in the field (section 4.4.2).

- **ENISA**: To identify and disseminate good practices of cooperation frameworks, by using existing legal instruments and possibly additional memorandum of understanding and cooperation agreements, among CSIRTs, LE and the judiciary at national and at cross-border level;
- **Member States**: To define and implement cooperation frameworks among CSIRTs, LE and the judiciary;
- **ENISA**: To assess the suitability of an EU cybersecurity certification scheme for cybercrime investigation tools.

6. BIBLIOGRAPHY/REFERENCES

Abrams, L. (2019, July 20). *Russian FSB Intel Agency Contractor Hacked, Secret Projects Exposed*. Retrieved from Bleeping Computer: https://www.bleepingcomputer.com/news/security/russian-fsb-intel-agency-contractor-hacked-secret-projects-exposed/

Andy Greenberg, W. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Cambridge Dictionary. (n.d.). *Prosecutor*. Retrieved July 27, 2018, from https://dictionary.cambridge.org/dictionary/english/prosecutor

Capgemini. (2019, June 24). *Capgemini and Altran create a global digital transformation leader for industrial and tech companies*. Retrieved from https://www.capgemini.com: https://www.capgemini.com/news/capgemini-and-altran-create-a-global-digital-transformation-leader-for-industrial-and-tech-companies/

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

Council of Europe. (2001, 11 23). *Convention on Cybercrime*. Retrieved from Council of Europe: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council of Europe. (2003, January 28). *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. Retrieved from Council of Europe: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

Council of Europe. (2019). *Preparation of the2ndAdditional Protocol to the Budapest Convention on Cybercrime.* Retrieved from https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff

Council of the European Union. (2017, October 2). *Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime".* Retrieved from http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf

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

Council, E. (2016a, April 27). *DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

Czech Republic, P. o. (2014). Retrieved from https://www.govcert.cz/download/kii-vis/preklady/Act_181_2014_EN_v1.0_final.pdf

EC3, E. (2017). Retrieved from https://www.europol.europa.eu/publications-documents/petya-ransomware-what-can-you-do

EFTA. (n.d.). *The EFTA States*. Retrieved September 05, 2017, from http://www.efta.int/about-efta/the-efta-states

ENI. (n.d.). *The European Neighbourhood Instrument (ENI).* Retrieved from https://ec.europa.eu/regional_policy/en/policy/what/glossary/e/european-neighbourhood-investment

ENISA. (2015). *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches'.* Retrieved July 06, 2017, from https://www.enisa.europa.eu/publications/cybersecurity-information-sharing

ENISA. (2015a). *ENISA – CERT Inventory.* Retrieved 07 06, 2017, from https://www.enisa.europa.eu/publications/inventory-of-cert-activities-in-europe

ENISA. (2016). *A good practice guide of using taxonomies in incident prevention and detection.* Retrieved from https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-preventiondetection/at_download/fullReport

ENISA. (2016a). *Report on Cyber Security Information Sharing in the Energy Sector.* Retrieved July 06, 2017, from https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector

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

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

ENISA. (2017b). Retrieved from https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

ENISA. (2018). *Cooperation between CSIRTs and LE: interaction with the judiciary.* Retrieved from https://www.enisa.europa.eu/publications/csirts-le-cooperation

ENISA. (2018a). *Review of Behavioural Sciences Research in the Field of Cybersecurity.* Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

ENISA. (2018b). *ENISA Programming Document 2019-2021.* Retrieved July 4, 2018, from https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2019-2021

ENISA. (2018c). Retrieved July 4, 2018, from 7th ENISA/EC3 Workshop: https://www.enisa.europa.eu/events/6th-enisa-ec3-workshop/7th-enisa-ec3-workshop

ENISA. (2019). *Online Training Material - Technical*. Retrieved from ENISA: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational

ENISA. (2019a). *ENISA publishes training course material on network forensics for cybersecurity specialists*. Retrieved August 08, 2019, from ENISA: https://www.enisa.europa.eu/news/enisa-news/enisa-publishes-training-course-material-on-network-forensics-for-cybersecurity-specialists

ENISA. (n.d.). *CEI – List of NIS Experts*. Retrieved July 4, 2018, from https://www.enisa.europa.eu/procurement/cei-list-of-nis-experts

ENISA. (n.d.a). *CSIRT Maturity*. Retrieved July 4, 2018, from https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

EU Commission. (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 from EU Commission: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=en

EU Commission. (2017, September 13). *ANNEXto the Commission Recommendationon Coordinated Response to Large Scale Cybersecurity Incidents and Crises*. Retrieved from EU Commission: https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF

EU Commission. (2018). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Fourteenth progress report towards an effective and genuine Security Union*. Retrieved from EU Commission: https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX%3A52018DC0211

EU Commission. (n.d.). *European Neighbourhood Policy And Enlargement Negotiations*. Retrieved August 08, 2019, from EU Commission: https://ec.europa.eu/neighbourhood-enlargement/instruments/overview_en

EU Commission. (n.d.). *The EU's Instrument contributing to Stability and Peace (IcSP)*. Retrieved from EU Commission: https://ec.europa.eu/fpi/news/eu%E2%80%99s-instrument-contributing-stability-and-peace-icsp_en

EU Council. (2002, July 12). *DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILof 12 July 2002concerning the processing of personal data and the protection of privacy in the electronic commu-nications sector (Directive on privacy and electronic communications)*. Retrieved from EU Council: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

EU Council. (2009, November 30). *COUNCIL FRAMEWORK DECISION 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings*. Retrieved from EU Council: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:328:0042:0047:EN:PDF

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

EU Council. (2016). *European Parliament and Council of the European Union. (2016, April 2016). Directive (EU) 2016/680 on protection of natural persons with regard to processing of personal data by competent authorities for purposes of prevention, investigation, detection or*. Retrieved July 30, 2019, from EU Council: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

EU Council. (2016, 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 from EU Council: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=IT

EU Council. (2016b, April 27). *DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detectio*. Retrieved from EU Council: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

EU Council. (2018, April 16). *Council conclusions on malicious cyber activities -approval*. Retrieved from EU Council: http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf

EU Council. (2019). *Regulation on ENISA (the European Union Agency for Cybersecurity).* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

EU Council. (n.d.). *Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communic*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0024

EU Court of Justice. (2014, April 8). *Judgment of the Court (Grand Chamber), 8 April 2014*. Retrieved from EU Court of Justice: https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2014.175.01.0006.01.ENG

EU Member States. (2007). *Treaty of Lisbon.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12007L%2FTXT

EU Parliament, C. a. (2012). *EU Charter of Fundamental Rights.* Retrieved from https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en

Eurojust. (2016). Retrieved from http://www.eurojust.europa.eu/press/PressReleases/Pages/2016/2016-12-01.aspx

European Commission. (2018a). *Operational Guidance for the EU's international cooperation on cyber capacity building*. Retrieved from https://ec.europa.eu/europeaid/sites/devco/files/guidelines-cybersecurity-na-20180820_en.pdf

European Union. (2019, July 1). *The 28 member countries of the EU*. Retrieved from https://europa.eu/european-union/about-eu/countries_en

European Union, M. S. (2012). *Treaty on the Functioning of the European Union.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

Europol. (2017). Retrieved from https://www.europol.europa.eu/newsroom/news/closing-online-crime-attribution-gap-european-law-enforcement-tackles-carrier-grade-nat-cgn

Europol. (2019). *Law enforcement agencies across the EU prepare for major cross-border cyber-attacks.* Retrieved from https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks

Gov CERT CZ. (2015). *Cyber Security Glossary*. Retrieved from Gov CERT CZ: https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

Krebs, D. (2019, January 19). *Courts Hand Down Hard Jail Time for DDoS*. Retrieved August 08, 2019, from Krebs on security: https://krebsonsecurity.com/tag/mirai/

KYPO by CSIRT MU. (n.d.). *KYPO CYBER RANGE*. Retrieved August 08, 2019, from KYPO by CSIRT MU: https://www.kypo.cz/en

Mattermost. (n.d.). *Mattermost*. Retrieved August 08, 2019, from Mattermost: https://mattermost.com/

MISP Project. (n.d.). *MISP Threat Sharing*. Retrieved from https://www.misp-project.org/

Mitrakas, A. &. (2009). *Digital Forensics and the Chain of Custody to Counter Cybercrime. In Socioeconomic and Legal Implications of Electronic Intrusion. doi:DOI: 10.4018/978-1-60566-204-6.ch010.*

Moret E., Pawlak P. (2017, July 12). *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?* Retrieved August 08, 2019, from ISS: https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime

National Institute of Standards and Technology. (2017, August). *NICE Cybersecurity Workforce Framework* . Retrieved from NIST: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Official Journal of the European Union. (2016, April 27). *DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

Popa R.A., S. E. (2016). Building web applications on top of encrypted data using Mylar. *Crypto ePrint Archive*. Retrieved from https://css.csail.mit.edu/mylar/mylar.pdf

UNODC. (n.d.). *University Module Series Cybercrime*. Retrieved August 08, 2019, from UNODC: https://www.unodc.org/e4j/en/tertiary/cybercrime.html

WP, Article 29. (2017, October). Retrieved from WP250rev.01: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

A ANNEX: ABBREVIATIONS

Abbreviation	Description
BKA	Bundeskriminalamt: German criminal police
BSI	Bundesamt für Sicherheit in der Informationstechnik: German national cybersecurity authority
C²	Command and Control
CCTV	Closed-Circuit Television
CEI	Call for Expression of Interest
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
CGN	Carrier Grade NAT
CIA	Confidentiality, Integrity, Availability
CIRCL	Computer Incident Response Centre of Luxembourg
CSIRT	Computer Security Incident Response Team
COE	Council of Europe
DDoS	Distributed Denial-of-Service (attack)
DNS	Domain Name System
DPA	Data Protection Authority
EC3	European Cybercrime Centre (Europol)
EFTA	European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland)
ENI	European Neighbourhood Instrument
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCTF	European Union Cybercrime Task Force
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation
FSB	Federal'naja služba bezopasnosti Rossijskoj Federacii – Federal Security Service of the Russian Federation
GDPR	General Data Protection Regulation

ICANN	Internet Corporation for Assigned Names and Numbers
IcSP	Instrument contributing to Stability and Peace
IOC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPA	Instrument for Pre-Accession Assistance
ISP	Internet Service Provider
LE	Law Enforcement
LEA	Law Enforcement Agency
MISP	Malware Information Sharing Platform
MLAT	Mutual Legal Assistance Treaty
MFT	Master File Table
MS	Member State
NCISA	National Cyber and Information Security Authority
NCSC	National Cyber Security Centre
n.d.	No Date
OSCE	Organisation for Security and Cooperation in Europe
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PED	Portable Electronic Device
SIENA	Secure Information Exchange Network Application
SoD	Segregation (or separation) of Duties
TCP	Transmission Control Protocol
UNODC	United Nation Office on Drugs and Crime

B EU LEGAL INSTRUMENTS RELEVANT IN THE AREA OF FIGHTING AGAINST CYBERCRIME

EU legal instruments relevant in the area of fighting against cybercrime are listed below. This is not an exhaustive analysis but an indicative one.

Regulations and directives:

Regulations of the European Parliament and of the Council	**Subject**
Regulation (EU) 2019/881 ([42])	Regulation on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
Regulation (EU) 2018/1725 ([43])	Regulation on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
Regulation (EU) 2016/679 ([44])	Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Regulation (EU) 910/2014 ([45])	Regulation on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
Directives (EU) of the European Parliament and of the Council	**Subject**
Directive (EU) 2016/1148 (NIS Directive) ([46])	Directive concerning measures for a high common level of security of network and information systems across the Union.
Directive (EU) 2016/680 ([47])	Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (LEA Directive).

([42]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN
([43]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN
([44]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=IT
([45]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN
([46]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
([47]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

Directive 2014/41/EU ([48])	Directive regarding the European Investigation Order in criminal matters.
Directive (EU) 2013/40 ([49])	Directive on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. This directive represents an effort of the EU to harmonise substantive criminal law defining offences targeted against information systems.
Directive 2002/58/EC ([50])	Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Additional acts:

Council Framework Decision	**Subject**
Decision 2009/948/JHA ([51])	Decision on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings.
Decision 2008/947/JHA ([52])	Decision on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions.
Recommendations	**Subject**
Commission Recommendations (EU) 2017/1584 ([53])	Recommendation on coordinated response to large-scale cybersecurity incidents and crises.
Communications	**Subject**
JOIN/2017/0450 final	Joint Communication Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.
COM(2016) 410 final ([54])	Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.
JOIN/2013/01 final ([55])	Joint Communication on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.
Proposals	**Subject**
COM/2018/225 final ([56])	Proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters.
COM/2018/226 final ([57])	Proposal for a directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

([48]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN
([49]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN
([50]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN
([51]) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:328:0042:0047:EN:PDF
([52]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0947&from=EN
([53]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584&from=EN
([54]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0410&from=EN
([55]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=en
([56]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN
([57]) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0226&from=EN

Finally, there are some additional EU instruments aimed at supporting the collaboration at international scale in the area of cybersecurity. They are: Instrument contributing to Stability and Peace ([58]) (IcSP) ((EU Commission, n.d.)), European Neighbourhood Instrument (ENI) (ENI, n.d.), and Instrument for Pre-Accession Assistance ([59]) (IPA) ((EU Commission, n.d.)). IPA consists of several systems aimed at help countries willing to integrate EU. Among these tools, cross-border instruments enhance cooperation.

Data protection and data retention

Given the importance of protecting privacy, it is necessary to specifically note the EU legislation on data protection and data retention.

The right to protection of personal data is a fundamental right. It is aimed at protecting 'personal data', i.e. 'any information relating to an identified or identifiable natural person ("data subject")' (Article 4, GDPR). The protection of privacy of electronic communications is specifically addressed under Directive 2002/58/EC. Within the European legal framework, this fundamental right is provided by several acts. Among them, the following are particularly significant:

Fundamental right	Legal act
Respect for private and family life	Article 7, Charter of Fundamental Rights of the European Union (EU Parliament, EU Charter of Fundamental Rights, 2012)
Protection of personal data	Article 8, Charter of Fundamental Rights of the European Union (EU Parliament, EU Charter of Fundamental Rights, 2012)
Right to the protection of personal data	Article 16, (ex-Article 286 TEC) of the Treaty on the Functioning of the European Union (TFEU) (European Union, 2012)

The protection of privacy as a fundamental right is also provided under the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms, also called European Convention on Human Rights (ECHR) (Council of Europe, 1950) and more precisely by Article 8 'Right to respect for private and family life'. It should be noted that further to the EU Member States' adherence to the ECHR, the European Union is expected to proceed with the accession to the ECHR ([60]) under the relevant legal obligation defined by the Treaty of Lisbon (Article 6, paragraph 2) (EU Member States, 2007).

The worldwide diffusion of IT and globalisation have caused and continue to cause new challenges for the protection of personal data. For this reason, three important acts aimed at strengthening the legal protection of personal data were issued in 2016. These acts are: Regulation (EU) 2016/679 (General Data Protection Regulation), Directive (EU) 2016/680 (Law Enforcement Data Protection Directive) and 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 (European Parliament and Council of the European Union, 2016) ([61]) (PNR Directive).

([58]) https://ec.europa.eu/fpi/news/eu%E2%80%99s-instrument-contributing-stability-and-peace-icsp_en
([59]) https://ec.europa.eu/neighbourhood-enlargement/instruments/overview_en
([60]) https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-completion-of-eu-accession-to-the-echr
([61]) https://eur-lex.europa.eu/eli/dir/2016/681/oj

The right to the protection of personal data is a fundamental right. Nevertheless, it 'is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality' (see recital 4, GDPR). In particular it is necessary to balance the right to the protection of personal data with requirements concerning prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Instead, data retention is the storage activity of 'traffic data' for a given period (which is called 'retention time') for the purposes of the prevention, investigation, detection or prosecution of criminal offences. Traffic data 'means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service' (see Article 1, letter d) of the Convention on Cybercrime (Council of Europe, 2001).

Some examples of traffic data are: the user ID(s) allocated; the user ID and telephone number allocated to any communication entering the public telephone network; the name and address of the subscriber or registered user to whom an internet protocol (IP) address, user ID or telephone number was allocated at the time of the communication; the user ID or telephone number of the intended recipient(s) of an internet telephony call; the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication; the date and time of the log-in and log-off of the internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the internet access service provider to a communication, and the user ID of the subscriber or registered user; the date and time of the log-in and log-off of the internet email service or internet telephony service, based on a certain time zone; the calling and called telephone numbers; the international mobile subscriber identity (IMSI) of the calling party; the international mobile equipment identity (IMEI) of the calling party; the IMSI of the called party; the IMEI of the called party; the calling telephone number for dial-up access; the digital subscriber line (DSL) or other end point of the originator of the communication; data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

Since these data can be very important for investigation purposes, the legislation in many Member States requires that the traffic data are stored in suitable archives. The problem arises that the legislation should balance the needs of data protection and the needs of data storage for the purposes of the prevention, investigation, detection or prosecution of criminal offences.

Such a balancing must necessarily comply with the principle of proportionality, but this is not always easy. This is clearly shown by the fact that the Grand Chamber of the Court of Justice of the European Union (EU Court of Justice, 2014) ([62]), on 8 April 2014, declared invalid Directive 2006/24/EC because of the breach of the principle of proportionality (EU Council, n.d.) . This was related to the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amended Directive 2002/58/EC.

At European level, the laws on data retention of the various states are sometimes significantly different from one another. In particular, the retention times are often different. The diversity of retention times sometimes appears to investigators as an obstacle to investigative cooperation.

([62]) Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others (Court of Justice of the European Union, 2014).

For this reason, European legislation that provides the same retention time in all Member States could result in improved cooperation.

Consequences of data breaches (European Court of Human Rights)

Data breach is only one of many possible information security incidents. It is a major incident and could lead to very heavy damage.

According to Article 4.12 of the GDPR, personal data breach 'means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

All personal data breaches are security incidents; however, not all security incidents are necessarily personal data breaches according to Article 29 Data Protection Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 (WP, Article 29, 2017).

In the case of a personal data breach, after the controller having become aware of it, two cases can occur:

(a) The personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In this case the controller is not obliged to notify the personal data breach to the competent supervisory authority (see Article 33.1 GDPR).
(b) The personal data breach is likely to result in a risk to the rights and freedoms of natural persons. In this case, the controller must notify the personal data breach to the competent supervisory authority. Such a notification must be delivered not later than 72 hours after the controller has become aware of it. If it is delivered after 72 hours, the reasons for the delay must be declared. This notification must include at least the following four points: a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; name and contact details of the data protection officer or other contact point where more information can be obtained; a description of the likely consequences of the personal data breach; a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects (see Article 33.3 GDPR).

Moreover, after becoming aware of a personal data breach, the processor shall notify the controller without undue delay.

In addition to the notification obligations established by the GDPR, depending on the specific cases, there may also be additional notification obligations provided for by other acts.

By way of example, the following notification obligations are mentioned here:

- Article 19.2 Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), which provides that 'Qualified and nonqualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein'.

- Articles 14 and 16 NIS Directive, which provide that operators of essential services and digital service providers notify security incidents to their competent authority.
- Data protection and data retention.

C ANNEX: QUESTIONNAIRE TO SUPPORT THE SUBJECT MATTER EXPERT INTERVIEWS

The questions below have been prepared to support the interviews with subject-matter experts to collect data for the 2019 ENISA roadmap of further activities in the area of CSIRT (computer security incident response teams) and law enforcement (LE) cooperation. The roadmap will not necessarily be made public; it is likely to be distributed instead to selected stakeholders.

This roadmap contributes to the implementation of 'Output O.4.2.2 – Support the fight against cybercrime and collaboration between CSIRTs and law enforcement' of the ENISA Programming Document 2019-2021, in particular to what is foreseen as publication: 'Roadmap to further enhance the cooperation between the CSIRTs and law enforcement and their interaction with the judiciary'.

(Link: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2019-2021).

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

The expected duration of the interview is 1 hour. Some of the questions below are common to CSIRTs, LEAs and judiciary (judges and prosecutor), while others are tailored to CSIRTs, LEAs and judiciary.

For information on how your personal data are processed, see the Privacy Statement below (after the questions).

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

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

SECTION 1 – QUESTIONS COMMON TO CSIRTs/LEAs AND JUDICIARY (PROSECUTORS AND JUDGES)

A. GENERAL

Q1: What do you expect from CSIRT/LE cooperation?

Q2: What do you expect from CSIRT/Judiciary cooperation?

Q3: In which particular fields (organisational/legal/technical/cultural) do you think cooperation can improve? Please provide examples where your team experienced an issue and improvement is necessary.

Q4: In which fields do you think cooperation is not possible?

Q5: Compared to other countries you may know, which are the fields in which cooperation works [A] best [B] important improvements can be made?

Q6: What are the hindrances to cooperation you may (never) overcome?

Q7: In case of unsuccessful cooperation experiences, what are the missing steps which should have been addressed? Please share success and failure stories. (What went well and what went wrong? What is the one single factor that can have a bad impact on CSIRT/LEA cooperation (legal, organisational, technical perspective)?)

B. ORGANISATIONAL

Q8: Do you have a protocol to report security incidents or cybercrime?

Q9: What is your definition of a security incident?

Q10: Have you ever attended a joint exercise where cooperation between CSIRTs/LEAs/Judiciary had been practiced? If so, do you find such exercises useful, and what are the main lessons learned there?

Q11: In your opinion, what kind of organisational measures would help the most to strengthen cooperation between the communities (CSIRT/LEA/Judiciary)?

B. TECHNICAL

Q12: Do you use any kind of taxonomy/glossary of terms that would support mutual understanding of the communities?

Q13: Do you know digital forensics? Do you know what a chain of custody is?

C. LEGAL

Q14: Have you ever asked for data based only on a trust relationship with other people? If you had requested data based on the trust relationship only, were those data sent to you?

Q15: Do you have any restrictions to share specific types of information with another community? If yes, what kinds of information/data types are you not allowed to share? Is there any data classification model that you follow as a guideline?

Q16: Are you familiar with Directive (EU) 2016/680 ([63]) on the processing of personal data for investigative purpose?

Q17: Are you familiar with the regulation of Directive (EU) 2016/680 concerning your background (judge/LEA/CSIRT) ([64])?

Q18: Are you familiar with recent EU legislation on personal data protection? Does it make it easier or harder for the communities to cooperate?

Q19: Are you familiar with the General Data protection Regulation at least for what concerns your case (judge/LEA/CSIRT)? Do you have any concerns on the 'Right to be Forgotten'?

Q20: Are you aware of the EU cybersecurity Act? How could EU cybersecurity certification influence the way that CSIRT, LE and the judiciary interact?

Q21: Are you aware of any formal rules (legal, internal policies, etc.) that regulate cooperation of your organisation with other communities (CSIRT/LE/JUD)? If not, what kind of rules should in your opinion regulate the cooperation (EU/national legislation, memoranda/agreements between the communities, soft-law, internal rules of each organisation, etc.)?

([63]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
([64]) This regulation refers, in particular, to General provisions, Principles, Rights of the data subject, Controller and processor, Transfers of personal data to third countries or international organisations, Independent supervisory authorities, Cooperation, Remedies, liability and penalties, Implementing acts.

SECTION 2 – CSIRT SPECIFIC QUESTIONS (TO BE POSED ONLY TO CSIRTs)

A. GENERAL

Q1A: In which case would you refrain from cooperating? Why?

Q2A: Cooperation in the area of investigation of a crime requires cooperation with other partners beyond the CSIRT network. Is your organisation ready for such a culture adaptation? What would be the challenges?

B. ORGANISATIONAL

Q3A: Are there topics your CSIRT does not address (general public, critical infrastructures cyberdefence, cybercrime, small and medium enterprises)?

Q4A: Are data requested from you more often by an LEA or a judge?
(a) What does your team do with the data, once it's been handed over to the LEA/judge?

Q5A: When you need to transmit data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, do you apply best practices for data collection and transmission?
(a) Traffic light protocol (TLP) codes, encryption, recipient verification

Q6A: Have you appointed a CSIRT–LEA liaison yet or have you any plans to do so in the near future? Is it a full time personal or shared role within your CSIRT?

Q7A: Do you inform your constituency upfront (when they contact you about an incident) that you will have to inform LEA at some case? Is this procedure published, publicly known?

Q8A: If you cooperate with LEA (see 2A), do you always include your own team (or parent organisation) legal team in the communication as support? Or is this handled by liaison person?

C. TECHNICAL

Q9A: How do you apply chain of custody within a CSIRT?

Q10A: Does your CSIRT provide training to LE?

(a) Yes
(b) No
(c) There is no need for such training

Q11A: Is there any information sharing tool you consider as a standard tool? Which one?

D. HUMAN

Q12A: What are the cultural main challenges for collaborating with LE?

C. LEGAL

Q13A: Can you share data with LE without raising trust issues with your CSIRTs partners?

Q14A: In your CSIRT, is there a person or a group of people who deal specifically with compliance with privacy regulations?

SECTION 3 – LEA-SPECIFIC QUESTIONS (TO BE POSED ONLY TO LEAs)

A. ORGANISATIONAL

Q1B: What kind of support would you expect from a CSIRT in an investigation? (e.g. use their technical expertise; contact points and cooperation mechanisms; cross check data, etc.)

Q2B: What would make a CSIRT a more trusted/reliable partner? (e.g. personnel background check?)

Q3B: Do you have police officers working as liaison officers in the CSIRT community? If yes, what would you expect of a liaison officer in the CSIRT?

Q4B: In which LE process would CSIRT be included first?

(a) Data collection
(b) Logs analysis
(c) C2 detection
(d) Server takedown
(e) Server seizure and analysis
(f) Other

Q5B: In which fields do you think you could share best practices or resources (technical or human)?
(a) Organisational
(b) Technical
(c) Human
(d) Legal

Q6B: Would you agree to open an instant messaging tool between CSIRTs and LE?

B. TECNICAL

Q7A: Is there a specific topic (ransomware, botnet, critical infrastructures) which can be used as a good first drill to initiate cooperation?

Q8B: What kind of cases or situation can be discussed to give priority to investigation or remediation?

Q9B: Would it be possible to use information-sharing tools (e.g.: MISP) to exchange technical data with CSIRTs?

C. HUMAN

Q10B: What would you expect from a CSIRT staff member in LE and vice versa?

D. LEGAL

Q11B: Have you ever relied on the application form for a European Investigation Order (EIO), either on your own initiative or following a judge's request?

Q12B: What kind of support would you expect from a CSIRT in an investigation? (e.g. use their technical expertise; contact points and cooperation mechanisms; cross check data, etc.)

Q13B: Would you recommend any changes in the criminal proceeding acts in order for LE to have greater legal powers?

Q14B: What are the conditions for intelligence received from a CSIRT to be actionable?

Q15B: In which case (if any) would you authorise a CSIRT to share investigation data?

Q16B: How is investigation secret handled and does this allow you to share investigation data with CSIRT in certain circumstances?

SECTION 4 – JUDICIARY (PROSECUTORS AND JUDGES) SPECIFIC QUESTIONS (TO BE POSED ONLY TO JUDICIARY)

A. GENERAL

Q1C: Are you familiar with the concept of CSIRT?

Q2A: What kind of value do you expect from cooperation with CSIRT (technical, expertise, intelligence)?

Q3C: What is the biggest non-legal obstacle you have identified when requesting data from a CSIRT?

Q4C: How do you think the cooperation across the three communities (CSIRT/LEA/Judiciary) could be improved?

B. ORGANISATIONAL

Q5C: Have you ever obtained data based on informal cooperation/based on trust between people?

Q6C: Have you ever cooperated directly with the CSIRT, or have you ever appointed CSIRT in the criminal investigation?

C. TECHNICAL

Q7C: Do you know what kind of information and expertise CSIRT can provide?

Q8C: Do you think such information/expertise could be useful for the criminal investigation/judiciary?

Q9C: Are there any legal provisions that prevent or make harder the cooperation with the CSIRT?

C. HUMAN

Q10C: Do you have any experience of interacting with CSIRT staff?

(a) Yes, if so, what are the main advantages/difficulties you encounter engaging with such personnel?

(b) No

Q11C: Are you willing/able to organise for your fellow magistrate and/or yourself a meeting with CSIRT?

(a) Yes
(b) No

D. LEGAL

Q12C: Can you accommodate the investigation secret on a case-by-case basis to allow CSIRT to share intelligence with the CSIRT network before the end of an investigation?

Q13C: Would you authorise LE to share intelligence with CSIRT on a by-default basis (authorised except when forbidden)?

Q14C: Is it easier to request data from a CSIRT in your state compared to a CSIRT from another state, or are there no differences?

Q15C: Are you familiar with the concept of European Investigation Order (EIO)?

Q16C: What is the biggest legal obstacle that you have identified when requesting data from a CSIRT?

Q17C: In the event that to request data from a CSIRT you must use the European Investigation Order (EIO), do you use the EIO or do you prefer to forgo data requests?

Q18C: Based on your working experience, have the data obtained from a CSIRT been inadmissible in a trial?

Q19C: Are you familiar with the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters?

Q20C: Are you familiar with the proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings?

Q21C: Is language a problem for requesting data abroad? Did you ever give up requesting data due to the difficulty in writing in a foreign language? Can you use translators in your work as a judge for requests to CSIRTs?

SECTION 5 – QUESTIONS ON MENTIONING OF NAME, AFFILIATION, AND COUNTRY

Q1: Do you agree on having your forename, surname, affiliation and country mentioned in the report (NOTE: it is not confirmed whether names of interviewees will be mentioned in the report)?

Q2: Do you agree on having your forename, surname, affiliation and country mentioned in the acknowledgements of the report? (NOTE: it is not confirmed whether names of interviewees will be mentioned in the acknowledgements of the report)?

Q3: Do you agree to having stated in the report that information on your country has been collected via an interview with a CSIRT/LE/judiciary (prosecutor/judge) representative?

Privacy Statement – ENISA Report on CSIRT-LE cooperation

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

The data controller of the processing operation is ENISA Core Operations Department. **The legal basis** for the processing operation is:

Article 5(1)(a) of Regulation (EU) 2018/1725, on the basis of Regulation (EU) No 526/2013, in particular the provisions establishing the tasks of ENISA. With the view of contributing to the fulfilment of such tasks and according to the ENISA Programming Document 2019-2021 as approved by Management Board in Decision No MB/2018/20 [2], ENISA is preparing a roadmap to further enhance the cooperation between the CSIRTs and law enforcement along with their interaction with the judiciary (see Output O.4.2.2 – Support the fight against cybercrime and collaboration between CSIRTs and law enforcement).

Article 5(1)(d) of Regulation EU 2018/1725, i.e. consent of the data subjects.

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

The data processors of the processing operation will be external experts who will be contracted by ENISA to support the data collection and drafting of the report. The online survey will be conducted by using the EU Survey tool [3]. The interviews will be conducted face to face, over the phone, via skype or with other means to be agreed with the interviewee.

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

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

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

The recipients of the data will be designated ENISA staff involved in the data collection and drafting of the report, as well as designated ENISA contractors supporting ENISA with the data collection and the drafting of the report (data processors). Only when explicit written consent is provided by the data subject, name, surname, affiliation, country, might be included in the acknowledgements of the roadmap. The roadmap will not necessarily be made public; it is likely to be distributed instead to select stakeholders. The data may also be available to EU bodies charged with compliance monitoring and inspection tasks.

Personal data will be kept up to a maximum period of 1 year after the publication and/or distribution of the roadmap, (possibly in March 2020). After the end of this period, the contact and professional data will be manually deleted. However, replies to survey/interviews will be kept by ENISA beyond this period in an anonymised form (without linking to specific respondents) for future ENISA projects.

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

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

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1543484984668&uri=CELEX:32018R1725
[2] https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2019-2021
[3] https://ec.europa.eu/eusurvey/home/welcome

D ANNEX: QUESTIONS OF THE ONLINE SURVEY

Brief survey for 2019 ENISA Report on CSIRT-LE cooperation

Fields marked with * are mandatory.

This short online survey has been prepared by ENISA, in conjunction with external experts, to support the data collection for the 2019 ENISA Roadmap of further activities in the area of CSIRTs (Computer Security Incident Response Teams) and law enforcement (LE) cooperation.

This roadmap contributes to the implementation of "Output O.4.2.2 - Support the fight against cybercrime and collaboration between CSIRTs and law enforcement" of the ENISA Programming Document 2019-2021, in particular to what is foreseen as publication: "Roadmap to further enhance the cooperation between the CSIRTs and law enforcement and their interaction with the judiciary".

Most questions are with closed answers but some free text boxes are also included in order to allow the respondents to add additional comments/information if they wish to do so. In this questionnaire, some free-text questions are included too.

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

For information on personal data processed within this specific survey, please download the following privacy statement:
Privacy_Statement.pdf

For information on personal data processed by the EUSurvey service itself, please click here.

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

*Name and surname

*Organisation

*Country
Please select the country

*Which community are you from?
Please select one answer
- CSIRT
- Law enforcement
- Both CSIRT and law enforcement (e.g. from CSIRT seconded to law enforcement or vice versa)
- Prosecutors
- Judges
- Other

GENERAL

1. What are the biggest challenges for the **CSIRT-LE** cooperation?

Please select one answer

- ○ Culture change
- ○ Technical
- ○ Legal
- ○ Procedural
- ○ Skillset discrepancies
- ○ Organizational
- ○ Other

2. What are the biggest challenges for the **CSIRT-Judiciary** cooperation?

Please select one answer

- ○ Culture change
- ○ Technical
- ○ Legal
- ○ Procedural
- ○ Skillset discrepancies
- ○ Organizational
- ○ Other

3. Do you think that a CSIRT-LE taxonomy should be based on:

Please select an order (1 - highest, 3 - lowest)

	1	2	3
LE constraints (legal, etc.)	○	○	○
CSIRT environment (vuln, etc.)	○	○	○
A mix of the two, without the vuln part	○	○	○

Fields marked with * are mandatory.

ORGANISATIONAL

4. What are the **four most significant** topics to address in a joint exercise, from a CSIRT/LE point of view?

at most 4 choice(s)

Select one or more answers

- ☐ Legal constraints on evidence collection
- ☐ Techniques used for the evidence collection
- ☐ Guaranteeing evidence integrity
- ☐ Investigations techniques (OSINT, seizes and searches results exploitation)
- ☐ Complementarities across the 3 communities in terms of duties and expertise (who does best what?)
- ☐ Investigation workflow (data flow across the 3 communities)
- ☐ Confidentiality management
- ☐ Information sharing management (installation, setup, taxonomy definition)
- ☐ Other

5. Do you think setting up regular sync **meeting** would be a good idea?

- ○ Yes
- ○ No

*Name and surname

*Organisation

6. In which **stage** of **the incident response life cycle**, the contribution of the CSIRT/LE/Judiciary would be helpful:

Please select one answer

- ○ Preparation
- ○ Detection and analysis
- ○ Evidence collection
- ○ Containment, eradication and recovery
- ○ Post-incident activity

7. Do you use any taxonomy/glossary that would support mutual understanding of the communities??

- ○ Yes
- ○ No

TECHNICAL

8. Do you use an **information-sharing tool**?

Please select one answer

- ○ Yes
- ○ No
- ○ No need to use such a tool

9. What are the **four most significant** qualities of an information-sharing tool?

at most 4 choice(s)

Select one or more answers

- ☐ Ease of use
- ☐ Sharing capabilities
- ☐ Investigations cross-checking
- ☐ Data quality and integrity
- ☐ Secure architecture - data security (in transit/at rest), role-based authentication etc.
- ☐ Integration with current tools, workflow tool, etc.
- ☐ Data analysis capabilities, visualisations
- ☐ Interoperability with existing systems across borders
- ☐ Having a single shared tool for the three communities
- ☐ Ability to share data with non-EU based LE/CSIRT entities
- ☐ Directly accepted by the judiciary for the purpose of prosecution or for criminal trial

Additional comments, if any

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

10. How the investigations are carried out? Which is the most common used **forensic technique**?

Please select one or more answers

- ☐ Memory forensics
- ☐ Network forensics
- ☐ Computer forensics
- ☐ Mobile forensics
- ☐ IoT forensics
- ☐ Digital forensics and OSINT (Twitter analysis, web crawling etc.)
- ☐ Digital forensics and Blockchain (Cryptocurrencies analysis tools etc.)
- ☐ TOR browser forensics (TOR network research, TOR nodes analysis etc.)
- ☐ Darknet forensics (Darknet website enumeration, Tools research (GPG tools, databases), etc.)
- ☐ Physical forensics (physical evidence)
- ☐ Other

11. What type of **digital evidence*** is the most commonly used (in a court)?

Please select one answer

- ○ Network data (internet)
- ○ Metadata
- ○ System files and system logs
- ○ Deleted files
- ○ Other

*Types of digital evidence based upon their source – volatile and non-volatile

12. What do you see as likely **future trends** in the area of **tools for cybercrime**?

Please select one or more answers

- ☐ Artificial Intelligence - AI
- ☐ Internet of Things - IoT
- ☐ Tor botnets
- ☐ New cryptocurrencies (non transparent, criminal-tailored)
- ☐ Other

13. What do you see as likely **future trends** in the area of **tools for attribution and investigation**?

Please select one or more answers

- ☐ Carrier Grade NAT - CGN
- ☐ Artificial Intelligence - AI
- ☐ Internet of Things - IoT
- ☐ Offensive investigations
- ☐ Automated surveillance of cybercriminal forum
- ☐ Big data for consolidating intelligence
- ☐ Other

14. Which are the **tools you use for evidence collection**?

14A. What are the key functionalities and the weakenesses of the tools you use for evidence collection

14B. What are the major weaknesses for these tools?

15. Which are the **tools you use for remediation**?

15A. What are the key functionalities of these tools?

15B. What are the major weaknesses for these tools?

16. Which are the **tools you use for coordination**?

16A. What are the key functionalities of these tools?

16B. What are the major weaknesses for these tools?

HUMAN

17. Do you think having CSIRT staff doing **internship or secondment** in police service would be a good idea?
- ○ Yes
- ○ No

18. What are the **main differences** between LE and CSIRT staff?

Please select one answer
- ○ Work's expectation
- ○ Skillset management
- ○ Personal KPIs
- ○ Working culture and behavior

LEGAL

19. Do you understand the term the "**Right to be Forgotten**"?
- ○ Yes, but I do not implement it
- ○ Yes, and I implement it
- ○ I am not aware of such a Right

20. With respect to these Directives and Regulations:
(1) Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)
(2) Regulation (EU) 2016/679 (General Data Protection Regulation)
(3) Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties:
- ○ I do not know any of these three legal acts
- ○ I know that these three legal acts exist, but I do not know the implications they have for my work
- ○ I know all three legal acts and I know the implications they have for my work
- ○ I know the existence and content of the following legal acts

21. In case you need to collect digital evidence, do you follow the **rules of Digital Forensics*?**
- ○ Yes
- ○ No
- ○ Sometimes
- ○ Other

*Please see OLAF forensics recommendations

22. Are there any **formal rules** (legal, internal policies, etc.) that regulate cooperation of your organisation with other communities (CSIRT/LE/JUD)?

- ☐ Legal framework
- ☐ Internal policies
- ☐ Other
- ☐ No formal rules in place

22A. What **kind of rules** should regulate the cooperation across the three communities (i.e. CSIRT/LE/JUD)?

Please select one or more answers

- ☐ EU legislation
- ☐ National legislation
- ☐ Memoranda/agreements between the communities
- ☐ Common soft-law
- ☐ Internal rules of each organization
- ☐ No need for an additional legal instrument
- ☐ Other

23. Do you think that **adoption of such rules** would improve the ability and motivation of your organization to cooperate with other communities?

- ○ Yes
- ○ No

24. Are you aware of a **EU cybersecurity certification framework** to come?

- ○ Yes
- ○ No

24A. How do you see the emerging EU cybersecurity certification framework influencing CSIRT/LE tools?

- ○ In terms of improved software
- ○ In terms of improved hardware
- ○ Greater assurance of forensics data
- ○ Mitigation of risk
- ○ Not aware of this framework

25. The digital evidence is collected based on the following **standards**:

Please select one or more answers

- ☐ ISO/IEC 27037:2012 - Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence
- ☐ ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems
- ☐ ISO 9000:2015 Quality Management Systems
- ☐ ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management
- ☐ Other

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

Thank you very much for your time and your input!

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

Submit

TP-03-20-124-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

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

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

enisa.europa.eu

ISBN: 978-92-9204-331-5
DOI: 10.2824/40199