EUROPEAN UNION AGENCY
FOR CYBERSECURITY

AN OVERVIEW ON ENHANCING TECHNICAL 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 www.enisa.europa.eu.

CONTACT

For contacting the authors please use team@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Alexandra Michota (ENISA), Andreas Mitrakas (ENISA), Dan Tofan, François Beauvois, Georgios Germanos, Gregoire Kourtis, Philip Anderson

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. In particular:

Maria Sanchez and other contributors from Europol EC3

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: 978-92-9204-342-1, DOI: 10.2824/13844

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As it has been stated in the Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2017, p. 13), “Finding useful information for cybercrime investigations, mostly in the form of digital traces, is a major challenge for law enforcement authorities”. Collaboration between Computer Security Incident Response Teams (CSIRTs) and Law Enforcement (LE) is the key to find such information and fighting cybercrime. A number of attacks that recently hit critical sectors brought about an increased level of cooperation, partly out of necessity; Wannacry (ENISA, 2017a) and ‘NotPetya’ (an updated version of Petya) attacks (Europol, 2017a) being the most recent examples.

As mentioned in the Council Note of 31 May 2017 Cybersecurity - Information from the Commission (Council, EU, 2017), “Conclusions drawn from the WannaCry attack include the need for CSIRTs, LE authorities and the private sector to work together and the need for LE authorities to have right tools to investigate these types of crimes and to prosecute criminals”.

The technical aspects, including tools and methodologies used, are an important component of the cooperation. This report aims to support the cooperation between CSIRTs - in particular, national and governmental, LE and the judiciary – in particular, prosecutors and judges, in their fight against cybercrime, by providing information on the technical aspects of the cooperation, identifying current shortcomings, and formulating and proposing recommendations to enhance their technical cooperation. Moreover, this report introduces some use cases to present the interaction among the different actors and the methodology and the tools used when CSIRTs, LE and the judiciary cooperate for responding to cybercrime.

The data for this report has been collected by means of desk research and an online survey.

The data collected identified a shared platform across CSIRTs, LE and the judiciary to be an effective solution to the technical challenges highlighted in previous ENISA reports. While designing the cooperation platform, there are important technical aspects that need to be considered. Interoperability, authentication of users and security of personal data are some of them. In addition, the platform should always be available, which is ensured at the level of technological infrastructure by various parameters such as network infrastructures that support its operation, software, hardware and durability - tolerance to risk factors such as power outages and natural disasters.

It is generally accepted that there is a reciprocal understanding of the needs between CSIRT and LE communities; however, information sharing between these communities occurs on an *ad-hoc* basis rather than in a systematic manner.

At this point, there are many international initiatives started, some at EU level and some outside the EU. Cross-sharing evidence seems to be on everyone’s agenda, although we all seem to be in very early stages.

There are plenty of tools available, belonging to different categories or having different features. Thus, a cooperation platform should be built taking into account the different functionalities and features of current tools and developments within the field

Core recommendations of this report on the development of a shared platform to improve cooperation between CSIRTs, LE and the judiciary include:

- ENISA and possibly EUROPOL EC3 and EUROJUST: to drive efforts towards the development of a **common platform**, considering all requirements and constraints expressed by the communities.
- CSIRTs, LE and the judiciary with the support of ENISA and possibly EUROPOL EC3 and EUROJUST: to work together towards a better **mutual understanding** of the **strengths, needs** and **limitations** of the three communities in relation to the sharing information.
- CSIRTs, LE and the judiciary with the support of ENISA and EUROPOL EC3: to facilitate the **sharing of experience** at strategic and operational cooperation.
- ENISA and possibly EUROPOL EC3 and EUROJUST: to promote the use of **Segregation (or separation) of Duties (SoD)** matrices to avoid overlapping duties across CSIRTs, LE and the judiciary in relation to the sharing information.
- CSIRTs, LE and the judiciary with the support of ENISA and EUROPOL EC3: to develop EU as well as national level requirements for their communities, on **what types of information** can be useful from their own perspectives, throughout the cybercrime investigation lifecycle.
- ENISA and possibly EUROPOL EC3 and EUROJUST: to consider and promote the adoption of a **common digital forensics framework** and CSIRTs and LE: to discuss and consider the adoption of it.
- ENISA and possibly EUROPOL EC3 and EUROJUST: to assess the suitability of **EU cybersecurity certification framework** for cybercrime investigation tools.

1. INTRODUCTION

1.1 PURPOSE

Collecting information on current cooperation across CSIRT, LE and the judiciary communities is a key step to enhance it. In 2019, the ENISA *Roadmap on the cooperation between CSIRTs and LE* (ENISA, 2019d) also highlighted the importance of the technical cooperation across the three communities; the purpose of this report is to better apprehend the technical aspects of the cooperation and challenges lying ahead.

This report analyses the tools used and tools required by various countries when cooperating in order to better manage the cybersecurity incidents, identifies the key technical challenges that prevent or limit effective cooperation, and looks for common tools through which cooperation can be strengthened and further enhanced.

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

1.2 BACKGROUND TO THE REPORT

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 LEA' has the goal to continue supporting the cooperation between the CSIRT and the law-enforcement communities and the extensions that this collaboration may have to the judiciary. (ENISA, 2018, p. 53).

This report is a continuation of 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 as project activities under Scenario 2.

1.3 REPORT OBJECTIVES AND SCOPE

1.3.1 Report objectives

The main objective of this report is:

- To support collaboration across CSIRTs, in particular, national and governmental, LE, prosecutors and judges.

1.3.2 Report scope

The report focuses on cooperation between national/governmental CSIRTs, LE and the judiciary, although most considerations made are largely applicable to CSIRTs in general (i.e. other than national/governmental CSIRTs).

The geographical coverage is limited to the EU (European Union, 2019) and EFTA (EFTA, n.d.)[1]. (See also (ENISA, 2015a). This does not mean however that all these countries are covered in the report and that no reference to other countries outside the EU and EFTA is made. Possible specific differences among the EU and EFTA, or between the EU and the United States, or the EU and Asia, also fall outside the scope of this report. This report does not seek to provide an exhaustive analysis, but rather focus on a small number of topics influencing

[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.

cooperation as it might become of interest for cross border investigations; hence, the geographic scoping is essential to remain limited to the EU only.

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

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

1.4 TARGET AUDIENCE

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

For the purposes of this report, 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 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, 2015b, p. 12) (ENISA, 2016b, p. 10). Governmental CSIRTs are teams whose constituency are the public administration networks (ENISA, 2015c);
- **Law enforcement (LE)**, police and police agencies are terms used in this report are synonymous and used to refer to police and police agencies, also used as synonymous. 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" (Council E. P., 2016c);
- **Judiciary** refers both to prosecutors and judges (a similar approach taken in (Council, EU, 2017). Prosecutor refers '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 LE and their interaction with the judiciary.

2. METHODOLOGY

2.1 DESK RESEARCH

Initially, desk research was conducted based on publicly available information sources, including ENISA publications.

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 online survey.

2.2 ONLINE SURVEY

An online survey was conducted to collect data to validate and further substantiate some findings. It was composed of 25 questions (see Annex D of the *Roadmap on the cooperation between CSIRTs and LE— Questions in the online survey* (ENISA, 2019d, p. 86)), 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 that is 'supported by the European Commission's ISA programme, which promotes interoperability solutions for European public administrations' (European Commission, n.d. b).

The invitation to complete the survey was disseminated via:

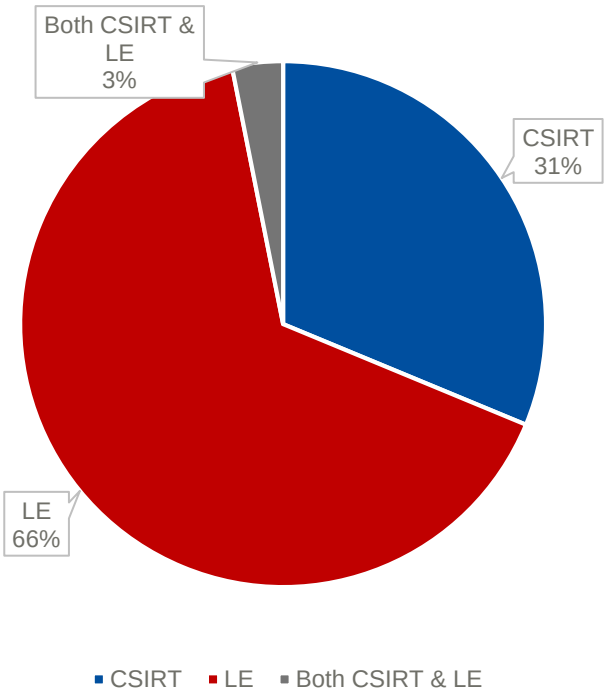
- A closed ENISA mailing list of European national and governmental CSIRTs.
- A Europol mailing list of the European Union Cybercrime Task Force (EUCTF), which is composed of the heads of the designated national cybercrime units throughout the EU Member States and Europol. The EUCTF[3] is an interagency group formed to allow the heads of National Cybercrime Units of EU member states, Iceland, Norway and Switzerland, along with representatives from Europol, CEPOL, the European Commission and Eurojust to discuss the strategic and operational issues related to cybercrime investigations and prosecutions within the EU and beyond (Council, EU, 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.

A total of 33 replies[4] were received, of these, 32 were from EU Member States (European Union, n.d.) and EFTA countries (EFTA, n.d.) and 1 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.

[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.

Figure 1: Overview of communities of respondents to the online survey



Of the 32 EU and EFTA respondents, 10 respondents were from the CSIRT community, 21 from the LE community and 1 belonged to both of these communities.

2.2.1 Data used to develop the recommendations

The recommendations in Chapter 6, have been developed based on research findings and the results of this report.

2.3 CONTRIBUTION BY SUBJECT MATTER EXPERTS

ENISA selected five external subject-matter experts from the list of NIS experts compiled following the ENISA CEI[5] (Ref. ENISA M-CEI-17-T01) (ENISA, n.d.).

Three of them contributed to this report by supporting the data collection and the drafting while two were reviewers. The two CEI experts contributing as reviewers reviewed this report in several rounds including the first draft in September 2019, an intermediate draft in early October 2019, and the final draft in late October 2019. They reviewed it in addition to ENISA reviewers and other external reviewers.

All five experts contributed ad personam.

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

[5] 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.

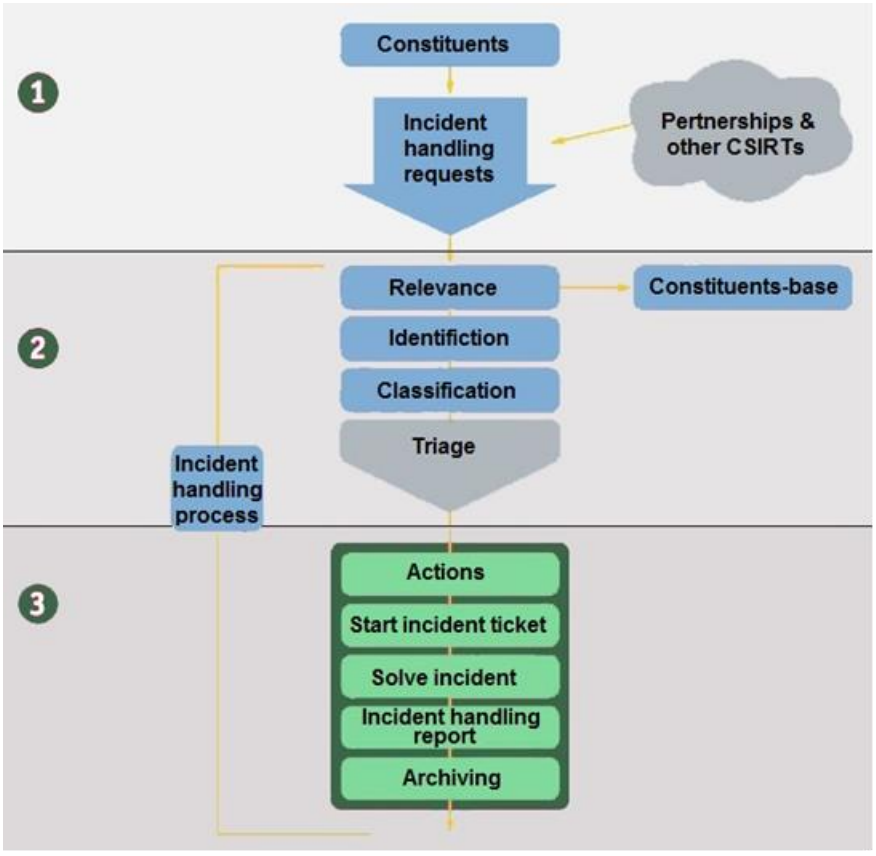
3. TOOLS USED IN THE CYBERCRIME INVESTIGATION LIFECYCLE

This chapter aims at outlining the similarities and differences of the most common and recognised tools used by CSIRTs and LE during the whole lifecycle of a cybercrime investigation. As the roles of CSIRTs and LE are not the same, some tools may be used by CSIRTs, some others from LE and some by both communities. The goal is to enumerate the main tools or tool categories/types used by both communities, at the same time providing as many examples as possible.

3.1 MAIN TOOLS USED IN CYBERCRIME INVESTIGATION LIFECYCLE

In general, the cycle of investigation starts when the authorities, CSIRTs, Law Enforcement Agencies (LEAs) or judicial authorities become aware that a cybersecurity incident or a cybercrime has taken place. This information may reach the authorities from multiple sources, e.g. a report from a victim (individual or representative of a legal entity), monitoring of online illegal activities by officials, information published on the media, information from CSIRTs or a LEA of another country, etc.

Figure 2: Incident handling process flow



Source: "ENISA Good Practice Guide for Incident Management": https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

A first responder, that may need to visit the 'crime scene', should take the appropriate measures to secure the scene, use appropriate tools and collect any available digital evidence, always following lawful procedures, according to the country's legislation (ENISA, 2019c).

After the first response, a thorough investigation needs to take place by an investigator, in order to get the full extent of the criminal activity, identify the victims, the damages and any losses, find the real identities of the perpetrators and any others involved in the crime. Tools for analysis and investigation are used in this phase.

To fully understand the crime that has been committed, the investigators firstly must collect information from multiple sources, e.g. interviews with the victim(s), requests to Internet Service Providers (ISPs), etc. They will possibly need to exchange information and cooperate with authorities from other countries, using tools for cooperation and secure communication. They may also need to deal with information in digital form, applying digital forensics techniques and tools in any seized equipment (e.g. collected during a search at a suspect's house). After all this information is collected, it must be analysed, so that the investigator identifies the perpetrator(s), based on the evidence.

The final step of the investigation is bringing the case to justice (if the action was taken by LE) or taking any other appropriate measures to remediate the incident (if any action was taken by CSIRTs), using specific tools for remediation.

The following sections, although not exclusive, outline the possible phases followed in an incident response/ cybercrime investigation (ENISA, 2010) (SANS, 2019), (CREST, 2019). In brief, the report will present:

- Tools for reporting;
- Tools for evidence collection;
- Tools for analysis and investigation;
- Tools for remediation;
- Tools for coordination and information sharing;
- Tools for secure communication.

3.2 TOOLS FOR REPORTING

Reporting is the first step within the cybercrime investigation lifecycle. CSIRTs and LE become aware, by different sources (open-source intelligence, monitoring services, reports of citizens, reports of IT administrator of companies etc.) of cybersecurity incidents that have taken place. It should be noted that not all cybersecurity incidents are cybercrimes (so LE do not need to be informed) and not all cybercrimes are considered cybersecurity incidents (so CSIRTs do not need to be informed). This means that CSIRTs and LE do not always have the same interest in incidents or investigations, which also affects the way they further handle each case.

Nevertheless, there are cases that may interest both CSIRTs and LE, so the need still exists for information exchange. Reporting is also important to avoid duplication of efforts and resources by CSIRTs and LE working on the same case (evidence collection, analysis, etc.). Reporting could be considered as part of the information sharing process.

Regarding the reporting to the judiciary, due to the role of the CSIRT community, direct reporting from CSIRTs to the judiciary is rare (ENISA, 2019a). It is generally accepted that there is communication, on the one side, between LE and the judiciary and, on the other side, between CSIRTs and LE. This means that there is an indirect communication between CSIRTs and the judiciary, via LEAs. CSIRTs typically support LE during the investigation of an alleged cybercrime. Cybersecurity incidents can be a source of illicit activities harbouring cybercrime.

The judicial authorities in several Member States direct the investigations for cybercrime.

From the answers provided by the participants in the online survey, there are no common tools for reporting and communication between CSIRTs and LE. The most traditional way of reporting is via email and telephone calls. Especially in urgent cases, direct contact between people is the most efficient way of communication. Secure communication channels are also of great importance and for this reason, largely PGP solutions are used.

A need for using a common language with terms that can be easily understood had been highlighted by the three communities (ENISA, 2017, p. 38); hence, a common taxonomy has been created, namely 'Common Taxonomy for Law Enforcement and The National Network of CSIRTs'[6], and it is used by CSIRTs, LE and the judiciary. The objective of the document created is to "support the CSIRTs and the public prosecutors in their dealing with LE in cases of criminal investigations, by providing a common taxonomy for the classification of incidents".

3.3 TOOLS FOR EVIDENCE COLLECTION

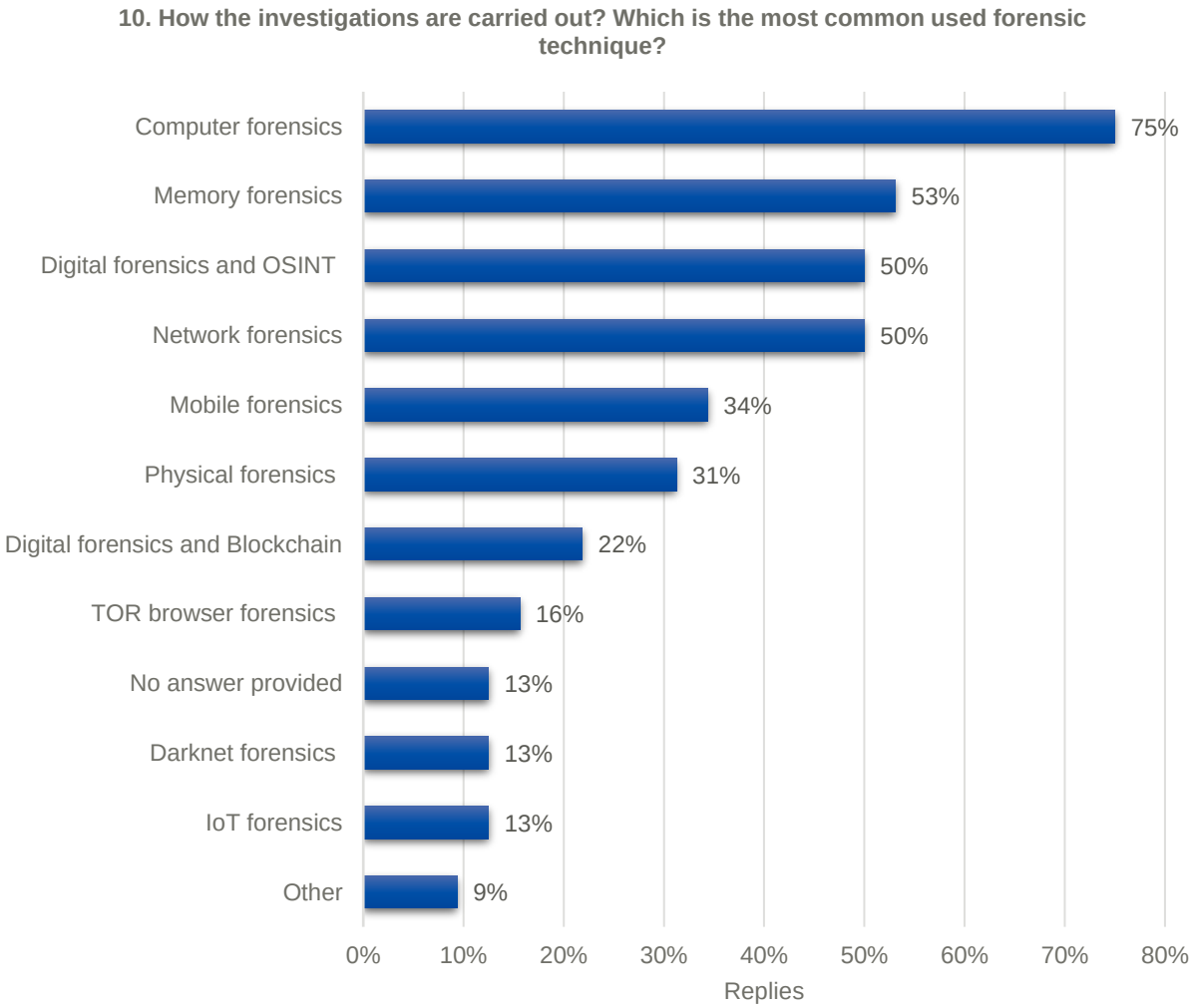
Evidence is perhaps the most important aspect of an investigation. Digital evidence has its own life cycle and digital forensics is an enormous modern scientific sector. CSIRTs, LE and the judiciary are interested in evidence collection, each community from their own standpoint. Evidence collection is important in order to identify, prosecute and convict criminals. LE handle and examine digital evidence with the purpose of further presenting their findings in court. On the contrary, CSIRTs' purpose when handling digital evidence is to identify the source of the cyber-attack, its effects and its consequences as fast as possible. Although evidence collection seems to be mostly a LE specific activity, CSIRTs can also offer assistance in this area.

According to the online survey results, various digital forensic techniques are used for collecting evidence; the most frequently used are the following:

- Memory forensics;
- Network forensics;
- Cloud forensics;
- Computer forensics;
- Mobile forensics;
- IoT forensics;
- OSINT (Twitter analysis, web crawling 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).

[6] https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts

Figure 3: Replies to Question 10 of the online survey



For the above-mentioned techniques, the respondents identified the use of several different tools either commercial or free or open-source or developed in-house. The major issue with evidence collection is the admissibility in criminal prosecutions. This means that someone can collect evidence using many different tools, simple or more complicated, commercial or open-source. It is important, though, especially for LE to collect evidence that will be admissible to the judicial procedures and in front of a court. From a CSIRT perspective, what is of great importance is the timing to collect evidence, so any tool can be used, even those developed in-house if it supports the normal activities of a CSIRT.

Some weaknesses of such tools have been highlighted by the participants of the online survey and are presented below:

- Slow speed of tools: this is also related to the evolution of disc/memory spaces;
- Rapid growth of tools: this means that tools get outdated very quickly;
- High cost of commercial tools: this could be an issue for certain LEAs, and need to be addressed by the seller;
- Limited options and functionalities of some tools: in addition to that, not all the tools support all the operating systems.

3.4 TOOLS FOR ANALYSIS AND INVESTIGATION

On the one hand, LE investigate cybercrime in order to identify the people who are involved in criminal activities and bring them to justice. Once evidence is collected, it must be analysed to provide useful information or intelligence for LE and prosecution authorities. On the other hand, CSIRTs analyse the evidence for the purpose of mitigating cyber threats and protecting the infrastructure and data of an organisation.

The analysis is performed based on the evidence collected. There are traditional analysis techniques and tools that can be used by analysts during an investigation of any type of crime. During the analysis phase, the analyst looks for relationships among entities, sequences of events, movement of money, narcotics, stolen goods or other commodities, activities involved in a criminal operation, etc.

According to the respondents, for analysis purposes, both commercial and open-source tools can be used as well as the skills of investigators and analysts.

Investigation techniques include not only data analysis but also several other traditional LE methods, such as interviewing of victims and suspects, undercover surveillance, access to non-public sources of information and more.

There are certain trends that seem to affect investigation and identification that have been identified as challenges by several organisations in the online survey:

- The analysis of “big data” by the LE is not considered an easy task; it is often time-consuming and requires specific knowledge;
- The Carrier-grade NAT (CGN)[7] technology also makes it difficult for LE to reveal the identity of criminals, as several users are hidden behind the same IP address;
- The Internet of Things (IoT) is an issue discussed mainly because forensic analysis of IoT devices is not a straightforward task in most cases;
- Artificial Intelligence (AI) offers an automated analysis that can be performed by LEAs, but this approach raises legal, ethical and technological issues.
- Analysis of cryptocurrencies transactions, which is fundamental for identifying the money flow, is often related to online criminal activities. Many online services exist that offer mixing and obfuscation services, making it difficult for LEAs to trace users behind digital wallets.

3.5 TOOLS FOR REMEDIATION

Remediation is a highly complex activity, with the purpose of restoring the systems and services damaged during an attack/incident.

The respondents from LEAs in the online survey did not indicate that restoration/remediation is part of their duty. Most of them mentioned that they focus mainly on the evidence collection phase.

CSIRT respondents indicated that systems recovery is part of their post-incident duties. Responses did not indicate clearly defined tools or activities, but merely that some national CSIRTs can perform such activities as coordinators or consultants.

Important aspects to be considered regarding remediation:

[7] 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

- Remediation operations are specific per each system. Only the owner of a system can choose the appropriate tools and activities for remediation, depending on the specificities of the environment.
- Remediation is usually an activity within a bigger domain called “Business Continuity and Disaster Recovery”. It involves many prerequisites to be in place, specific procedures, tools and people.
- Choosing the right tools to perform remediation depends on the environment that must be restored. There are different types of data backup (e.g. cloud, on-site, Redundant Array of Independent Disks - RAID, tapes etc.).
- National CSIRTs might be involved in coordination activities as regards remediation; they might need to be actively involved only when they manage the systems or have in-depth experience in certain technologies.
- Nobody, within the respondents, indicated specific tools to be used in the remediation phase.

3.6 TOOLS FOR COORDINATION (AND INFORMATION SHARING)

Due to the borderless nature of cybercrime and cybersecurity incidents, the same incident may affect several countries. In such cases, it is important for CSIRTs and LEAs of different countries to be able to work together on the same cases, exchange information and take coordinated actions, according to their mandates.

Within the LE community and specifically in the field of cybercrime, cooperation among LEAs of the EU Member States and a few Third countries takes place through Europol, the European Cybercrime Centre and in major cases through the Joint Cyber-crime Action Taskforce (J-CAT)[8].

Europol’s position at the heart of the European security governance system allows it to serve as a:

- support centre for law enforcement operations;
- a hub for information on criminal activities;
- centre for law enforcement expertise.

Europol also supports the law enforcement activities of the Member States through a network of liaison officers. This network consists of liaison officers who are responsible for facilitating the exchange of information between the Member States; each liaison officer represents his/her Member States. In this way, messages and requests from one country to another are sent through the liaison bureau.

The European Cybercrime Centre (EC3)[9] was set up “to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime”. EC3 has been involved in tens of high-profile operations. One big innovation that took place within the EC3 is the establishment of the J-CAT. “J-CAT’s objective is to drive intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the joint identification, prioritisation, preparation and initiation of cross-border investigations and operations by its partners.”[10]

[8] https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce
[9] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[10] https://www.europol.europa.eu/

Another mechanism for coordinating actions during major cyberattacks against information systems is the "Law Enforcement – Emergency Response Protocol (LE ERP)". The LE ERP has been recognised by the EU Council and the Member States as one of the key mechanisms at EU level providing an EU coordinated response to large-scale cybersecurity incidents and crises[11]. LE ERP includes setting up Europol's Virtual Command Post, a secure communication channel to facilitate real-time critical communications and on a need-to-know basis with the different stakeholder groups.

It should be also noted that according to the Directive on Attacks against Information Systems 2013/40/EU[12] and the Council of Europe's Convention on Cyber-crime[13], networks of 24/7 contact points have been established, so that direct communication and information exchange can take place among relevant LEAs of Member States in cases of attacks against information systems, but also several types of cybercrime.

Coordination plays an important role in incident response. Most often cybercrime cases or cybersecurity incidents have a cross-border dimension, meaning that there is a need for a certain level of coordination. CSIRTs usually take the lead in collecting large amounts of data related to malicious activities, a part of which could end up in LE related investigations that later will lead to the identification and incrimination of culprits.

The path to incrimination is challenging, according to a study published by Third Way on their website[14]; less than 1% of cybercrimes in the United States see an enforcement action taken against the attackers. In addition, for that 1%, there is immense cooperation and coordination effort in place.

In recent years, many successful takedown operations have taken place as a result of the cooperation across CSIRTs, LE and private sector players[15].

The online survey responses indicate a basic level of cooperation taking place between CSIRTs and LE, but mostly with regular tools such as phone or email.

There are clear signs of cooperation within communities, but not necessarily among communities. For example, the majority of CSIRTs across the EU are using the same tools such as a Request Tracker for Incident Response (RTIR)[16] ticketing system (Hall, 2015), Malware Information Sharing Platform (MISP)[17] or other similar malware information-sharing platforms, messaging, email clients, etc.

The CSIRT community is also supported by EU level initiatives, such as the CSIRTs network established by the NIS Directive (ENISA, 2016), Trusted Introducer and the specific activities that ENISA has supported over the last years. A common technical platform for cooperation and exchange of information is also under development (MeliCERTes[18]).

Survey responses suggest that the members of the CSIRT community have more skills and resources to develop in-house applications. Several tools mentioned by the respondents are

[11] Draft Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises,10085/18, 19 June 2018.
[12] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040
[13] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[14] https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors
[15] https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation
[16] https://bestpractical.com/rtir
[17] https://www.misp-project.org/
[18] https://ec.europa.eu/digital-single-market/en/news/call-tender-advance-melicertes-facility-used-csirts-eu-cooperate-and-exchange-information

developed by members of the CSIRT community. In addition, they intensely rely on open-source software. On the other side, LE use mainly commercial tools but they can also rely on tools developed by the CSIRT community.

The LE community presents similar signs of inter-member cooperation. Survey responses indicate, in general, that LEAs across the EU use mainly similar tools and do make use of the cooperation mechanisms put in place at EU level. There is a strong level of cooperation and coordination at EU level through EUROPOL, that hosts some EU wide available cooperation tools (e.g. SIENA[19], SIRIUS [20]). EUROPOL also established EC3 to "strengthen the law enforcement response to cyber-crime in the EU"[21].

However, the online survey responses do not indicate the use of advanced coordination tools between the two communities. Cooperation does take place, but only basic tools such as email and telephone are used. There are though, several examples where well-established cooperation mechanisms and tools are put in place.

One is in the UK, where the National Crime Agency (NCA) and the National Cyber Security Centre (NCSC) are tasked with responding to different aspects of cyber-attacks[22]. In this respect, NCA investigates the most serious and complex attacks affecting the UK while NCSC protects critical services from cyber-attacks. According to the source, this model was tested "during the WannaCry attack in which the NCA led the criminal investigation, while the NCSC developed advice on limiting damage, protecting uninfected computers, and establishing the scale of the incident". The online survey replies identify NSCS using several internal cooperation tools developed by the NCA.

Based on the interviews conducted for preparing the *Roadmap on the cooperation between CSIRTs and LE* (ENISA, 2019d), the Malta Police Force - Cyber Crime Unit[23], is currently working on a project for implementing MISP and other information-sharing platforms between CSIRT and LEAs.

The Belgium Federal Computer Crime Unit also mentioned that they are using a coordination tool developed by their national CSIRT.

The French National Police created a CSIRT for supporting investigation. As a full member of the French CSIRT community and TF-CSIRTs Network, it shares information directly with CSIRTs by using a MISP.

Some coordination tools used by the CSIRT community are the following:

- Incident response ticketing systems - RTIR;
- Messaging platforms – Mattermost[24], Threema[25];
- Software to structure information – Taranis[26];
- Collecting and processing security feeds (such as log files) – IntelMQ[27].

[19] https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena
[20] https://www.europol.europa.eu/newsroom/news/europol-launches-sirius-platform-to-facilitate-online-investigations
[21] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[22] https://www.computerweekly.com/news/450430399/UK-cyber-defenders-set-to-build-on-existing-capability
[23] https://pulizija.gov.mt/en/police-force/police-sections/Pages/Cyber-Crime-Unit.aspx
[24] https://mattermost.com
[25] https://threema.ch/en
[26] https://github.com/NCSC-NL/taranis3/wiki
[27] https://github.com/certtools/intelmq

Among others, two coordination tools used by the LE community are the following:

- Secure information exchange network application – SIENA;
- A platform for facilitating online investigations – SIRIUS.

3.7 TOOLS FOR SECURE COMMUNICATION

When dealing with cybercrime, secure communication is of the highest importance. The processing and sharing of sensitive data require appropriate protection.

Section 4.2.1 of the ENISA report *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement* (ENISA, 2017, p. 28) provides more insights into the types of tools used by each community.

The most significant tool that is used for information exchange among LEAs in different countries is Europol's SIENA. SIENA ensures the secure exchange of sensitive and restricted information among LE of Member States.

Other than the above, the organisations make use of encrypted emails to communicate between themselves.

The online survey did not reveal any serious progress in this area as the CSIRT community continues to use OpenPGP[28] besides other protocols that provide end-to-end encryption over the network, such as Transport Secure Layer (TLS). Tools enumerated in the previous subchapter also provide certain levels of security.

It is worthwhile to mention the MeliCERTes platform, serving as a network for establishing confidence and trust among the national CSIRTs of the Member States and for promoting swift and effective operational cooperation. A modular platform that interlaces various services that not only offers a complete security incident management solution but also allows CSIRTs to share information and collaborate with each other within verified trust circles. Each module specialises in a task essential to security incident management[29].

In some cases, LE rely on secure email services, while in the few cases where using CSIRT powered tools, they rely on the security provided by the developers. EU level cooperation platforms, hosted by Europol, offer adequate levels of protection, but can only be used for "LE to LE" type of cooperation.

[28] https://www.openpgp.org/about/
[29] https://github.com/melicertes/csp

4. REGULATORY REQUIREMENTS

4.1 REGULATORY REQUIREMENTS FOR USING TOOLS DURING INVESTIGATIONS

This subchapter examines different types of restrictions/constraints that CSIRTs and LEAs might have when using specific tools. Currently criminal investigations may also have a digital dimension. The many ways information technology impacts our lives have also influenced the way criminal investigations are conducted. Over the last decade, the use of digital evidence in the LE and justice sector has encountered an exponential increase in Europe. Digital evidence has become important not only for cybercrime but for all sorts of crimes.

In some cases, the use of tools might be influenced/ restrained by different national or international regulatory frameworks.

The authors of *Handling and Exchanging Electronic Evidence Across Europe*, (Biasiotti M. J., 2018) provide useful insights on how digital evidence is currently handled in the EU. They mention that although Member States might have in place-varied legislation that regulates the collection and handling of digital evidence, there are two elements that must be guaranteed in any case, that is relevance and authenticity. Nevertheless, these requirements are difficult to be met due to some peculiar characteristics of digital evidence, namely fragility and immateriality (difficult to associate with physical objects). That is why the "chain of custody" becomes very important. A proper chain of custody should contain details on how the digital evidence was handled from the moment collected until presented in court.

At European level, there is still neither a unified legal framework nor shared rules that make it possible to handle digital evidence and its possible exchange in a uniform manner across Member States". At international level, the Council of Europe Convention on cybercrime (Council of Europe, 2001), often referred to as the 'Budapest Convention', is the first and most relevant international treaty on cybercrime and electronic evidence.

At EU level, the European Commission has submitted a proposal for a regulation on production and preservation for electronic evidence in criminal matters[30]. Within the Impact Assessment[31], that preceded the above proposal, it is clearly mentioned that "some crimes cannot be effectively investigated and prosecuted in the EU because of legal constraints in cross-border access to electronic evidence".

In the same light, the European Commission proposed on 5 February 2019 to start international negotiations on cross-border access to electronic evidence, necessary to track down dangerous criminals and terrorists. This initiative is called "E-evidence - cross-border access to electronic evidence[32]" and aims to ensure that the Second Additional Protocol (under negotiation) to the Council of Europe "Budapest" Convention on Cybercrime is compatible with EU law, as well as the proposed EU rules on cross-border access to electronic evidence.

Significant progress has been done in this area, as problems have been identified and actions have been proposed. Nevertheless, it will take some time until the real impact will be assessed at Member States level.

[30] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN
[31] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN
[32] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

Useful conclusions and recommendations are also provided in:

- EU Council conclusions on improving criminal justice in cyberspace, 9 June 2016[33];
- European Informatics Data Exchange Framework for Courts and Evidence[34] - (EVIDENCE), the EU CORDIS project that aimed at creating a Common European Framework for the correct and harmonised handling of electronic evidence during its entire life cycle; among the outstanding results of the project we can enumerate The Digital Forensics Tools Catalogue[35] and The Electronic Evidence Categorisation Tool.

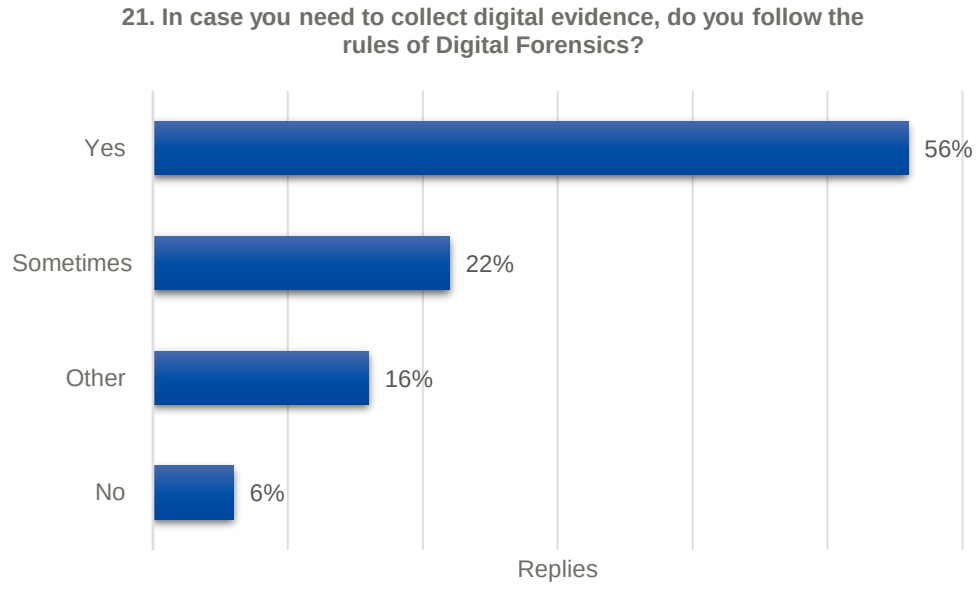
In the US, National Institute of Standards and Technology - NIST has developed a Computer Forensics Tool Testing Program (CFTT)[36], to "establish a methodology for testing computer forensic software tools by developing general tool specifications, test procedures, test criteria, test sets, and test hardware" to ensure their reliability; a catalogue of tools is provided by NIST (NIST, 2019).

As regards the admissibility of evidence in court, progress still needs to be done not only at EU but also at international level; standards that provide guidelines related to the evidence collection process and forensic methods are also required.

Figure 4 depicts that the communities identify the need of following digital forensic rules when evidence is collected. 56% of the online survey participants replied that they follow a set of digital forensic rules during the evidence collection phase, while 6% replied that they have not identified such a need. Some respondents also indicated some specific frameworks.

Following forensic rules when collecting evidence does not guarantee the admissibility of evidence in criminal proceedings. However, the development and adoption of a common framework of digital forensic rules could increase the likelihood of evidence admissibility in court; this could be beneficial for the communities.

Figure 4: Replies to Question 21 of the online survey



[33] https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf
[34] https://cordis.europa.eu/project/rcn/185514/reporting/en
[35] https://www.dftoolscatalogue.eu/dftc.home.php
[36] https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

4.2 THE IMPACT OF CURRENT REGULATORY DEVELOPMENTS

Recent EU level regulatory developments have a clear impact upon any type of digital data processing. Any proposed platform needs to comply with existing and forthcoming legislation at national, European and international level. Characteristic examples are the EU General Data Protection Regulation (Regulation EU 679/2016 (Council E. P., 2016a)), the Network and Information Security Directive, also known as NIS Directive, (Directive EU 2016/1148 (Council E. P., 2016b)), the E-evidence framework (European Commission, n.d, a), the EU Cybersecurity Certification framework (European Commission, n.d., b) and more.

4.2.1 GDPR Implications on the use of different tools

The new EU General Data Protection Regulation was adopted on the 24th of May 2016 and entered into force on the 25th of May 2018. The objective of the regulation is the "protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data".

The GDPR underlines seven key principles that must be respected by those processing personal data:

- Lawfulness, fairness and transparency: these three core principles are referring to processor/controller being honest and respecting the regulation.
- Purpose limitation: the data must be collected for specified, explicit and legitimate purposes.
- Data minimisation: the volume of data collected should be limited to what is necessary to fulfil the purposes for which they are processed.
- Accuracy: The data must be accurate and kept up to date.
- Storage limitation: the data must be stored only for the time period that is strictly necessary in relation to the purpose for which they were collected.
- Integrity and confidentiality: this is clearly a requirement for security of processing. Among others, data should be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. This should be achieved by using appropriate technical or organisational measures.
- Accountability: this principles defines that the controller and the processor shall be responsible for, and be able to demonstrate compliance with, all the above.

Article 6 of the regulation deals with the lawfulness of processing, mainly stating that there must be a legal basis for the processing, either being a legal obligation, legitimate interest, explicit consent, or another basis, as explained in the article.

Another important aspect of the GDPR is that it requires the implementation of "privacy by design" and "privacy by default" principles. This means that controllers and processors must put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights.

Article 2, par.2 (d) of the GDPR stipulates that the regulation does not apply to the processing of personal data "*by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".* As the GDPR does not apply in these cases, a more specific legislative document was adopted in parallel with the GDPR, the Directive (EU) 2016/680 on the protection of natural persons regarding the processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data, which also entered into force on May 25th 2018.

The Directive is designed to protect citizens' fundamental right to data protection when personal data is processed by law enforcement authorities for law enforcement purposes. The Directive is expected to facilitate cross-border cooperation in the fight against crime and terrorism.

This practically means that LEAs that use tools to process personal data have to do so lawfully, fairly, and only for a specific purpose, always linked to the fight against crime.

Police and criminal justice authorities are obliged to apply the principles of data protection by design and data protection by default at the beginning of any personal data processing. When developing applications, criteria definition needs to be developed first by both communities.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever the processing of personal data takes place: consent, performance of a contract, legal obligation, vital interests, public task or legitimate interest. Fairness means that handling of personal data should take place only in ways that people would reasonably expect, and they should not be used in ways that have unjustified adverse effects on the individual. Transparent processing is about being clear, open and honest with people from the start about who the data controller and processors are, and how and why they use personal data. [37]

Additionally, the Directive provides that processing of personal data by these bodies will fall under the control of Independent Supervisory Authorities; however certain exceptions are introduced for the judiciary, as Article 45 par. 2 of the Directive stipulates that "*Each Member State shall provide for each supervisory authority not to be competent for the supervision of processing operations of courts when acting in their judicial capacity*".

Nevertheless, CSIRTs do not fall into the same category, as they are considered data controllers/processors, as their operations are regulated by the GDPR and not like LE by the 2016/680 Directive[38]. Notably, recital 49 of the GDPR provides that the processing of personal data "for the purposes of ensuring network and information security […] by computer security incident response teams (CSIRTs) constitutes a legitimate interest of the data controller concerned".

The provisions of recital 50[39] could also provide a legal basis for personal data processing, through national laws, for certain CSIRTs constituencies (e.g. national, governmental): "*if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member state law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful*". CSIRTs must be very careful, as the principles stated above also apply to them. Transparency and accountability along with the "right to be forgotten" are important, as a data subject may request access to its data, or even deletion. Therefore, appropriate measures should be in place to handle these requests by "locating" the data stored and processed through different CSIRT tools. When dealing with attacks, the temptation of collecting too much data should be avoided. Storage limitation should also be applied, and data removed after some time has passed.

There are significant challenges in cybersecurity, such as threat intelligence that is a service that needs huge amounts of data, collected over many years, in some cases. Data maximisation is rather applied to what is collected, as in aggregating any information that could be relevant as

[37] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/
[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680
[39] http://www.privacy-regulation.eu/en/recital-50-GDPR.html

an input. Furthermore, access to certain useful online services, such as WHOIS, have been restricted due to privacy concerns.

Considering the above, further clarifications are needed as regards the lawful operation of CSIRTs under GDPR. National CSIRTs can further analyse data protection issues, covering also other types of CSIRT services that might be offered within their countries. Considerations of using common platforms and data transfer tools among different countries should also be made. The EU data protection framework, in particular, the GDPR and LE DP Directive, impose specific restrictions to CSIRTs and LE also when sharing data with international organisations and onwards with third countries. Sharing with non-EU countries requires an adequate level of data protection. This could require CSIRTs and LE to revisit their framework of sharing information with corresponding authorities of third countries.

4.2.2 NIS Directive and its implications on the use of tools

The EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, known also as the NIS Directive, is the first piece of EU-wide cybersecurity legislation (Council E. P., 2016b). The goal is to enhance cybersecurity across the EU, through enhancing national capabilities, cross-border cooperation and national supervision of critical sectors (ENISA, 2016).

Among other things, the NIS Directive established an EU wide cooperation framework for national CSIRTs (the CSIRTs Network). Between the tasks attributed to the group are coordination and exchange of information as regards incidents.

What had been done at EU level through informal groups is now done officially through the CSIRTs Network. The group already has periodic meetings, supported by ENISA.

Along with the adoption of the NIS Directive, there is also a notable technical development, namely MeliCERTes, a facility used by the CSIRTs in the EU to cooperate and exchange information. ENISA will oversee operating the central aspects of the MeliCERTes facility and will support the operation of the EU CSIRTs Network. National CSIRTs have also been allocated EU funds, to develop national technical platforms, able to integrate with MeliCERTes.

The conclusion is that soon, the EU CSIRT community will have all the necessary tools to cooperate properly among themselves.

Along with the NIS Directive, new legislation has been adopted in all Member States, strengthening the role of the national CSIRT or similar institutions. Every Member State will now have a stronger national CSIRT and a cyber supervisory scheme covering at least seven essential industries (energy, banking and financial markets, transport, water, health, digital operators).

Tools used within this area need to focus more on cooperation and be able to facilitate secure data exchange among many peers. National CSIRTs should be able to perform analyses at industry level, but also at national level and to cooperate with other CSIRTs across the EU. New tools, such as MeliCERTes, must be able to support this exponential growth in the number of cooperating parties, and sources of information.

However, the NIS Directive does not put too much emphasis on cooperation with LE and the judiciary. Besides the demand for “consult and cooperate” with LEAs, expressed in Art. 8, no other parts of the NIS Directive mention such initiatives. The NIS Directive supports the delivery of secure and dependable essential services to to EU citizens.

Therefore, this is still a grey area and the questions remain, such as how a fully developed CSIRT community, equipped with tools and a proper cooperation framework, can also contribute to the cybercrime investigation lifecycle, by serving LE and the judiciary with the proper data to identify and incriminate responsible persons.

4.2.3 The role of the cybersecurity certification framework

The EU Cybersecurity Act (Regulation EU 2019/881 (Council E. P., 2019)) establishes an EU certification framework for information and communication technology (ICT) digital products, services and processes, which enables the creation of EU certification schemes. Although several security certification schemes exist in the EU for ICT products, measuring the security and trust of these products, these are not based on a common framework. After massive cyberattacks e.g. ransomware cases, the need for providing rated assurance level has also been highlighted in the area of cybercrime investigation as various tools are used in all cybercrime investigation lifecycle phases.

The new framework will provide a set of rules, technical requirements, standards and procedures so that security and trust of products could be measured. Users and service providers alike will be able to determine the level of security assurance of the products, services and processes they procure, make available or use.

In particular, each European scheme should specify:

- the categories of products and services covered;
- the cybersecurity requirements, for example by reference to standards or technical specifications;
- the type of evaluation (e.g. self-assessment or third-party evaluation);
- the intended level of assurance (e.g. basic, substantial and/or high).

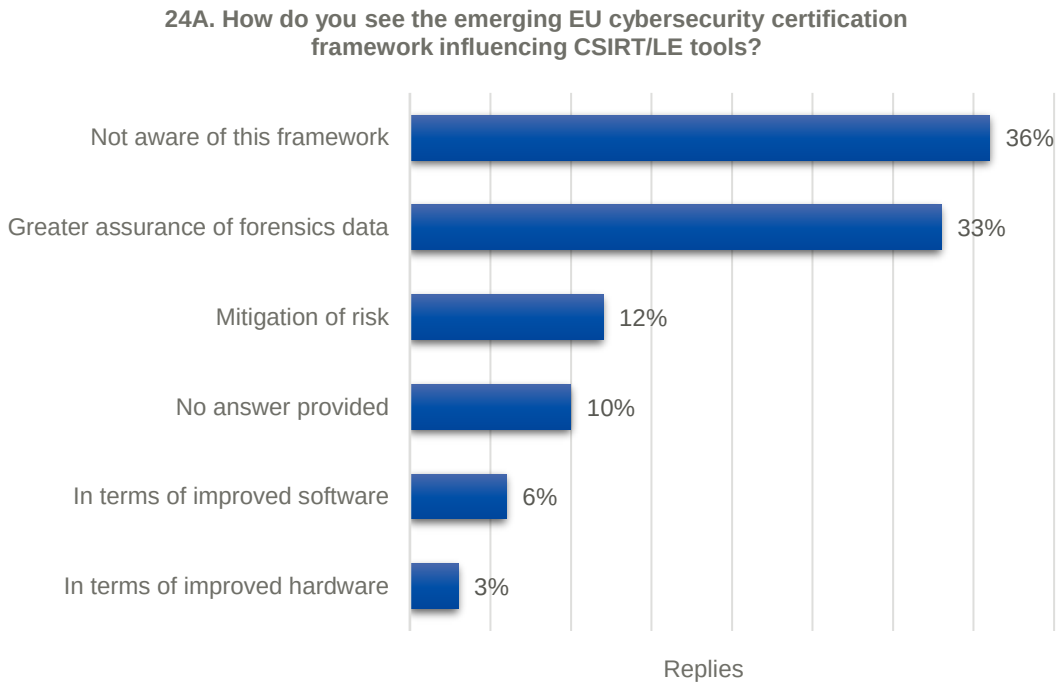
To describe the cybersecurity risk, a certificate may refer to three assurance levels that result from estimating the level of risk in relation to the intended use of the product, service or process (focusing on probability and impact of an incident). The resulting certificate will be recognised in all EU Member States, making trade easier across different countries.

For instance, evidence management is the key part of a cybercrime investigation and prosecution. The increasing requirement of storing, preserving, sharing and managing various forms of digital records used as evidence in a criminal court highlights the need for using tools that can provide assurance that the data is trustworthy, accurate, complete, secure and subsequently admissible in a court for prosecuting the suspect.

It is expected that all the tools used by CSIRTs and LE during the cybercrime investigation lifecycle for collecting evidence, analysing data, investigating cases, communicating etc. will need to fulfil the requirements set up by a certification scheme.

55% of the online survey participants replied that they are aware of the emerging EU cybersecurity certification framework. Figure 6 depicts how the Member States see the impact that EU cybersecurity certification may have on the use of CSIRT/LE tools provided throughout the cybercrime investigation lifecycle. 54% of the participants see that the security certification framework will have positive impact on the technical cooperation across the three communities; in particular, 33% of the respondents consider that the EU cybersecurity certification framework will provide greater assurance of the forensics data, 12% replied that it will mitigate various risks that arise during a cybercrime investigation case, while 6% claim that this framework may improve the tools in terms of software and 3% in terms of hardware.

Figure 5: Replies to question 24A of the online survey



4.2.4 Standards and certifications available

There are several useful best-practice standards for implementing effective cybersecurity. These standards also cover the use of tools and techniques within an organisation. Therefore, it is important to understand the role that each standard fulfils, its scope and how it is combined with other standards.

Certification plays a critical role in increasing trust and security for different products and services, within communities, and refers to the confirmation of certain characteristics of a product or service. This can only be beneficial to the EU internal market, as it improves the functioning conditions by increasing the level of security. The purpose of the Cybersecurity Certification Framework is to establish an EU level scheme to attest that the evaluated ICT products, services and processes and comply with specified security requirements for the purpose of assuring cybersecurity. The CSIRTs, LE and the judiciary can surely find the new framework as a fit for purpose.

Cybersecurity standards are generally applicable to all organisations no matter what their size is or the industry/sector they represent. Several people need to work together to develop a standard, at European level ETSI[40] and CEN-CENELEC[41] guidelines are followed; while at international level, people follow the guidelines provided by ISO/IEC standards.

Concerning the international-level cases, the people who are working together aiming to develop a new standard are independent technical experts nominated by ISO members, for specific subject areas. The standard development workflow is as follows: they begin the process with the development of a draft that meets a specific market need; then, this is shared for commenting and further discussion. The voting process is the key to consensus. If that is

[40] https://www.etsi.org/standards/types-of-standards
[41] https://www.cencenelec.eu/STANDARDS/Pages/default.aspx

achieved, then the draft is on its way to becoming an ISO standard. If an agreement is not reached, then the draft will be modified further and voted on again[42].

ISO/IEC 27001 is the international standard for best practice Information Security Management Systems (ISMS). Its main scope is the protection and preservation of information under the principles of confidentiality, integrity and availability. The standard offers a set of best-practice controls that can be applied to an organisation based on the risks it faces and implemented in a structured manner in order to achieve externally assessed and certified compliance[43].

ISO/IEC 27032 is the international standard that focuses on cybersecurity. The standard provides guidance for improving the state of cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

- information security;
- network security;
- internet security;
- critical information infrastructure protection (CIIP)[44].

ISO/IEC 27035 is the international standard for incident management. Incident management forms the crucial first stage of cyber resilience. This standard also includes guidance for updating policies and processes to strengthen existing controls following analysis of the event and minimise the risk of recurrence[45].

ISO/IEC 27031 is the international standard for ICT readiness for business continuity. The standard describes the key concepts and principles of ICT readiness for business continuity and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity[46].

ISO/IEC 22301 is the international standard for business continuity management systems and forms the final part of cyber resilience. The standard specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise[47].

The Cloud Security Alliance's Cloud Controls Matrix (CCM) is a set of controls designed to maximise the security of information for organisations that take advantage of Cloud technologies[48].

The NIST Cybersecurity Framework (NIST CSF) "provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes". In particular, NIST CSF provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber-attacks.

[42] https://www.iso.org/developing-standards.html
[43] https://www.iso.org/isoiec-27001-information-security.html
[44] https://www.iso.org/standard/44375.html
[45] https://www.iso.org/standard/44379.html
[46] https://www.iso.org/standard/44374.html
[47] https://www.iso.org/standard/50038.html
[48] https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/

5. CONSIDERATION OF REQUIREMENTS FOR A SHARED PLATFORM

As the main objective of this report is to streamline cooperation between the communities, there are different types of requirements that must be considered when using such tools or proposing initiatives in this area.

5.1 COMPONENTS

The concept of "people, process and technology" has been the cornerstone Information Technology Infrastructure Library - ITIL[49] for many years. These parts are considered the keys to successful project implementation and organizational change. In other words, for a new cooperation platform to be successful and operational, an approach that optimises the relationships between the three is required.

- **People:** It is necessary to identify the key role players from the CSIRT, LE and the judiciary communities and understand how each of them can contribute in the fight against cybercrime. The aim is to highlight conflicting or overlapping duties performed by one community or more. CSIRTs, LE and the judiciary should identify the key responsibilities for their communities and then link them with the skills required to fulfil these duties.
- **Process:** The suitable processes in order for an advanced collaboration platform to be successful need to be defined. Then, process variations, exceptions, interdependencies and supporting processes should also be considered. The three communities have to review these processes, make sure that they understand what is expected from each party and express their concerns for any possible gaps or other issues.
- **Technology:** This part should be the final consideration once the issue is clearly understood and the solution requirements have been clearly defined. Technology will cover the needs that people and processes require, but not vice versa. Careful consideration needs to be given to the automated integration with other existing platforms.

5.2 GENERAL FEATURES

As identified throughout this study, a shared platform across CSIRTs, LE and the judiciary seems to be an effective solution to the technical challenges highlighted in previous ENISA reports (ENISA, 2019a). While designing the cooperation platform, there are important technical aspects that need to be considered. Interoperability, authentication of users and security of personal data are some of them. A significant aspect that also needs to be considered is the platform availability, which is ensured at the level of technological infrastructure by various

FEATURES

Usability, accessibility (Role-Based Access Control- RBAC model), secure architecture - data security (in transit/at rest); security by design and by default, integration with current tools, workflow tool, etc. Interoperability with existing systems across borders, Ability to share data with non-EU based CSIRT/LE entities (e.g. the U.S. etc.)

[49] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-process-integration/operational-it-processes/itil

parameters such as network infrastructures that support its operation, software, hardware and durability - tolerance to risk factors such as power outages, natural disasters, etc.

At this point, there are some initiatives that have already started at EU level e.g. the Horizon 2020 - H2020[50] project for developing a Lawful evidence collecting & continuity platform (LOCARD)[51]. Cross-sharing evidence seems to be also on researchers' agenda. However, all the efforts are being done are still in very early stages.

Such a cooperation platform must be built on existing expertise and current developments within the field. There are plenty of tools available with different features and can be used for various investigation purposes; this subchapter presents a non-exhaustive list of the features they have in common.

5.2.1 Security

The platform should provide security and reliability, ensuring the following parameters:

- **Integrity**: it is crucial to ensure that the information has not been tampered. All communities should be able to use certain datasets, preserving the initial form, while passing through different "hands".
- **Identification**, **authentication and accountability**: As all communities will be working within the same datasets, they should be able to attribute information to certain users/institutions. For this purpose, users should be properly identified, authenticated and a thorough accountability mechanism should be put in place so that every action performed is traceable.
- **Confidentiality**: All data must remain confidential, assured through the best possible security measures.
- **Authorisation and role-based access**: Certain institutions might desire to keep certain datasets confidential or available only to small communities. The platform should allow authorisation based access as well as role-based access.
- **Availability**: this refers to the availability of information whenever an authorised user attempts to access it.
- **Non-repudiation**: this is strictly related to accountability.

An example of how a platform should perform is presented below:

A national CSIRT might want to share some Indicators of Compromise (IoC) recently collected with certain members of the CSIRTs Network. Once the members of the CSIRTs Network have access, additional information might be added by them to the initial IoC. At some point, enough data might be available to help LE launch an investigation. At this stage, owners of data (CSIRTs) might want to authorize certain LE officers to have access to information related to these incidents. Certain LE might want to open cases based on the initial data and share them with the other members of the LE community. This could lead to a cross-border case, that would eventually be followed by a takedown.

The security of the platform requires a complex set of guidelines and rules relating to the organisation of its administrator and hosting provider, the processes executed, the services provided, the technical infrastructure available, as well as the legal framework for personal data protection and security of communications.

[50] https://ec.europa.eu/programmes/horizon2020/en
[51] https://locard.eu/

5.2.2 Interoperability

Interoperability refers to the ability to collaborate with different organisations in a homogeneous and efficient way to achieve common goals. This also involves the ability of two or more systems to exchange information and then use these information in a useful and meaningful manner. Interoperability is recognised internationally as one of the most important issues for achieving efficient operation of information systems in businesses and organisations of all sizes and industries.

For this situation, interoperability must be assured at the semantic, organizational and technical layers. The semantic layer has been assured mainly by the work published in 2016 by ENISA and EUROPOL, on a *Common Taxonomy for Law Enforcement and CSIRTs* (ENISA EUROPOL EC3, 2016). Although further work must be done to completely synchronize terminologies between the two communities, the current taxonomy can provide a satisfactory level of understanding.

Considering technical interoperability, the aim that is being set is to transfer and use information in a seamless and efficient way between the parties registered in the platform.

As mentioned in the ENISA report *Information sharing and common taxonomies between CSIRTs and Law Enforcement* (ENISA, 2016), although multiple standards exist for the sharing of information, Structured Threat Intelligence eXpression – STIX[52], appears to be the preferred mechanism for the information exchange between CSIRT and LE communities. As more and more organisations and vendors support STIX, this seems to be the right choice for such a platform. In cases where the CSIRT/LE taxonomy does not fit the needs of some constituents, we can adopt the multi-taxonomy practice. A thorough analysis has to be performed to determine how many taxonomies/standards have to be supported within the platform.

Organisations might need to implement internal changes as well as to adopt the new interoperability standards, as some internal processes and procedures might be affected by the changes. The amount of change needed has to be decided on a case-by-case approach.

At EU level, the European Interoperability Framework (EIF) is a jointly agreed approach to deliver European public services in an interoperable manner. It offers public administrations concrete recommendations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that both existing and new legislation do not compromise interoperability efforts[53].

5.2.3 Key functionalities

This subchapter will attempt to identify key-shared functionalities that tools must have to properly accomplish their goals.

Working with digital evidence involves certain measures to be applied, depending on the operations developed. Accurate collection of logs, not tampering with evidence while collecting data, correctly identifying the timestamp to correlate different types of events etc. are just a few items on a long list.

FUNCTIONALITIES

Incident reporting, evidence management, anonymisation support, data analysis capabilities, visualisations, investigations cross-checking and report production.

[52] https://oasis-open.github.io/cti-documentation/
[53] https://ec.europa.eu/isa2/eif_en

Like many other digital platforms, the proposed platform will have to follow certain international standards and other general design features, such as usability, accessibility, interoperability, security by design and by default, etc.

1. **Interoperability**: sharing electronic evidence is crucial; however, it must be done in a way the other parties can read it. Interoperability between platforms and data collecting tools should be included in the general features of this platform. The platform should also permit the export data to a certain format, in order to be imported in other tools too.
2. **Adherence to international standards**: being able to exchange data between parties means they should be able to understand a common language. Developing an information-sharing framework or language seems to be one of the key elements. As discussed by (Biasiotti M. , 2017) currently CybOX, DFAX15 and the Unified Cyber Ontology (UCO), are the "most suitable standards to represent data and metadata related to an evidence exchange". However, these are standards used by LE. CSIRTs use mainly STIX/TAXII[54] standards for exchanging data. A common platform should be able to understand and translate the different "languages" used by the communities.
3. **Preservation of chain of custody**: The EVIDENCE[55] project developed a proof of concept application on the digital evidence exchange, which includes support for maintaining a detailed continuity of evidence (also called a chain of custody). Preserving the authenticity of evidence collected while transmitted from one entity to another is crucial. CSIRTs do have more informal methods of collecting data, but LEAs follow many procedures before acquiring evidence.
4. **Accountability**: being able to track one's actions is a necessity, closely linked with the ability to preserve the chain of custody.
5. **Security**: being able to preserve the confidentiality, integrity and availability of data stored and exchanged within the platform is another requirement needs to be considered.
6. **Analytics**: this feature allows the thorough analysis of collected data to measure one's activity and helps to present statistics on the use of the platform.

5.2.3.1 Incident reporting (ticketing)

A major functionality for the platform is incident reporting and management of the related "tickets". Ticketing software converts all incoming reports from multiple channels into tickets. A ticketing system offers prioritization, tracking and following-up of each case opened in the system. This can help different entities to communicate better and handle issues more efficiently. The ticketing software can also provide better statistics on the incident handling processes.

Therefore, by using a ticketing software, all the data inserted into the platform will be classified based on tickets/cases. CSIRTs and LE might define and classify cases in a different way.

The platform should allow to ingest data in many forms and organize them according to each actor's needs. Data acquired must also be sanitized, so that only pertinent data remain and collection of irrelevant data to be eliminated.

Current ticketing systems are considered too simple and do not appropriately support large investigations. The platform should allow for several layers of tickets and regrouping of tickets into broader folders.

[54] https://oasis-open.github.io/cti-documentation/
[55] http://www.evidenceproject.eu/the-activities/deliverables.html

5.2.3.2 Evidence management

Management of evidence related to a crime/incident is also of great importance for the collaborating parties. The platform should provide officials with the ability to track all procedures regarding digital evidence. The recommended evidence management solution is based on the data lifecycle stages i.e. the collection, the processing, the storage, the transfer and the maintenance. The platform must provide a clear insight into the chain of custody for e-evidence.

The final goal is to provide LE and the judiciary with enough evidence to successfully conclude cybercrime investigations and convict criminals. Evidence management is of utmost importance.

CSIRT processes and procedures might not adhere to the official ones used in court that are followed by LE and the judiciary.

The platform will have to be supported by a comprehensive framework of data collection and analysis that will help the involved communities to better manage the evidence.

5.2.3.3 Anonymisation support

Data anonymization is the process in which personally identifiable information, like age, gender, name, etc., is changed or removed from a set of data so that it would be impossible to determine the individual the data belongs to. Since the platform will be used by several entities and will be containing personal data, there is a need for data anonymisation, not only for security reasons but also to comply with the relative legislation on personal data processing. It should be noted that anonymised data are not considered personal data, according to the data protection legislation. Nevertheless, not all cases allow anonymisation and the processing of personal information may often be necessary for the objectives pursued. In such cases, pseudonymisation can be used instead. Pseudonymised data still allow for some form of re-identification of the data subject, while anonymous data do not. Therefore, pseudonymised data are considered as personal data (Regulation EU 2016/679, recital 26 (Council E. P., 2016a)).

5.2.3.4 Data analysis capabilities, visualisations

Data analysis is the process of transforming raw data into usable information, in order to add value to the statistical output[56]. It is different from data visualisation that involves the visual representation of data, ranging from single charts to comprehensive dashboards. Effective visualisations significantly reduce the amount of time it takes for someone to process information and access valuable insights. The platform should provide these types of functionalities to facilitate the cooperation and interaction across CSIRTs, LE and the judiciary.

5.2.3.5 Investigations cross-checking

The platform should be facilitating investigations crosschecking. Investigators and other officials will be able to identify relationships among people, objects, modi operanti, etc. Thus, investigation of cases will be easier, while at the same time, de-confliction will be available. Nevertheless, it is important that the platform to be linked to different sources of data, held by several entities on their systems.

5.2.3.6 Generated reports

Another very useful functionality of the platform is the automatic generation of reports, during an investigation or once thesis completed. The reports produced should be customisable and shareable with the concerned stakeholders. A report could include technical, strategic or other types of details, depending on who the recipient is. Thus, its content should be easily understood by the reader and include only information for the specified purposes.

[56] https://stats.oecd.org/glossary/detail.asp?ID=2973

5.2.3.7 Information sharing

The core functionality of such a common platform is the information sharing capability. The entities need to be able to share information, in a controlled and secure way. Access to information should be regulated according to the “need-to-know” basis, always in accordance with the existing legislation.

For achieving the abovementioned objective, different kinds of limitations that might affect the sharing process has to be taken into account. Even if CSIRTs might be able to share all kinds of data, LE and judiciary investigations might contain classified data, which cannot be shared with other communities.

In this respect, it becomes important for the platform to have access restriction capabilities. Access should be allowed at user or group level. At the same time, sharing and access policy should be established.

A classification scheme should be put in place to accommodate requirements from all involved communities. CSIRTs usually use the Traffic Light Protocol - TLP protocol[57], while LE and the judiciary might rely a lot on classified information.

Information sharing should be done at community level (e.g. CSIRTs only) or organizational level (some CSIRTs and some LEAs). This means the platform should have role-based, group-based and individual-based sharing capabilities.

5.2.3.8 Access management

The platform should finally provide IT managers with tools and technologies for controlling user access to critical information, defining and managing the roles and access privileges of individual network users as well as the circumstances under which users are granted (or denied) those privileges.

The platform should implement a clear Segregation of Duties (SoD), by disseminating the tasks and associated privileges for specific processes among multiple people aiming to prevent and detect errors and irregularities (ISACA, 2019). An indicative example of SoD is provided by ENISA in form of a matrix (see E ANNEX: SOD MATRIX)

The platform should have strong access management capability as well as strong authentication in place (e.g. at least two factor authentication). The platform should be able to define individual users along with user groups or even organisations units (institutions or communities). Access logs should be widely available, providing details on the user’s actions within the platform.

[57] https://www.us-cert.gov/tlp

6. CONCLUSIONS AND RECOMMENDATIONS

6.1 CONCLUSIONS

6.1.1 Filling in the gaps

In this study, we have estimated the degree of maturity of the technical cooperation across CSIRTs, LE and the judiciary throughout the lifecycle of cybercrime investigation. The main takeaway is that all three communities are mature, with their own well-established processes in place and have identified, adopted or developed the proper tools for performing their duties.

The CSIRT community has proven, by far, to be the most sophisticated and flexible in terms of tools. Members of the community have identified a broad range of tools (either commercial or open-source), for different kinds of tasks and the more mature members have also taken the lead in developing certain tools and making them available for the whole community (e.g. MISP). Steps are being taken currently, at EU level, for enhancing technical cooperation and the exchange of information among members, via the development of an EU level cooperation platform (MeliCERTes).

The survey has shown that LE rely heavily on a variety of tools during the stages of cybercrime investigation. As their job and goals are very specific, it is not a surprise that the same or similar tools are used by LE across the EU. Nevertheless, due to the fact that the tasks of LE are related to judicial procedures, LEAs do not have the same flexibility and freedom as the CSIRT community to use in-house developed tools or even open-source tools. Tools used by LEAs should provide an adequate level of assurance, so that collected evidence could be admissible in court.

However, survey responses did indicate notable cooperation between the two communities however without the use of dedicated tools. Basic tools for communication and information exchange, such as emails and telephone, are usually used. There are though, several examples within the Member States, where well-established cooperation mechanisms and tools are put in place at national level.

Despite the fact that judicial authorities had not provided feedback in the online survey, based on the results presented in a previous ENISA report (ENISA, 2019a), it had been highlighted that there is cooperation between LE and the judiciary, while CSIRTs have direct cooperation with prosecutors and judges, only when CSIRT experts are called as witnesses in court.

6.1.2 Analysing the necessity of a common platform

It is more than obvious that all three communities have different roles within the cybercrime investigation lifecycle. Nevertheless, reducing cybercrime and its consequences is the desired outcome for all actors involved. This leads to the conclusion that the parties should strengthen their cooperation and aim for a faster and more efficient response.

CSIRT community has taken serious steps towards improving inter-CSIRT cooperation in the EU. Platforms such as MeliCERTes will improve cooperation and incident response across the EU. The LE community has also taken similar steps to improve LE interagency cooperation within the EU, through platforms such as SIENA and SIRIUS, hosted by Europol.

The new Regulation proposal regarding European Production and Preservation Orders for electronic evidence in criminal matters (European Commission, 2018), represents also a big step forward in harmonising the way information is exchanged in criminal investigations.

All prerequisites leading to successful cooperation across the three communities appear to be in place. Building a common platform for these three communities that are actively involved in the cybercrime investigation lifecycle phases should be an important next step to consider at the policy level. At least, as a start, effort should be directed into drafting the required functionalities and the technical specifications for designing and subsequently developing such a platform. When drafting the technical specifications of this platform, all the requirements the communities have should be considered.

6.2 RECOMMENDATIONS

Some recommendations are proposed for the relevant stakeholders.

6.2.1 Recommendations for ENISA and possibly EUROPOL EC3 and EUROJUST

- To closely monitor the developments within the area and support involved parties in achieving the desired level of technical cooperation.
- To consider and promote the adoption of a common digital forensic framework.
- To assess the suitability of EU cybersecurity certification framework for cybercrime investigation tools and services.
- To drive efforts towards the development of a common platform, considering all requirements and constraints expressed by the communities.
- To facilitate the sharing of experience at strategic and operational cooperation across the three communities.
- To promote the use of Segregation (or separation) of Duties (SoD) matrices to avoid overlapping duties across CSIRTs, LE and the judiciary in relation to the sharing information.

6.2.2 Recommendations for CSIRTs

- To highlight specific services that can be delivered to LE.
- To identify specific requirements that LE and the judiciary might have, in terms of cooperation at national level, and try to accommodate by providing the necessary information to them.
- To discuss and consider the adoption of a common digital forensic framework.
- To develop CSIRT specific requirements for a common cooperation platform.

6.2.3 Recommendations for LE

- To develop EU and national level requirements for the CSIRT community, on what types of information provided by CSIRTs can be useful for LE, throughout the cybercrime investigation lifecycle.
- To discuss and consider the adoption of a common digital forensic framework.
- To develop LE specific requirements for a common cooperation platform.

6.2.4 Recommendations for the judiciary

- To develop EU level requirements for the CSIRT and the LE community, on what data can be useful and how to exchange it properly.
- To develop evidence collection and management rules in order the digital records to be admissible in court.
- To develop specific requirements for a common cooperation platform.

7. BIBLIOGRAPHY/REFERENCES

Best Practical. (2019, October 23). *RTIR*. Retrieved from Best Practical: https://bestpractical.com/rtir

Biasiotti, M. (2017). A proposed electronic evidence exchange across the European Union. *Digital Evidence and Electronic Signature Law Review*. doi:10.14296/deeslr.v14i0.2337

Biasiotti, M. J. (2018). *Handling and Exchanging Electronic Evidence Across Europe .* Springer International Publishing.

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

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

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

Council, E. P. (2016a). *Regulation EU 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Council, E. P. (2016b). *Directive EU 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Council, E. P. (2016c, April 27). *Directive (EU) 2016/680 n 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 crimin.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

Council, E. P. (2019). *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).* Retrieved from https://eur-lex.europa.eu/eli/reg/2019/881/oj

Council, EU. (2017, May 31). Retrieved from Notes: http://data.consilium.europa.eu/doc/document/ST-9621-2017-INIT/en/pdf

Council, EU. (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

CREST. (2019, November 12). *Cyber Security Incident Response Guide*. Retrieved from https://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide-1.pdf

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

ENISA. (2010). *Good Practice Guide for Incident Management.* Retrieved from https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

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

ENISA. (2015b). *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. (2015c). *CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs.* Retrieved from https://www.enisa.europa.eu/publications/csirt-capabilities

ENISA. (2016). *Information sharing and common taxonomies between CSIRTs and Law Enforcement.* Retrieved from https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

ENISA. (2016). *NIS Directive*. Retrieved from https://www.enisa.europa.eu/topics/nis-directive

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

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

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

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

ENISA. (2019a, Jan). *Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary.* Retrieved from https://www.enisa.europa.eu/publications/csirts-le-cooperation: https://www.enisa.europa.eu/publications/csirts-le-cooperation

ENISA. (2019b, October 23). *Incident Handling Automation*. Retrieved from https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation

ENISA. (2019c, November 11). *Electronic evidence - a basic guide for First Responders*. Retrieved from https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders

ENISA. (2019d). *Roadmap on the cooperation between CSIRTs and LE.* Retrieved from https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation

ENISA EUROPOL EC3. (2016). *Common Taxonomy for Law Enforcement and CSIRTS.* Retrieved from https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts

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

European Commission. (2018, April 17). *European Production and Preservation Orders for electronic evidence in criminal matters*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN

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

European Commission. (n.d, a). *E-evidence - cross-border access to electronic evidence*. Retrieved from https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

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

European Commission. (n.d., b). *The EU cybersecurity certification framework*. Retrieved from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

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. (n.d.). *Countries*. Retrieved from https://europa.eu/european-union/about-eu/countries_en

Europol. (2017a, June 28). *New wave of ransomware affecting businesses: what to do?* Retrieved September 06, 2017, from https://www.europol.europa.eu/newsroom/news/new-wave-of-ransomware-affecting-businesses-what-to-do

Europol. (2019, October 23). *SECURE INFORMATION EXCHANGE NETWORK APPLICATION*. Retrieved from Europol: https://www.europol.europa.eu/activities-

services/services-support/information-exchange/secure-information-exchange-network-application-siena

EUROPOL. (2019, October 23). *SIRIUS Project*. Retrieved from https://www.europol.europa.eu/activities-services/sirius-project

Hall, J. (2015). Retrieved from Incident Tracking In The Enterprise: https://www.sans.org/reading-room/whitepapers/incident/paper/36092

ISACA. (2019, November 12). *Glossary*. Retrieved from https://www.isaca.org/Pages/Glossary.aspx?tid=1835&char=S

Mattermost. (2019, October 23). *Product*. Retrieved from https://mattermost.com/product/

MISP. (2019, October 23). *Home*. Retrieved from https://www.misp-project.org/index.html

NCSC-NL. (2019, October 23rd). *Taranis3*. Retrieved from https://github.com/NCSC-NL/taranis3/wiki

NIST. (2019, November 12). *Computer Forensics Tools & Techniques Catalog*. Retrieved from https://toolcatalog.nist.gov/

NIST. (2019, October 23). *Glossary*. Retrieved from Computer Security Resource Centre: https://csrc.nist.gov/glossary/term/role_based-access-control

OASIS Cyber Threat Intelligence Technical Committee (CTI TC). (2019, November 12). *CTI-Documentation*. Retrieved from https://oasis-open.github.io/cti-documentation/

OpenPGP. (2019, October 23). *About*. Retrieved from https://www.openpgp.org/about/

SANS. (2019, November 12). *Incident Handlers Handbook*. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Threema. (2019, October 23). *FAQ*. Retrieved from https://threema.ch/it/faq/why_secure

A ANNEX: ABBREVIATIONS

Abbreviation	Description
AI	Artificial Intelligence
BSI	Bundesamt für Sicherheit in der Informationstechnik - Federal Office for Information Security (Germany)
C&C	Command-and-Control
CCM	Cloud Controls Matrix
CEN	Comité Européen de Normalisation - European Committee for Standardisation
CENELEC	Comité Européen de Normalisation en Electrotechnique - European Committee for Electrotechnical Standardisation
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
CFTT	Computer Forensics Tool Testing Program
CGN	Carrier-grade NAT
CIIP	Critical Information Infrastructure Protection
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CTI TC	OASIS Cyber Threat Intelligence Technical Committee
DDoS	Distributed Denial-of-Service (attack)
DoS	Denial of Service (attack)
DP	Data Protection
EC3	European Cybercrime Centre (Europol)
EFTA	European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland)
EIF	European Interoperability Framework

EIO	European Investigation Order
ENISA	European Union Agency for Cybersecurity
ENP	European Neighbourhood Policy
ETSI	European Telecommunications Standards Institute
EU	European Union
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
FKIE	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie - Fraunhofer Institute for Communication, Information Processing and Ergonomics (Germany)
GDPR	General Data Protection Regulation
H2020	Horizon 2020
ICT	Information & Communication Technology
IEC	International Electrotechnical Commission
IHAP	Incident Handling Automation Project
IM	Incident Management
IoC	Indicator of Compromise
ISMS	Information Security Management Systems
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library
J-CAT	Joint Cybercrime Action Taskforce
LE	Law Enforcement
LE ERP	Law Enforcement – Emergency Response Protocol
MISP	Malware Information Sharing Platform
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty

NCA	National Crime Agency (UK)
NCSC	National Cyber Security Centre (UK)
NIS	Network Information Security
NIST	National Institute of Standards and Technology (United States)
NIST CSF	National Institute of Standards and Technology (United States) Cybersecurity Framework
NMR	No More Ransom
OSP	Online Service Providers
PGP	Pretty Good Privacy
PoC	Point of Contact
RAID	Redundant Array of Independent Disks
RTIR	Request Tracker for Incident Response
RBAC	Role-Based Access Control
SIENA	Secure Information Exchange Network Application
SoD	Segregation (or separation) of Duties
STIX	Structured Threat Intelligence eXpression
TIP	Threat Intelligence Platform
TLP	Traffic Light Protocol
UCO	Unified Cyber Ontology

B ANNEX: TECHNOLOGIES USED BY THE COMMUNITIES

System	Description
IntelMQ	IntelMQ is a solution for CERTs for collecting and processing security feeds, pastebins, tweets using a message queue protocol. It is a community-driven initiative called IHAP (Incident Handling Automation Project) which was conceptually designed by European CERTs during several information security events. Its main goal is to give to incident responders an easy way to collect and process threat intelligence thus improving the incident handling processes of CERTs. (ENISA, 2019b)
Mattermost	Mattermost is an open-source messaging platform that enables secure team collaboration. (Mattermost, 2019)
Malware Information Sharing Platform (MISP)	MISP is a free and open-source software helping information sharing of threat intelligence including cybersecurity indicators. A threat intelligence platform for gathering, sharing, storing and correlating IoC of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information." (MISP, 2019)
OpenPGP	OpenPGP is a non-proprietary protocol for encrypting email communication using public-key cryptography. It is based on the original PGP (Pretty Good Privacy) software. The OpenPGP protocol defines standard formats for encrypted messages, signatures, and certificates for exchanging public keys. (OpenPGP, 2019)
Role-Based Access Control (RBAC)	RBAC is access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. (NIST, 2019)
Request Tracker for Incident Response (RTIR)	RTIR builds on all the features of RT and provides pre-configured queues and workflows designed for incident response teams. It is the tool of choice for many CERT and CSIRT teams all over the globe. RTIR has tools to correlate key data from incident reports, both from people and automated tools, to find patterns and link multiple incident reports with a common root cause incident. (Best Practical, 2019)
The Secure Information Exchange Network Application (SIENA)	SIENA is a state-of-the-art platform that meets the communication needs of EU law enforcement. The platform enables the swift and user-friendly exchange of operational and strategic crime-related information among: - Europol's liaison officers, - Analysts and experts - Member States third parties with which Europol has cooperation agreements. (Europol, 2019)

SIRIUS	The SIRIUS project was created by Europol in October 2017 as a response to the increasing need of the EU law enforcement community to access electronic evidence for internet-based investigations, as more than half of all criminal investigations today include a cross-border request to access electronic evidence (such as texts, e-mails or messaging apps). The SIRIUS project, spearheaded by Europol's European Counter-Terrorism Centre and European Cybercrime Centre, in close partnership with Eurojust and the European Judicial Network, aims to help investigators cope with the complexity and the volume of information in a rapidly changing online environment, by providing guidelines on specific Online Service Providers (OSPs) and investigative tools; and sharing experiences with peers, both online and in person. Through continued collaboration with Eurojust and the European Judicial Network, the SIRIUS project is now also open to judicial authorities. The multidisciplinary SIRIUS community on the restricted platform on the Europol Platform for Experts has access to a wide range of resources, updated continually. (EUROPOL, 2019)
Structured Threat Intelligence eXpression (STIX)	STIX is a language and serialization format used to exchange cyber threat intelligence (CTI). enables organizations to share CTI with one another in a consistent and machine-readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. (OASIS Cyber Threat Intelligence Technical Committee (CTI TC), 2019)
Threema	Threema is 'an end-to-end encrypted instant messaging application for iOS, Android and Windows Phone. In addition to text messaging, users can make voice calls, send multimedia, locations, voice messages and files'. (Threema, 2019)
Taranis	Taranis is a software to structure information from various sources about vulnerabilities. It scans the internet for texts about digital threats and vulnerabilities in software, hardware, and operating systems. (NCSC-NL, 2019)

C ANNEX: OPERATION AVALANCHE & ANDROMEDA BOTNET TAKEDOWN

An example of joint action and cooperation among several entities around the world was the takedown of the Andromeda botnet (also known as Gamarue), which took place on 29th November 2017. It is still considered today as a significant dismantling of the longest-running malware families. The case included not only cooperation between the public and private sector, but also coordinated actions among LEAs, judicial authorities and CSIRTs.

According to Microsoft research, Andromeda's goal was to distribute almost 80 malware families. Within a period of six months, it was detected that an average of over 1 million machines were blocked every month.

Earlier in 2016, after several years of investigation, judicial and LE authorities from Germany, United States of America, along with Europol, Eurojust and other partners had dismantled the international criminal infrastructure Avalanche, which was used, among others, as a delivery platform to launch and manage mass global malware attacks such as Andromeda.

While preparing the Avalanche joint action, the German Cybersecurity Authority, the Federal Office for Information Security (BSI) and the Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) analysed over 130 TB of captured data and helped identifying the server structure of the botnet, allowing for the shutdown of thousands of servers and, effectively, the collapse of the entire criminal network. During the Avalanche Operation, 5 individuals were arrested, 37 premises were searched, and 39 servers were seized. Abuse notifications were sent in relation to over 200 compromised servers. Victims of malware infections were identified in over 180 countries. Avalanche was a remediation operation as well as a LE operation. The main effect was to sanitize German cyberspace from the Avalanche botnet but apart from the German victims, feeds with sinkholed data were sent to CSIRT teams all over the world in order to do victim mitigation.

The dismantling of Andromeda was heavily based on knowledge and intelligence gained during the Avalanche case by LE, combined with the intelligence provided by private-sector partners. Europol played a coordination role in both operations.

Thus, on November 29th 2017, the United States of America Federal Bureau of Investigation (FBI), in close cooperation with the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Task Force (J-CAT), Eurojust and private sector partners, took jointly action against servers and domains, which were used to spread the Andromeda malware.

According to Europol 1500 domains of the malicious software were sinkholed, while according to Microsoft[58], during 48 hours of sinkholing[59], approximately 2 million unique Andromeda victim IP addresses from 223 countries were seized.

In parallel, sinkhole measures were necessary, across several countries (both EU and non-EU), as globally 55 per cent of the computer systems originally infected in Avalanche were still infected at the time of the joint action. This was the part where CSIRTs were involved in the operation. When sinkholing is employed at a 100% scale, infected computers can no longer reach the criminal C&C computer systems and criminals can therefore no longer control the infected computers. After the operation, the victims' computers communicated with the LE servers instead of the attackers C&C. The feeds with victim information (geo-localized IP address and timestamp) were sent to the responsible national CSIRT in an automatic manner in order to do further victim mitigation at national level. In this way, the sinkholing infrastructure captures victims' IP addresses, which can subsequently be used for notification and follow-up through dissemination to National CSIRTs and network owners.

In terms of regulatory instruments, the Mutual Legal Assistance Treaty (MLAT) process was used and not the European Investigation Order (EIO).

During the preparation of the Operation Avalanche and the Andromeda botnet takedown, according to the representative of EC3, the collaborating partners used to have conference calls every week, with a duration of an average of 2 hours. Communication was based on PGP channels. Secure information exchange channels were used between LE representatives. It can be easily understood that private partners are not allowed to have access to certain LE tools for coordinating the case.

As key cooperation challenge in both cases has been identified, the not well-structured communication among the public and private partners, LE, judicial authorities and CSIRTs. Therefore, the need for a coordination platform has been highlighted; its key functionalities should include:

- Information sharing;
- Tasking for not overlapping others' duties and for better monitoring;
- Discussion groups; real-time communication is of great importance too;
- Sharing of tactics followed; it should be noted that efforts are being done for developing a manual with best practices;
- Capability of creating investigation (user) groups with access rights to certain types of information.

Furthermore, user-friendliness and accessibility are very important features for a collaboration platform.

Finally, the security aspect should be considered when designing such a platform as well as respecting the relevant legislation on personal data protection.

In conclusion, the Andromeda botnet takedown was a significant example of international law enforcement working together with judicial authorities, CSIRTs and industry partners to identify the most significant cybercriminals and the dedicated infrastructure they use to distribute malware on a global scale.

[58] https://www.microsoft.com/security/blog/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/
[59] Sinkholing is an action whereby traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security company.

D ANNEX: NO MORE RANSOM

The No More Ransom (NMR)[60] initiative could be characterized as an "alternative" and innovative way of cooperation among LE, CSIRTs, public and private partners. The NMR portal has helped more than 200.000 victims of ransomware to recover their files free of charge since it was first launched in July 2016. More than 3 million individual visitors from over 188 countries have accessed the portal looking for information or for a specific solution to their ransomware infection[61].

More specifically, NMR is an initiative by Europol's European Cybercrime Centre (EC3), the National High-Tech Crime Unit of the Netherlands' police, Kaspersky Lab and McAfee to help victims of ransomware to retrieve their encrypted data without having to pay to the criminals. Ransomware has been around for a number of years and victims are forced to either pay a ransom or lose their files.

Victims of ransomware can visit the following portal: https://nomoreransom.org, upload samples of their encrypted files and check if there are available decryption tools for the malware family that infected their systems. After a quick assessment by the 'Crypto Sheriff', if the appropriate decryption tool is available the victim is prompted to the guidelines to download the tool and recover their data. Victims' data are not stored or shared with third parties; the information is deleted as soon as the assessment is performed.

By restoring access to their infected systems free of charge, the partnership provides users with a third choice they did not have before, as it counts with more than 90 tools capable of decrypting over 120 different types of ransomware families[62]. The tools are provided at the discretion of the NMR partners.

The NMR portal, initially released in English, is available in 35 other languages.

The initiative is the first public-private partnership of its kind. It is based on the cooperation between more than 150 partners and it is recognized globally as an excellent effort on cybercrime remediation since some $108 million profit have been prevented from going to the pockets of criminals. 42 LEAs, 5 EU Agencies and 101 public and private entities have joined this project since 2016.

Since the launch of the portal, Politie Police (Belgium), Politia Romana (Romania), Police Nationale (France) and CERT Polska (Poland), together with other eleven private companies, have contributed to the development of new unique decryption tools. These tools are presented in the NMR portal and are available to the public through the related websites.

Many other LEAs and CSIRTs "kindly offer their time and resources to help promote NMR at the national and international level".

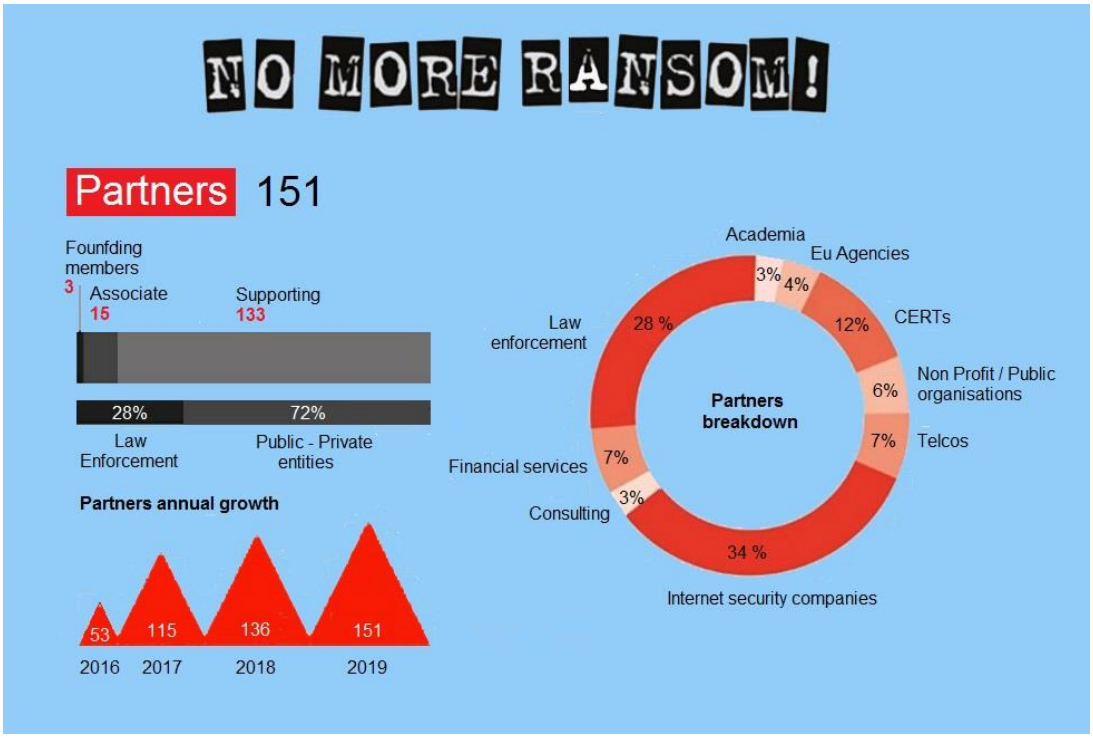
[60] www.nomoreransom.org
[61] https://www.europol.europa.eu/newsroom/news/no-more-ransom-108-million-reasons-to-celebrate-its-third-anniversary
[62] https://www.europol.europa.eu/publications-documents/infographic-3rd-anniversary-no-more-ransom

The objectives of the NMR project is neither the remediation nor cybercrime prevention. This is a stand-alone approach that provides decryption tools only for certain ransom threats i.e. HildaCrypt[63], Muhstik[64], GalactiCryper[65], Avest[66], Yatron[67], FortuneCrypt[68], WannaCryFake[69], Syrk[70], JSWorm 4.0[71], Iams00rry[72], ZeroFucks[73], and Mira[74]. Technical cooperation is required between the 'Associated partners' who provide the decryption tools and the 'Supporting partners' who inform the public. This cooperation focuses on:

- providing decryption tools
- circulating the related link for accessing the portal

In Figure 7 below, the infographic shows data about the partners are available:

Figure 7: No More Ransom Project



[63] https://www.nomoreransom.org/en/decryption-tools.html#HildaCrypt
[64] https://www.nomoreransom.org/en/decryption-tools.html#Muhstik
[65] https://www.nomoreransom.org/en/decryption-tools.html#GalactiCryper
[66] https://www.nomoreransom.org/en/decryption-tools.html#Avest
[67] https://www.nomoreransom.org/en/decryption-tools.html#Yatron
[68] https://www.nomoreransom.org/en/decryption-tools.html#FortuneCrypt
[69] https://www.nomoreransom.org/en/decryption-tools.html#WannaCryFake
[70] https://www.nomoreransom.org/en/decryption-tools.html#WannaCryFake
[71] https://www.nomoreransom.org/en/decryption-tools.html#JSWorm40
[72] https://www.nomoreransom.org/en/decryption-tools.html#Iams00rry
[73] https://www.nomoreransom.org/en/decryption-tools.html#ZeroFucks
[74] https://www.nomoreransom.org/en/decryption-tools.html#Mira

E ANNEX: SOD MATRIX

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

TP-02-20-187-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 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: 978-92-9204-342-1
DOI: 10.2824/13844