Information sharing and common taxonomies between CSIRTs and Law Enforcement

FINAL

VERSION 1.0

PUBLIC

DECEMBER 2015

About ENISA

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

Authors

In alphabetical order:

- Deloitte Bedrijfsrevisoren / Reviseurs d'Entreprises, Belgium[1]
- Jo De Muynck, ENISA
- Dr. Silvia Portesi, ENISA

Contact

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

Acknowledgements

We would like to thank the experts interviewed for their valuable insight during the data collection phase. In addition, we would like to thank the EC3 who kindly helped us with reaching out to the Law Enforcement Agencies.

[1] The analysis and the compilation of this report was produced in collaboration with Deloitte Bedrijfsrevisoren / Reviseurs d'Entreprises BV o.v.v.e CVBA/SC s.f.d SCRL ('Deloitte Belgium'), commissioned by ENISA according to tender ref. ENISA D-COD-15-T14. The contributors from Deloitte were Dan Cimpean (Partner), Luc Beirens (Director), Joris Lambrechts (Senior Manager), Alexander Cespedes Arkush (Manager) and Cédric De Quirini (Consultant).

ISBN: 978-92-9204-163-2, DOI: 10.2824/189989

Table of Contents

Executive summary

This Report on Information Sharing and Common Taxonomies between CSIRTs and Law Enforcement Agencies (LEAs) was produced at the initiative of ENISA with the objective to enhance cooperation both between the Member States (MS) of the EU and between related Network and Information Security (NIS) communities.

With this study, which is a continuation of ENISA's work done in the area of fight against cybercrime, ENISA aims at identifying which information can be shared between CSIRTs and LEAs and how this can be achieved from a technical and organisational perspective.

This report presents four proposals:

- A taxonomy for the exchange of information based on desk research, to define a common vocabulary for the description of cyber incidents based on the approval of the majority of the community.
- A sharing mechanism for the exchange of information, based on a taxonomy. This element is still being debated, as explained further on in this document.
- An update model for the taxonomy, to answer new requirements that could arise from the CSIRTs and the LEAs.
- A roadmap for the implementation of the taxonomy in the exchange of information across CSIRTs and LEAs and the potential use of a sharing mechanism to enhance these exchanges.

There is a large consensus that a proposal for a taxonomy developed by CERT.PT[2] is a good starting point for the exchange of information between CSIRTs and LEAs. This taxonomy fulfils the requirements identified during this study, is easy to use and implement, while offering opportunities for future updates. In addition it takes into account the Budapest Convention[3] and the Cybercrime Directive[4], and provides a definition of the incidents and events it describes.

However, while a taxonomy allows to classify the information that is exchanged, it does not necessarily provide a format for the exchanged data. Therefore, although there is no commonly agreed format yet, using a common sharing mechanism could offer advantages such as automation of the analysis of the data and the creation of statistics. Based on the research performed, STIX[5] has been identified as an appropriate candidate. It has a high level of recognition by the CSIRTS and LEAs

[2] CERT.PT became part of the National Cybersecurity Centre in Portugal (CNCS). More information can be found here: http://www.cncs.gov.pt/home/index.html
[3] Convention on Cybercrime, Budapest, 23.XI.2001: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
[4] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF
[5] Structured Threat Information eXpression, a structured language for cyber threat intelligence: https://stixproject.github.io/

communities and it can be used together with any taxonomy and offer a model of which parts can be implemented separately, allowing a step-by-step approach.

Finally, to enhance the use of a taxonomy, it should also be kept up-to-date and evolve according to the requirements of CSIRTs and LEAs. Therefore, an update model should be put in place to ensure the further development of the taxonomy. Based on the information collected from CSIRTs and LEAs and the possibilities of alignment with corresponding EC3 activities, a dynamic update of the taxonomy through regular physical meetings with the stakeholders seems to be best suited.

1 Introduction

1.1 Background

As of 2015, ENISA's core operational activities are aligned with the four Strategic Objectives (SOs) from the ENISA strategy document and the multi annual planning for 2015 to 2017, which are summarised in ENISA's Work Programme 2015[6].

The work packages in SO4 aim 'to **enhance cooperation** both **between the Member States (MS) of the EU** and **between related Network and Information Security (NIS) communities**'. The overall goal is to 'build up targeted NIS communities to meet policy goals' through a 'learn by doing approach'.

Work Package (WPK) 4.1 aims at 'supporting EU cooperation initiatives amongst NIS–related communities in the context of the Cybersecurity Strategy of the European Union[7] (EU CSS)' through two deliverables.

The goal of the first WPK 4.1 deliverable (which is the focus of this study) is to 'develop and provide guidance based on good practice for cooperation between key stakeholder communities'.

The goal of the second WPK 4.1 deliverable is to 'identify practices of Member States in addressing different sector regulation challenges of managing cyber security issues'. This is to be achieved through a 'stocktaking on Member States regulatory approaches for Cyber Security, with an emphasis on cross-sector information sharing'.

1.2 Study Objectives and Scope

The study at hand aims to collect and present information on the previous and ongoing projects facilitating information sharing between CSIRTs and Law Enforcement. It aims at investigating which information can be shared between CSIRTs and Law Enforcement and how this can be achieved technically and organisationally.

The scope of this study are CSIRTs and Law Enforcement Agencies in the European Union. It does not cover other organisations than the selected communities (such as, for example, ISPs).

[6] ENISA Work Programme 2015 Including Multi-Annual Planning: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015
[7] Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

1.3 Purpose of this document

The purpose of this study is to propose a solution for the exchange of information between CSIRTs and Law Enforcement Agencies (LEAs) in the form of a **roadmap** and a **common taxonomy**, as well as a **mechanism** to share information based on this common taxonomy and a **model** on how to update the taxonomy to new phenomena.

This study outlines an initial proposal for:

- A **common taxonomy** that could be used for **sharing information** between CSIRT and LEA communities.
- A **mechanism** to share information between both communities based on this taxonomy.
- A **model to update** the taxonomy to new phenomena (such as new kind of attacks or a new vulnerability type).
- A **roadmap** for the introduction of the proposed taxonomy to both communities and the implementation of a sharing solution between CSIRTs and LEA communities.

In addition, this study outlines:

- How this study aligns with the Operational Action Plan (OAP) 4.1 working group[8] EMPACT (The European Multidisciplinary Platform against Criminal Threats) Cyber Attacks 2015 to avoid any overlap between both activities.

[8] Europol EC3 leads the OAP 4.1 meetings. The OAP 4.1 initiated last year had three objectives: defining a common taxonomy, defining exchange standards and achieving statistics. Up until now the first objective has been progressed. The aim for this year (2015) is to achieve the second and third objective as well. In order to achieve the second objective it is important to define use cases for sharing information between CSIRTs, LEA and third parties.

2 Proposition of a taxonomy for the exchange of information between CSIRTs and LEAs

In order to defend against evolving threats, information sharing is key. The sharing of information about cyber events and incidents allows others to defend against such attacks and help others to detect and react to these attacks. The main obstacle in the exchange of information is the current lack of standardization in the communication. There is no common understanding on how to exchange information, limiting the amount of information that can be exchanged and the possibilities of automation of this exchange.

Based on the previous work done by ENISA on the exchange of information between CSIRTs and LEAs, it seems that a common language[9] should be identified to enable a better exchange of information between them. Since the CSIRT and LEA communities have different goals[10], their way of representing and classifying information about cyber events and incidents are not necessarily similar, and the situation can be very different from one EU Member State to another. For example, while many LEAs use the NATO classification system[11], most CSIRTs use the Traffic Light Protocol (TLP[12]).

Moreover, while LEAs store information based on investigations, the CSIRTs also collect information on types of attacks that are not related to specific infection cases, in order to provide statistical information on the current threat landscape. LEAs, for example, collect information that can be used during an investigation to find evidence of a crime and incriminate its author. They also collect information on potential criminal actions which take place on the Internet. CSIRTs, on the other side, try to collect information on the current threat and attack vectors, and therefore tend to collect and share more information not directly related to a specific attack, such as vulnerabilities, attackers and behaviours.

Due to this difference in goals, the management of information by CSIRT and LEAs is very different. The way the information is stored and used can vary, and there is no common vocabulary used to define the types of threats and incidents.

To harmonise such exchanges of information, the first step is the choice of a common taxonomy that could be adopted by Member States of the European Union to classify information. This would allow the users of such a taxonomy to use the same vocabulary, by defining a common language, therefore making it easier to share the information between the users of the taxonomy.

Towards this end, this chapter details how a selection of a common taxonomy to be proposed for the exchange of information between CSIRTs and LEAs has been done, based on requirements highlighted by the interviews and possibilities of alignment of this study to the OAP 4.1 working group (presented in section 2.2.1).

[9] 'Language' describes here a common definition of the vocabulary used to describe events and incidents.
[10] While CSIRTs focus mainly on blocking cyber-attacks and restoring a normal situation at the victim side, LEAs focus on identifying criminals behind the attacks.
[11] The NATO classification system: http://www.nato.int/structur/AC/135/ncs_guide/english/e_1-6-1.htm
[12] Protocol to encourage classification systems: https://www.cert.be/traffic-light-protocol-tlp

2.1 Definition of a taxonomy

To further refine the scope of this study, the first step is to provide the definition of a taxonomy. According to the ENISA webpage on ontologies[13], the definition of a taxonomy is the following: 'a taxonomy is most often defined as a classification of terms and has a close relationship with the use of ontology. There are three characteristics that define a taxonomy:

- **A form of classification scheme** to group related things together and to define the relationship these things have to each other.
- **A semantic vocabulary** to describe knowledge and information assets.
- **A knowledge map** to give users an immediately grasp of the overall structure of the knowledge domain covered by the taxonomy, which should be comprehensive, predictable and easy to navigate.'

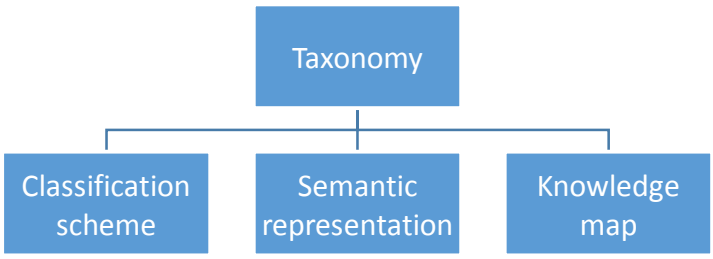


Figure 1 – Definition of a taxonomy[13]

Note that an ontology is a closely related concept. The definition of an ontology consists of the definition of domain concepts (e.g. objects, attributes and processes) and their properties/relationships. This goes beyond the purpose of harmonising and standardising the exchanges of information. In the view of the authors, LEAs and CSIRTs should first achieve the same vocabulary enabling a common language before describing more complex relations between concepts.

2.2 Alignment of this study with the EMPACT OAP 4.1 working group towards the choice of a taxonomy

This section presents the EMPACT OAP 4.1 working group, the objectives of aligning both activities for the choice of a taxonomy and how both of them are aligned at this stage of the project. One of the main objectives of the OAP 4.1 working group is to improve sharing of information between CSIRTs, LEAs and third parties and enable the generation of statistics on events and incidents. Due to the similarities between the OAP 4.1 working group and this study, an alignment of both activities benefits both communities.

[13] Based on ENISA's pages on ontology: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/ontology and https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/ontology/ontology_taxonomies

2.2.1 Description of the OAP 4.1 working group

The European Multidisciplinary Platform against Criminal Threats[14] (EMPACT) Cyber Attacks 2015, OAP 4.1[15] (OAP 4.1 working group) project is a multi-stakeholder initiative, taking into account the interest of EC3 (representing Europol), ENISA, and various CSIRTs and LEAs representatives within the European Union.

The OAP 4.1 working group had three main goals at the time of writing:

1. Defining a **common taxonomy** for the exchange of information related to incidents and events in cyber security.
2. Defining an **exchange standard** to enable the sharing of information based on the taxonomy.
3. Create **statistics** based on the information exchanged.

At the time of drafting this report, EC3 stated that the first goal, defining a common taxonomy, was in progress and that they aim to achieve two additional goals by the end of 2015. The six use cases presented in the first deliverable of this study are based on the use cases that were defined within the OAP 4.1 working group to help determine activities that the use of a common taxonomy should enable. It was agreed with ENISA that these use cases would serve as input to this study.

Additionally, the members of the OAP 4.1 working group are in the process of setting up a governance structure to allow revisions of a common taxonomy that could be updated during bi-annual meetings.

The Common Taxonomy for the National Network of CSIRTs[16] (hereafter the 'CERT.PT taxonomy') is, at the time of writing, considered as an appropriate candidate by the OAP 4.1 working group for a common taxonomy for the exchange of information. In this context, EC3 requested feedback about the CERT.PT taxonomy from the EU Cybercrime Task Force (EU CTF) for which no objection at that time was raised.

2.2.2 Use cases to be enabled by a common taxonomy

A set of possible use cases to be enabled by a common taxonomy have been identified in the context of the OAP 4.1 working group. These use cases highlight the interaction between actors (CSIRTs and LEAs but also other actors such as ISPs, which are out of the scope of this study). These use cases also support the goals to be achieved in the context of the work performed by ENISA in the fight against cybercrime[17]. Below is a summary of the use cases.

---

[14] EU Policy Cycle - EMPACT: https://www.europol.europa.eu/content/eu-policy-cycle-empact
[15] OAP: Operational Action Plan, part of the EMPACT as project to combat the priority threats.
[16] The Common Taxonomy for National Network of CSIRTs (2014) is developed by the Fundação para a Computação Científica Nacional (FCCN) and CERT.PT. It aims at describing a common taxonomy for the classification of incidents within the National Network of CSIRTs in Portugal. In presents a technical perspective and a 'high level legal characterisation' to facilitate the ontological harmonization of incidents within the Portuguese Network, the international network of CERTs and foreign criminal investigation police forces (Law Enforcement Agencies) or other similar bodies, such as the INTERPOL and the Europol.
[17] ENISA fight against cybercrime: https://www.enisa.europa.eu/activities/certs/support/fight-against-cybercrime

1. **Alerts from CSIRTs to LEAs**: with the common taxonomy and a common formatted message, LEAs can receive and automatically treat large amounts of data in less time, thus perceiving the evolution of incidents both quantitatively and geographic ways.
2. **Alerts among CSIRTs**: **CSIRTs** and their networks can optimise incident case analysis, promoting correlation of the security events and therefore act or react, jointly, within borders or with other EU **CSIRTs**. This should result in faster incident mitigation and additional information collection for incidents containing procedures and overall protectionism for the EU.
3. **Reporting of statistics**: Sharing statistics among the identified actors will allow information cross-checking with other sources, thus validating (or not) and spotting commercial distortions on the security Information market.
4. **LEAs alerts to CSIRTs**: **CSIRTs** can benefit from better anticipation of significant security events, access to correlated information that can highlight motivation of criminal actors.
5. **Joint actions based on previous contributions:** Because of the stronger collaboration between LEAs and **CSIRTs**, consolidated by the statistics and the data exchanged, campaigns of criminal prevention can be created and directed towards geographic areas populated by security incidents, now perceived and visualised by tools that deal with the shared information.
6. **ISPs enrolment:** ISPs can be enabled as active actors in this field, and both CSIRTs and LEAs can take advantage of their participation in terms of public image, since they will be able to 'make available' a 'security image' to its clients.

These use cases were further elaborated within the scope of this study. They represent the flow of information between CERTs and LEAs and an alignment with the information collected during the interviews.

2.2.2.1 Use case 1: Alerts from CSIRTs to LEAs

Through the interviews of CSIRTs and LEAs, it often appears that sharing information from CSIRTs to LEAs would be very interesting for the LEAs, and sometimes information about incidents and botnets is already shared. Although some LEAs are not able to treat such information due to the lack of resources, many consider that being able to receive data from CSIRTs would be (or is) an advantage for their work. Through the use of a taxonomy, the LEAs might be able to receive and automatically treat data in less time, which might allow them to perform analysis and perceive the evolution of cyber incidents.

Since the nature of activities of CSIRTs and LEAs differ from each other, the information they collect and the way they collect it are fundamentally different too. According to most respondents, LEAs are therefore interested in information that CSIRTs possess since it represents additional information that they can use in investigations, or to prevent criminal activities.

One of the limitations often encountered during the interviews performed for this study is the need for the approval of the victim. When CSIRTs help an organisation after an attack, they often need the organisation to file an official complaint before being able to provide information about the attack to LEAs. But apart from this limitation, exchange of information from CERTs to LEAs does not seem to have any other constraints.

2.2.2.2 Use case 2: Alerts among CSIRTs

Based on the interviews performed, it appeared that some communication between CSIRTs is already in place, although it is not always automated. But, even without automation, the CSIRT community often collaborates by sharing information. This information is sometimes exchanged through sharing platforms but is also simply sent by e-mail in a structured (CSV) or unstructured (PDF report) file. The community therefore seems to be interested in the implementation of a common taxonomy for the exchange of information, to facilitate these exchanges by the use of a common vocabulary.

Through the exchange of information structured on a common taxonomy, the CSIRTs might be able to perform incident analysis and correlate security events. This would enable joint reactions between CSIRTs across the European Union, and thus result in better incident mitigation.

2.2.2.3 Use case 3: Reporting of statistics

The exchange and correlation of information might allow the stakeholders to create statistics based on the common taxonomy by gathering and analysing the data exchanged,. Indeed, since the exchanged data is currently in different formats and uses different descriptions for events and incidents, it is currently very hard to create statistics on their frequency and type.

By defining the types of events and incidents and providing a clear classification of the information exchanged, a common taxonomy would facilitate the creation of statistics. While the CSIRTs and LEAs might not have resources to create such analysis of the exchanged data to provide statistics, Europol could be the central point to gather and analyse the exchanged information. This would allow Europol to create statistics at the European Union level.

The creation of such statistics might enable the detection of trends and tendencies in cyber incidents, enabling a better focus of the prevention and detection performed across the EU.

2.2.2.4 Use case 4: LEA alerts to CSIRTs:

Based on information collected during the interviews, although the alerts from CSIRTs to LEAs should not be a problem in most countries (as detailed in section 2.2.2.1), the sharing of information from LEAs to CSIRTs often encounter more constraints. LEAs are subject to restrictions regarding their inquiries, and can rarely disclose information to any other organisation. Besides this constraint, resources are also a problem: some LEAs do not have enough time or budget to gather and share information that could be useful to CSIRTs. Also, there is in some cases a lack of certainty from the LEAs about what kind of information could be useful for CSIRTs, due to a lack of formal or informal exchanges between a CSIRT and a LEA.

Nevertheless, most CSIRTs and LEAs mentioned during the interview that an exchange of information from the LEA to the CSIRT would be very interesting in terms of creation of statistics and analysis of incidents across the country. Some CSIRTs and LEAs also mentioned the possibilities for joint actions in case of specific attacks.

CSIRTs might therefore better anticipate, through sharing of information, security incidents and prevent them, as well a better correlate data to highlight the motivation of threat actors.

2.2.2.5 Use case 5: Joint actions based on previous contributions

Based on the exchange of information and the collaboration that might follow, the sharing of information between CSIRTs and LEAs could motivate prevention campaigns and joint actions in case

of detection of an incident. In some countries, cooperation between CSIRTs and LEAs is already in place for some specific cases where collaboration allows a quicker response and analysis.

This kind of collaboration might also be enhanced by the creation of statistics on incidents (use case 3) where geographic areas that are targeted by specific security incidents could be visualised and therefore allow international actions across the EU.

2.2.2.6 Use case 6: ISP enrolment

Although the exchange of information with actors other than CSIRTs and LEAs is not part of the scope of this study, it was still observed based on the interviews, that CSIRTs often have a specific collaboration with other actors such as ISPs. In some countries, LEAs even ask CSIRTs to make specific requests to ISPs regarding botnets, allowing CSIRTs and ISPs to collaborate and take them down.

The exchange of information with ISPs, like the exchange between CSIRTs, is currently often unstructured, or not based on any taxonomy. The use of a taxonomy for these exchanges is expected to enable better communication by adding structure to the information exchanged, and thus enable faster processing

According to some members of the OAP 4.1 working group, the participation of ISPs in such exchanges might also improve their public image, by providing more security to their clients.

2.2.3 Synergies between this study and the OAP 4.1 working group

Many synergies can be observed between this study and the OAP 4.1 working group:

- **The goal of the study:** one of the goals of this study, the definition of a common taxonomy for the sharing of information between CSIRTs and LEAs, aligns directly with the first goal of the OAP 4.1 working group: the definition of a taxonomy for the exchange of information related to incidents and events in cyber security. However, while this study focuses specifically on CSIRTs and LEAs, the OAP 4.1 working group also considers the use of the taxonomy for the exchange of information with third parties as the next step to take, once the exchange of information is in place between CSIRTs and LEAs. One of the interviewees explained that although the OAP 4.1 working group would not directly focus on other parties than CSIRTs and LEAs, they consider that enabling the exchange of information using a specific taxonomy could motivate other parties to align to that taxonomy.
- **ENISA and EC3 are considered as an authority by both communities:** through the interviews it was observed that ENISA has the recognition in the CSIRT community to propose a taxonomy for the exchange of information between CSIRTs and LEAs. During these interviews, it was also observed that Europol had a similar authority regarding the LEAs. Therefore, it can be considered that both agencies have a level of authority to propose the use of a common taxonomy. This synergy has been confirmed during the 4th ENISA/EC3 workshop of the 8th and 9th October 2015[18] where the attendees, through anonymous voting, confirmed that ENISA and EC3 were best positioned to determine the CSIRT and LEA communities to adopt a common taxonomy and a sharing mechanism.

[18] 4th ENISA/EC3 workshop: https://www.enisa.europa.eu/activities/cert/events/4th-enisa-ec3-workshop

- **The next steps for the study:** the OAP 4.1 working group intends to improve the communication between CSIRTs and LEAs, if possible this year (2015), by attaining both second and third goals of the working group (defining an exchange standard and creating statistics). Along the same lines, this study proposes a roadmap for the introduction of a common taxonomy and the use of a sharing mechanism. Besides, this study is in line with the work performed by ENISA until now, which targets the enabling communication between CSIRTs and LEAs, and ENISA plans to continue working to attain this goal in the future.

2.2.4 Objectives of aligning this study with the OAP 4.1 working group for the taxonomy

The goal of this study is to propose a common taxonomy to improve information sharing between CSIRTs and LEAs, and the creation of a roadmap for the introduction of such a solution. Similarly, the OAP 4.1 working group intends to define a taxonomy for the exchange of information related to incidents and events in cyber security, and use it in an exchange standard. This section presents the several objectives of the alignment of the OAP 4.1 working group and this study.

2.2.4.1 Objective 1: Propose a common taxonomy to ensure alignment in the communities

An alignment of this study and the work done in the OAP 4.1 working group effectively results in a proposal for a common taxonomy. Since the OAP 4.1 working group and ENISA both operate at the EU level, proposing a common taxonomy to LEAs and CSIRTs shows that both communities are working towards the same goal.

2.2.4.2 Objective 2: Improve efficiency in the promotion of the taxonomy and exchange mechanism

As mentioned previously, ENISA and Europol are both considered authoritative when it comes to making recommendations for CSIRTs and LEAs. Their alignment on a common taxonomy is expected to encourage the use of the taxonomy by both communities. This should increase acceptance of the taxonomy in the Member States. This could be particularly relevant for LEAs, for which the implementation of a taxonomy might take a longer time than for the CSIRTs due to the way they are structured. On the contrary, having only EC3, for example, proposing a taxonomy to the LEAs and the CSIRTs could make it more challenging to promote the taxonomy to CSIRTs and could slow down the process of improving the exchange of information.

2.2.5 How both this study ant the OAP 4.1 working group are being aligned

To attain the objectives mentioned in the previous section, this study was conducted in collaboration with the OAP 4.1 working group. The first step of the collaboration with EC3 on this study was a joint meeting. By participating to this meeting on the OAP 4.1 working group on Monday 4 May 2015, direct information on the status of the OAP 4.1 working group was obtained. One of the examples of the alignment that was enabled by this meeting are the use cases: EC3 provided ENISA with a set of six use cases defined by the OAP 4.1 working group and, through the interviews performed for this study, the study team enriched the use cases with details on how and why the information about cyber incidents could be shared. In addition, EC3 provided support to ENISA

during this study by using the EUCTF[19] list to request an interview to the Member States LEAs. Furthermore, EC3 informed ENISA of the progress of the study regarding the taxonomy and the sharing mechanism that was being considered. For example, the current taxonomy being considered for the exchange of information between CSIRTs and LEAs was the taxonomy created by CERT.PT, and provided ENISA with a copy of this taxonomy.

Finally, this study aims at giving a better overview of the current situation in CSIRTs and LEAs across Member States and the next steps to take regarding the implementation of a taxonomy and a sharing mechanism between CSIRTs and LEAs, which should provide useful input to EC3 for the OAP 4.1 working group.

[19] Established in 2010, the European Cybercrime Task Force (EUCTF) is an expert group made up of representatives from Europol, Eurojust and the European Commission, working together with the heads of European Union cybercrime units to facilitate the cross-border fight against cybercrime.

2.3 Methodology for the selection of a taxonomy

One of the main purposes of this study is the proposal of a taxonomy for information exchange between CSIRTs and LEAs. This section details the methodology applied and the choices made to select a taxonomy that would fulfil the requirements expressed during the interviews of CSIRTs and LEAs and be updated with a new phenomenon that might be encountered, while staying in line with the OAP 4.1 working group. The chosen taxonomy will allow CSIRTs and LEAs to define a common language when sharing information, based on the classification[20] of events and incidents.

The first section **'Results of the desk research'** presents previous work performed by ENISA in the 'Fight against cybercrime' and 'Actionable information' area that have been considered in this study.

The second section **'Results of the analysed taxonomies'** details possible requirements for a future taxonomy that were expressed during the interviews. Associated with the use cases, this composes the base of the selection of a taxonomy for the information exchange.

This section is based on information collected during interviews with CSIRTs and LEAs. These interviews were mostly performed in a semi-structured manner, by asking the interviewees open questions and allowing them to provide any complementary information considered useful for this study. A total of 14 CSIRTs and 12 LEAs provided input, either by providing written answers, or during phone calls.

The third section **'Requirements for a taxonomy based on the needs for information CSIRTs and LEAs as expressed during the interviews'** presents a global overview of the taxonomies that were considered by this study, either obtained from the desk research or provided by Member States. It also lists taxonomies that could not be obtained due to their level of classification.

The last section **'Input from the OAP 4.1 working group about the taxonomy selected'** presents the input provided by OAP 4.1 working group about the taxonomy they selected and how the choice of the taxonomy has been made while keeping both activities aligned and answering the requirements detailed in the second section.

2.3.1 Results of the desk research

In 2010, ENISA started supporting operational collaboration initiatives between CSIRTs and LEAs. In this context, various activities have been launched since then. The following sections summarise the key input to this report.

The desk research supporting this study focused mainly on ENISA's work done in the fields of 'the fight against cybercrime' and 'Actionable Information'. It also keeps in mind the outcomes of the Impact Analysis of ENISA's support to Computer Emergency Response Teams (CERTs).[21] This impact assessment has served as a basis for a proposed roadmap to 2020. The following studies were taken into account.

[20] The repartition of events and incidents into classes, not to be confused with the level of classification of a document.
[21] Impact Analysis and Roadmap: https://www.enisa.europa.eu/activities/cert/other-work/supporting-the-cert-community-impact-analysis-and-roadmap

2.3.1.1 ENISA work done in the field of 'the fight against cybercrime'

- **A flair for sharing - encouraging information exchange between CERTs** - This report[22] focuses on the legal and regulatory aspects of information sharing and cross-border collaboration of national and governmental national and governmental CSIRTs in Europe.
- **The Fight against Cybercrime - Cooperation between CERTs and LEA in the fight against cybercrime** - The aim of this report is to improve the capability of national and governmental CSIRTs, to **address the NIS aspects of cybercrime**. It focuses on supporting national and governmental CSIRTs and their hosting organisations in the EU Member States in their collaboration with the LEAs. It also intends to be a first collection of practices collected from mature CSIRTs in Europe, including among other things workflows and collaboration with other key players, in particular different law enforcement authorities, in the fight against cybercrime.
- **Give and Take - Good practice Guide for Addressing NIS Aspects of Cybercrime -** The document constitutes a 'work in progress', a snapshot of the status of ENISAs support for CSIRTs and LEAs at the time of the publication, and includes good practice and recommendations for both communities.
- **The Directive on attacks against information systems - A Good Practice Collection for CERTs on the Directive on attacks against information systems** - This report provides an analysis of the legal framework created by the Directive, coupled with a stock taking on relevant existing national activities and good practices. Secondly, it identifies key areas and, where appropriate, guidelines and recommendations derived from these good practices.
- **Electronic evidence - a basic guide for First Responders** - The guide aims to be a practical tool explaining the principles of sound evidence gathering and raising the right questions for collecting and securing digital evidence.
- **ENISA's traditional workshop 'CERTs in Europe'** has been organised since 2005 for the national and governmental CSIRTs in Europe and is one of the most efficient and indispensable methods for ENISA in supporting teams in their daily work and improving their capabilities. In 2011 ENISA started to collaborate with Europol. The first joint workshop was held in Prague and had a focus on CSIRT cooperation with law enforcement. From 2012 the annual ENISA workshop was split into two parts, one part aims only at national and governmental CSIRTs and has a technical focus, and the other aims at both national and governmental CSIRTs and law enforcement representatives, organised together with Europol/EC3. While in 2014, the first part of the workshop focused on being an opportunity to provide EU national and governmental CSIRTs teams' technical specialists with a possibility to share and discuss about the latest developments and challenges with regard to CSIRTs services, the second part of the workshop (later renamed to ENISA/EC3 workshop) kept the focus on cooperation between national and governmental CSIRTs in Europe and their national Law Enforcement counterparts. Representatives from both communities were invited to these events.
- **The 4th ENISA/EC3 workshop**[23] – an annual gathering of both CSIRT and LEA communities, focused on cooperation between national and governmental CSIRTs in Europe and their national Law Enforcement counterparts, during which a presentation of this study was made

[22] A flair for sharing - encouraging information exchange between CERTs: https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing
[23] 4th ENISA/EC3 workshop: https://www.enisa.europa.eu/activities/cert/events/4th-enisa-ec3-workshop

and the draft of the report was sent to all attendees. The feedback received from the participants served as input to this study.

2.3.1.2 ENISA's work done in the field of 'Actionable Information'

Extracting timely information that can be immediately acted on from vast amounts of all types of data flowing in remains a challenge. This type of information is referred to as 'actionable information'[24]. In the field of data sharing between CSIRTs and LEAs, being able to extract actionable information from the data transferred as well as selecting the data to transfer to fit the need of the receiver is a central point.

- **Actionable Information for Security Incident Response study**[25] - This study is a good practice guide for the exchange and processing of actionable information.
- **Standards and tools for exchange and processing of actionable information inventory**[26] - This report is an inventory of 53 information sharing standards and 16 information management tools relevant to the concept of actionable information.
- **ENISA Threat Landscape 2014**[27] - This report consolidates the top cyber threats and emerging threat trends in various technological and application areas.

[24] Actionable Information: https://www.enisa.europa.eu/activities/cert/support/actionable-information
[25] Actionable Information for Security Incident Response study: https://www.enisa.europa.eu/activities/cert/support/actionable-information/actionable-information-for-security
[26] Standards and tools for exchange and processing of actionable information inventory: https://www.enisa.europa.eu/activities/cert/support/actionable-information
[27] ENISA Threat Landscape 2014: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

2.3.2 Results of the analysed taxonomies

To enable sharing of information, a common taxonomy should answer the needs of CSIRT and LEA communities. The classification offered by a common taxonomy should be acceptable for both communities while being easy to use and implement in any tool that is used, and be easy to adapt. This section reviews the pros and cons of each taxonomy presented in the first deliverable.

The table below provides an overview of the 'pros' and 'cons' of each taxonomy.

NR.	TAXONOMY	PROS	CONS
1.	**CERT NIC.LV taxonomy**	N/A	Outdated.
2.	**The common language**	N/A	Outdated.
3.	**The eCSIRT taxonomy**	N/A	Outdated.
4.	**CERT.PT taxonomy**	Proposed choice of OAP 4.1 working group. Owned by the OAP 4.1 working group. High-level. Already in use in Portugal.	Simplicity of the classification.
5.	**AVOIDIT taxonomy**	N/A	Limited recognition by the business.
6.	**Data Harmonization Ontology**	Created by CSIRTs. Ease of use.	Limited recognition by the business. Simplicity of the classification.
7.	**VERIS**	High level of detail. Significant recognition by the business.	Complexity. (More input and a better technical knowledge from the user required). Owned by a private entity.
8.	**CybOX**	High level of detail. Significant recognition by the business.	Complexity (More input and technical knowledge from the user required). Owned by MITRE[35].
9.	**Hungarian taxonomy**	*N/A due to classification*	*N/A due to classification*
10.	**Phänomene Cybercrime**	Details each element from a high-level point of view.	Crime-specific Draft version, in German
11.	**CSIRT-MU taxonomy**	High-level.	Limited amount of types of events.

NR.	TAXONOMY	PROS	CONS
12.	**Esquema nacional de seguridad Gestión de ciberincidentes**[28]	High-level. Considers classification, danger and potential impact.	Limited amount of types of events.

Table 1 - Pros and Cons of the studied taxonomies

2.3.2.1 Taxonomy 1, 2 and 3: The CERT NIC.LV taxonomy, 'the common language' and the eCISRT taxonomy

These three taxonomies are presented in the documentation on existing taxonomies on the ENISA website[29]. Although they may be an appropriate comparison point for the creation or the selection of a taxonomy, the website mentions that they are now outdated and should not be used apart as inspirational material to create a new taxonomy.

2.3.2.2 Taxonomy 4: The CERT.PT taxonomy

The CERT.PT taxonomy was presented by EC3 as the preferred choice of the common taxonomy (EC3 reached out to the LEA community through the EUCTF. At the time, no objections were raised by the LEA community).

Although named 'CERT.PT' taxonomy, it is a product of a collaboration between several European CSIRTs (from Austria, Belgium, Estonia and also CERT-EU) and the Portuguese police. CERT.PT worked in collaboration with the police to add value to the taxonomy by introducing international legal references into the taxonomy, reviewing the objectives of the taxonomy and proposing it to EC3 as a candidate for a common taxonomy.

One of the main advantages of this taxonomy is that it could be easily adapted to fit the needs of both communities or to take into account the new phenomena that could occur.

Secondly, the taxonomy intends to be precise while maintaining a high level of classification to be easily used and understood across the communities of CSIRTs and LEAs. If in the future, more details would become required for some parts of it, the taxonomy could be updated to add the required information.

Finally, the taxonomy is already in use by some LEAs and CSIRTs and seems to have proven its efficiency in the exchange of information.

However, one of the disadvantages is that the CERT.PT taxonomy is a very high-level classification. The categories of incidents and events presented in this taxonomy are very broad. Therefore, an incident described using the CERT.PT taxonomy would not provide many details regarding the

[28] Esquema nacional de seguridad Gestión de ciberincidentes: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html
[29] Existing taxonomies: https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-taxonomy/existing-taxonomies

incident itself. The taxonomy is therefore easy to use and statistics can created based on its classification, but it limits the level of details of the classification of an incident.

2.3.2.3 Taxonomy 5: The AVOIDIT taxonomy

The AVOIDIT[30] taxonomy is documented as a taxonomy to represent attacks in an innovative way to allow a detailed classification, by characterising the attacks by five classifiers: attack vector, target, operational impact, informational impact and defence. Although being innovative, this taxonomy has not currently reached acceptance by any of the communities and no implementation or use of it was found during the time of drafting this study.

2.3.2.4 Taxonomy 6: Data Harmonization Ontology

The ontology has been created by many CSIRTs as part of the AbuseHelper[31] activity.

The taxonomy provided for the classification of abuse events is well-documented and quite simple to use. It also defines key Indicators of Compromise (IOC) to be used as basis to communicate abuse events. It also contains details of required fields that should appear in every report sent.

Although more detailed than the CERT.PT taxonomy, it seems that it has not reached a critical mass of users and it seems to have a limited response from the business industry outside of the CSIRT community.

2.3.2.5 Taxonomy 7: The Vocabulary for Event Recording and Incident Sharing (VERIS)

This taxonomy[32] is available on the internet and seems to be quite complete and useful for the description of incidents. It has a good recognition by the business and can easily be implemented.

Although the VERIS taxonomy is an appropriate candidate and has additional features like the specific database to store information, the main difficulty is the adaptation to fit the needs of the CSIRT and LEA community. Adapting the taxonomy to the needs of this study is feasible, since the data is available on GitHub[33], but it would then deviate from the framework provided by Verizon and make it more challenging to use for a future expansion of the sharing between the CSIRT and LEA communities.

The level of complexity of the taxonomy seems to be rather high compared to others like the Data Harmonization Ontology or the CERT.PT taxonomy. It therefore allows a more fine-grained detail of events and incidents, but requires more input and a better technical knowledge from the user.

[30] AVOIDIT: A Cyber Attack Taxonomy: http://www.albany.edu/iasymposium/proceedings/2014/6-SimmonsEtAl.pdf
[31] AbuseHelper: https://bitbucket.org/clarifiednetworks/abusehelper/wiki/Home
[32] The Vocabulary for Event Recording and Incident Sharing: http://veriscommunity.net/
[33] GitHub is a web-based repository hosting service offering distributed revision control and source code management (SCM) functionality. https://github.com/

2.3.2.6 Taxonomy 8: Cyber Observable eXpression (CybOX)

The CybOX[34] taxonomy, provided by MITRE[35] in parallel to STIX[36] and TAXII[37], provides a well-structured taxonomy for threats and events and has a good acceptance by the business. Similarly to the VERIS taxonomy, it is available on the Internet but the main difficulty for this study is the fact that it is owned by MITRE and therefore not easily adaptable to the needs of the community without deviating from the original taxonomy.

The level of complexity of this taxonomy is rather high and requires more input and technical knowledge from the user. Therefore, it may prove more challenging to be used by LEA.

2.3.2.7 Taxonomy 9: The taxonomy used in Hungary by CSIRTs and LEAs

It was mentioned that a taxonomy, developed by the Hungarian police, was already in use in Hungary for the sharing of information between CSIRTs and LEAs. This taxonomy or concrete examples of its use could not be shared with ENISA as it is classified.

2.3.2.8 Taxonomy 10: Phänomene Cybercrime taxonomy

The Swiss Federal Police mentioned during their interview that they were drafting a taxonomy for the exchange of information in Switzerland and agreed to send it to ENISA to report on it in this study. The Swiss Federal Police taxonomy, named 'Phänomene Cybercrime' is currently only available in German. It is divided in three categories: 'Cyber-WK' (representing the general attacks), sexual offenses and defamation.

The 'Phänomene Cybercrime' taxonomy describes every type of attack and action in a detailed manner to avoid any confusion, but the information is classified according to the type of crime more than the type of attack. For example, 'Forbidden porn' is also part of that taxonomy, while it is not technically an attack but illegal use of a network. Although this type of taxonomy might be adapted for the exchange of information between LEAs, it might be less relevant for the CSIRTs.

2.3.2.9 Taxonomy 11: CSIRT-MU taxonomy, Czech Republic

CSIRT-MU mentioned during their interview that they were drafting a taxonomy for the exchange of information with the LEAs and agreed to send it to ENISA to use it in this study.

The CSIRT-MU taxonomy is high-level and contains around twenty types of attacks and their description, with links to the Czech law and the Decree on cyber security. It also contains indications for the CSIRT remediation and usable evidence.

[34] Cyber Observable eXpression (CybOX): https://cybox.mitre.org/
[35] MITRE is a not-for-profit organization that operates research and development centres sponsored by the federal government. http://www.mitre.org/
[36] Structured Threat Information eXpression, a structured language for cyber threat intelligence: https://stixproject.github.io/
[37] Trusted Automated eXchange of Indicator Information, a transport mechanism for the exchange of threat information: https://taxiiproject.github.io/

2.3.2.10 Taxonomy 12: Esquema nacional de seguridad Gestión de ciberincidentes

During feedback received after the workshop of the 4th ENISA/EC3 workshop, this taxonomy was presented by CCN-CERT[38]. This taxonomy includes issues that were encountered in Spain and has been published in May 2015 as part of the CCN-STIC-817 security guide issued by CCN-CERT.

The taxonomy includes three levels of classification: the type of cyber incidents, including type, description and subtype, the danger of these incidents and the potential impact.

Although the taxonomy is very broad (high-level classification) and lacks complexity compared to others like CybOX or VERIS, it is still easy to implement. Besides, the way it considers the different subtypes of classification (type, danger and impact) could be of use for CSIRTs and LEAs to estimate the importance of the problem.

2.3.3 Requirements for a taxonomy based on the needs for information CSIRTs and LEAs as expressed during the interviews

Throughout the 26 interviews, this study was able to capture requirements expressed by the different communities concerning the taxonomy for the exchange of information between CSIRTs and LEAs. This section details these requirements and how each taxonomy presented in this deliverable meets the requirements.

These requirements are considered as validated by the interviewees (14 CSIRTs and 12 LEA representatives) according to the following formula:

- At least 30% of the interviewees mentioned this information.
- At least 51% of the interviewees mentioning this information have agreed to the statement.

If these conditions are met, the information is considered as 'sufficiently justified' and the requirement based on this information should be taken into account for the selection of the taxonomy. If it is not the case, the information is mentioned in this study as 'information with limited justification' and the requirement won't be considered as verified by the community and is therefore not a priority requirement that the taxonomy should meet.

[38] CCN-CERT: national Spanish CSIRT: https://www.ccn-cert.cni.es/

The following table summarises the requirements expressed through the interviews.

NR.	REQUIREMENT	JUSTIFICATION [39]	VERIS	CYBOX	AVOIDIT	DHO [40]	CERT.PT	PHÄNOMENE CYBERCRIME	CISRT-MU	ENSGC [41]
1.	Take the level of maturity of the LEAs in term of technical capabilities into account	High	No	No	No	Yes	Yes	Yes	Yes	Yes
2.	Be able to transmit high- and low-level data	High	Yes	Yes	No	No	No	No	No	No
3.	Be as complete as possible regarding the types of events and incidents	Limited	Yes	Yes	Yes	No	No	No	No	No
4.	Have a classification[42] that is stable throughout time	Limited	Yes	Yes	Yes	Yes	Yes	No	No	N/A[43]
5.	Have information fields that are mandatory	Limited	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
6.	Have a description of terms used to agree upon terminology	Limited	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7.	Be updated regularly during meetings with the stakeholders	Limited	No	No	No	No	Planned[44]	N/A[45]	N/A[14]	N/A[46]
8.	Take into account the Budapest Convention[47] and the Cybercrime Directive[48]	Limited	No	No	No	No	Yes	Yes	Yes	No
9.	The taxonomy should be mapped to the relevant EU legislation and where possible to the legislation in the Member States	High	No	No	No	No	Yes	No	Yes	No

Table 2 - requirements for a taxonomy

[39] This column shows whether information has been sufficiently justified or less expressed by the members of the CERT and LEA communities during the interviews.
[40] DHO: Data Harmonization Ontology.
[41] ENSGC: Esquema nacional de seguridad Gestión de ciberincidentes.
[42] The repartition of events and incidents into classes, not to be confused with the level of classification of a document.
[43] The update of the classification has not been given at the time of the study.
[44] As detailed below, if the CERT.PT taxonomy is confirmed by the OAP 4.1 working group as the taxonomy to be used for information exchange, they will ensure regular updates of the taxonomy through bi-annual meetings of stakeholders.
[45] The update of this taxonomy is not yet relevant since it is at draft version.
[46] The update of the classification has not been given at the time of the study.
[47] Convention on Cybercrime, Budapest, 23.XI.2001: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
[48] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

During the 4th ENISA/EC3 workshop, these requirements were presented to the attendees and the majority of them validated them as representative (of the needs of both taxonomies) during the anonymous voting session, although 38% of the voters answered that the requirements were not representative. It must be noted that this only represents the opinion of the attendees of the workshop and therefore does not represent the opinion of either community.

The following sections detail the different requirements and how the taxonomies meet these requirements.

2.3.3.1 Requirement 1: The taxonomy should take the level of maturity of LEAs in term of technical capabilities into account

The first requirement concerns the abilities of LEAs to implement advanced technical solutions. Many interviewees mentioned that the technical abilities of the LEAs were often less advanced than the CSIRTs technical capacity. This requirement is one of the justified pieces of information obtained during the interviews and can therefore be considered as a main requirement.

To take that difference in technical level into account, the taxonomy should be simple to implement and understand, with a clear definition of its vocabulary. This might help in overcoming the difference in capabilities to implement a taxonomy that was observed between CSIRTs and LEAs. This would allow all stakeholders to implement and use the taxonomy in an easy and efficient manner.

The level of detail of a common taxonomy should also be accessible enough to describe events and incidents in a precise way while still being understandable and easily usable. For example, having too many levels of detail for the type of events and incidents (if one event has several subtypes which in turn have several subtypes etc.) would make classification complex for the user, while being allowed to divide the information between a limited amount of high-level classes would limit the level of detail but allow the user to easily classify the information.

Regarding the available taxonomies, the CERT.PT taxonomy, the Esquema nacional de seguridad Gestión de ciberincidentes, the Phänomene Cybercrime and the Data Harmonization Ontology could be considered as easy to use while VERIS, CybOX and the AVOIDIT taxonomies are more complex to use because of the level of detail available. The CSIRT-MU taxonomy, although easy to use, might be unnecessarily simple for most countries in the EU.

This requirement was supported by the votes of the workshop where the ease of use of the taxonomy was confirmed as an important element for the exchange of information.

2.3.3.2 Requirement 2: The taxonomy should fit for both high- and low-level data

Throughout the interviews, we observed that CSIRTs and LEAs share both high- and low-level data, even if the exchange of information is not structured. For the taxonomy to be adopted by all parties, it would be useful to be able to make use of the taxonomy to classify the information that is already exchanged – this is one of the justified pieces of information obtained during the interviews and can therefore be considered as the main requirement.

If a common taxonomy allows the user to classify the information that is already sent between CSIRTs and LEAs, this would have a positive effect on the perception of the use of the taxonomy. In addition, if a taxonomy would be kept up-to-date by regular adaptations to new phenomena, it might allow both communities to integrate into the taxonomy those types of information that cannot yet be classified.

Regarding the sharing of low-level data (the three first levels of the pyramid of pain[49]: hash values, IP addresses and domain names), all taxonomies allow the sharing of such information. The difference in the taxonomies appears when the stakeholders want to share high-level information (such as tactics, techniques and procedures). While the VERIS and the CybOX taxonomies allow the sharing of (at least a part of) such information, the AVOIDIT taxonomy is not as complete, and the CERT.PT taxonomy, the Esquema nacional de seguridad Gestión de ciberincidentes, the Data Harmonisation Ontology, the CSIRT-MU taxonomy and the Phänomene Cybercrime are not as detailed and focus more on incidents and events.

2.3.3.3 Requirement 3: The taxonomy should be as complete as possible regarding the types of events and incidents

This information is not part of the information considered as being sufficiently justified since it was less expressed by the members of the communities during the interviews.

Three CSIRT representatives mentioned during the interviews that, in order to be useful for the exchange of information, a common taxonomy should be exhaustive regarding the types of events and incidents. Having an exhaustive taxonomy would allow CSIRTs and LEAs to fit any kind of event and incident into the classification of the taxonomy thereby possibly raising the acceptance of the taxonomy.

This requirement can be linked with the first one ('the taxonomy should take the level of maturity of the LEAs in term of technical capabilities into account') since the level of complexity of a taxonomy is proportional to its completeness in terms of events and incidents. While all taxonomies try to be as complete as possible, the level of detail and subcategories about an incident or an event may vary from one to another. In that regard, VERIS, the AVOIDIT taxonomy and CybOX are the most complete (but also the most complex) while, the CERT.PT taxonomy, the CSIRT-MU taxonomy, the Phänomene Cybercrime and the Data Harmonization Ontology define events and incidents with high-level description. The Esquema nacional de seguridad Gestión de ciberincidentes also falls in that category but has an interesting point of view on classification, danger and impact.

2.3.3.4 Requirement 4: The format of the taxonomy should be stable in time

This information is not part of the information considered as being sufficiently justified since it was less expressed by the members of the communities during the interviews.

During the interviews, two CSIRTs mentioned that, to ensure that a taxonomy would not constantly change, it should stay stable throughout time and avoid being adapted too regularly. This would allow both communities to use the taxonomy without having to update its implementation into tools too often, which would be time and resource intensive.

Based on the comparison with the other requirements, we can see that this requirement should stay in balance with the possibility to update the taxonomy. While updating the taxonomy too often might be a problem for CSIRTs and LEAs, it also needs to be kept up-to-date to take new phenomena into account.

[49] The pyramid of pain is a diagram that shows the relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny those indicators to them: http://detect-respond.blogspot.fr/2013/03/the-pyramid-of-pain.html.

Regarding the stability of a taxonomy, the VERIS taxonomy has been updated last year (2014) and Verizon is planning an annual or bi-annual update. CybOX is also updated with a mean of twice a year since 2011. However, the Data Harmonisation Ontology, the CERT.PT taxonomy and the AVOIDIT taxonomy have not been updated since they were firstly drawn up. It must be noted that if the OAP 4.1 working group selects the CERT.PT taxonomy as the common taxonomy to use for the exchange of information between CSIRTs and LEAs, they plan to update the taxonomy yearly through meetings of its stakeholders. For the CSIRT-MU taxonomy and the Phänomene Cybercrime, since they are still at draft version, they might evolve anytime.

The case of the Esquema nacional de seguridad Gestión de ciberincidentes is a bit specific since its release date was in May 2015, the year of this report. It has therefore not been updated yet.

During the ENISA/EC3 workshop, the attendees mentioned the fact that the stability of the taxonomy was indeed an important concern for the exchange of information.

2.3.3.5 Requirement 5: Some information should be mandatory in the taxonomy

This information is not part of the information considered as being sufficiently justified since it was less expressed by the members of the CSIRT and respectively the LEA communities during the interviews.

Three CSIRTs and one LEA representative mentioned during the interviews that some fields of the taxonomy should always be mandatory when the taxonomy is used to classify information. That way, if the information is exchanged based on the proposed taxonomy, the recipient of the information can be sure that a minimal set of information will always be provided.

Most of the fields in the CybOX taxonomy are not mandatory, while VERIS and the Data Harmonization Ontology have some mandatory fields. The CERT.PT, the Esquema nacional de seguridad Gestión de ciberincidentes, the CSIRT-MU taxonomy, the Phänomene Cybercrime and the AVOIDIT taxonomy do not specify which fields are mandatory but are high-level description so all information can be considered as mandatory by default (missing information would void the use of these taxonomies).

2.3.3.6 Requirement 6: The taxonomy should have a description of the terms used to agree upon terminology

This information is not part of the information considered as being sufficiently justified since it was less expressed by the members of the communities during the interviews.

One CSIRT representative and two LEA representatives mentioned during the interviews that, to ensure that CSIRTs and LEAs use the same vocabulary regarding cyber incidents, the taxonomy should describe the terms used to classify the information, such as types of events and incidents. This would avoid confusion while classifying or sharing information based on the taxonomy.

All taxonomies presented in this study describe the terminology used to classify information.

During the 4th ENISA/EC3 workshop, the attendees also mentioned that this requirement was important to be able to classify the information correctly, and that the description of each element of the taxonomy was necessary.

2.3.3.7 Requirement 7: The taxonomy should be updated regularly during meetings with its stakeholders

This information is not part of the information considered as being sufficiently justified since it was less expressed by the members of the communities during the interviews.

During the interviews, one CSIRT representative and four LEA representatives mentioned that the taxonomy should be updated on a regular basis. This should be done by having regular meetings between the relevant stakeholders using the taxonomy. Updating the taxonomy would ensure that it stays up-to-date and adapts to new phenomena encountered by the stakeholders.

VERIS and CybOX are maintained by institutions that manage their updates, although they take into account users' remarks. The data Harmonization Ontology and the AVOIDIT taxonomy are not updated anymore and the CERT.PT will be adapted in the future if it is chosen by the OAP 4.1 working group as the promoted common taxonomy for this information exchange. The CSIRT-MU taxonomy and the Phänomene Cybercrime are currently being drafted so their update process is not yet known. Regarding the Esquema nacional de seguridad Gestión de ciberincidentes, it has just been created so the update process is not known yet at the time of this study.

During the 4th ENISA/EC3 workshop, the update of the taxonomy was indeed mentioned as important for the evolution and the use of the taxonomy in the exchange of information.

2.3.3.8 Requirement 8: The Budapest Convention and the Cybercrime Directive should be taken as legal basis for the taxonomy

This information is not part of the *information considered as being sufficiently justified* since it was less expressed by the members of the communities during the interviews.

Some LEA representatives mentioned during the interview that the Budapest Convention[50] and the Cybercrime Directive[51] should be taken as legal basis for the taxonomy. This element was also supported by an anonymous vote during the 4th ENISA/EC3 workshop where 67% of the voters were of the opinion that the taxonomy should include a mapping to both European and National legislations.

VERIS and CybOX are US-based and do not take into account the Budapest Convention and the Cybercrime Directive. In addition, the Data Harmonization Ontology and the AVOIDIT taxonomy do not make any mention of it. The Phänomene Cybercrime and the Esquema nacional de seguridad Gestión de ciberincidentes are not linked with the Budapest Convention and the Cybercrime Directive. Therefore, the CERT.PT taxonomy and the CSIRT-MU taxonomy are the only ones aligning to this Convention and Directive since it has been constructed for the exchange of information with the European LEA.

[50] Convention on Cyber crime, Budapest, 23.XI.2001: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[51] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

2.3.3.9 Requirement 9: The taxonomy should be mapped to the relevant EU and Council of Europe legal framework and where possible to legislation in the Member States

Based on the specification of this study, the selected taxonomy should be mapped to the relevant EU legislation such as the Cybercrime Directive, to the Budapest Convention and, where possible, to the national legislation of the Member States.

Among the taxonomies examined by this study, the CERT.PT taxonomy and the CSIRT-MU taxonomy are the only ones that reference the legislation – they specify EU legislation and the corresponding national regulations. It must be underlined that the Esquema nacional de seguridad Gestión de ciberincidentes underlines the procedure of a declaration of an incident to the CCN-CERT.

2.3.3.10 Other possible requirements based on feedback received after the ENISA/EC3 workshop

In addition to the requirements mentioned in the previous sections, one CSIRT is of the opinion that a taxonomy should support the categorisation of classified information, such as EU SECRET and NATO SECRET. However, based on the information collected during the interviews, it seems that in the current context of information sharing between CSIRTs and LEAs, it does not seem that such information is exchanged actively. Therefore such a requirement may be further considered in a future context, but not within the scope of this study

2.3.4 Input from the OAP 4.1 working group regarding the taxonomy selected

During the OAP 4.1 working group meeting in The Hague on the 4 May 2015 with EC3 and through interviews with two LEA representatives, the following information was provided:

- The OAP 4.1 working group can relate to the definition of a taxonomy[52] used in this study: a taxonomy is most often defined as a classification of terms and has a close relationship with the use of ontology.
- The OAP 4.1 working group is currently setting up a governance structure in order to revise the common taxonomy during bi-annual meetings.
- The OAP 4.1 working group considers that STIX could possibly be a good candidate as sharing mechanism to use for the exchange of information between CSIRTs and LEAs using the chosen common taxonomy. To be able to use STIX, the OAP 4.1 working group should define STIX profiles[53] for LEAs.

This input provided by the OAP 4.1 working group stakeholders has been taken into consideration for the choice of the taxonomy and a sharing mechanism for the exchange of information between CSIRTs and LEAs. The possibilities of alignment of this study to the OAP 4.1 working group were also taken into account as they might provide the advantages previously mentioned in this document (in 'Objectives of aligning this study with the OAP 4.1 working group for the taxonomy').

[52] Ontology and taxonomies for critical infrastructures: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/ontology

[53] Profiles are a mechanism to describe a particular usage of STIX as practiced by a community, organization, or tool.

2.4 Verification that the preferred taxonomy (CERT.PT taxonomy) fits the requirements highlighted during the interviews and identified from desk research

This section presents the result of the analysis of the taxonomies considered by this study. For each taxonomy, this section verifies whether it meets requirements identified at the previous section.

2.4.1 Why the CERT.PT taxonomy is best adapted for the exchange of information between both communities

As detailed in the next section (the analysis of the requirements met by each taxonomy), the CERT.PT taxonomy seems to be best fitted for the exchange of information, based on the minor complexity of the taxonomy, its possibilities of evolution based on the needs of both communities and its legal basis for the consideration of events and incidents.

Proposing the CERT.PT taxonomy may also have the advantage of aligning this study to the OAP 4.1 working group, as detailed in the section 'Objectives of aligning this study with the OAP 4.1 working group for the taxonomy'.

2.4.2 Analysis of the requirements met by each taxonomy

In the summary table in the previous section 'Requirements for a taxonomy based on the needs for information CSIRTs and LEAs as expressed during the interviews', we can observe two tendencies in the taxonomies considered by this study:

- Taxonomies tending to be as detailed as possible, that are therefore complex to use but exhaustive, managed by organisations that have the ownership of the taxonomy, and
- High-level taxonomies that are easy to use and do not contain a highly detailed structure to describe the incidents and events.

This can be determined by observing the mapping of the first three requirements ('The taxonomy should take the level of maturity of LEAs in term of technical capabilities into account', 'The taxonomy should be able to transmit high- and low-level data' and 'The taxonomy should be as complete as possible regarding the types of events and incidents').

Based on our observations, we can see that the use of a complex and exhaustive taxonomy may not be a solution per se – the choice between complexity and completeness should be done according to the capabilities of the stakeholders in information exchange.

For the exchange of information between CSIRTs and LEAs, considering the high difference in terms of technical capabilities between Member States, we consider that a better approach might be to start with a taxonomy that is simple to use to make sure that it gets accepted by all CSIRTs and LEAs as a common basis. At a later stage, if there would be a preference for an increase of the level of detail, the taxonomy could be further elaborated by the stakeholders to meet the new requirements. Towards this end, two taxonomies would fit the best to the first three requirements, the Data Harmonization Ontology and the CERT.PT taxonomy.

The preference for the ease of use of a taxonomy was further supported by an anonymous vote during the 4th ENISA/EC3 workshop where a majority of respondents expressed that the ease of use of a taxonomy should be the priority against the level of detail. Additionally, 30% of the voters answered that both should be considered as priority. The need for an easy-to-use but also detailed taxonomy might be answered by starting to exchange information based on a simple taxonomy and upgrade it to a higher level of detail afterwards, when the use of the taxonomy would be well implemented.

According to the requirements that were expressed during the interviewed CSIRTs and LEAs, we can observe that the CERT.PT taxonomy is best fitted for the exchange of information between CSIRTs and LEAs since it is based on the Budapest Convention and the Cybercrime Directive, and that there is a possibility that it may be selected by the OAP 4.1 working group as the taxonomy to be used for information sharing between CSIRTs and LEAs, and therefore be regularly updated based on the requirements of the communities.

The CERT.PT taxonomy is also the only taxonomy presented in this study to reference EU legislation, which has been identified as a requirement, which was supported by the votes during the 4th ENISA/EC3 workshop.

The following table presents a summary of the possible advantages of using the CERT.PT taxonomy for the exchange of information between CSIRTs and LEAs:

NR.	ADVANTAGES OF THE CERT.PT TAXONOMY
1.	The CERT.PT taxonomy is easy to use and implement since it describes events and incidents at a high level.
2.	The CERT.PT taxonomy, if it is chosen by the OAP 4.1 working group, will be updated regularly through meetings of its stakeholders.
3.	The classification provided by the CERT.PT taxonomy makes all fields mandatory, which provides consistency for the creation of statistics.
4.	The CERT.PT is based on the Budapest Convention and the Cybercrime Directive.
5.	The events and incidents mentioned in the CERT.PT taxonomy are described, which provides a common understanding of used terms.

Table 3 - Advantages of the CERT.PT taxonomy

In addition to the advantage that the CERT.PT taxonomy is being considered as a potential candidate by the OAP 4.1 working group, it is already being implemented into some tools by some CSIRTs to exchange information according to its classification and has proven efficient.

During the 4th ENISA/EC3 workshop, the participants confirmed, during the closing session of the workshop, that according to them the CERT.PT taxonomy is sufficiently accepted by the CSIRT and LEA communities.

For the future update of the CERT.PT taxonomy, the use of the other inputs and feedback provided after the 4th ENISA/EC3 workshop, such as the Esquema nacional de seguridad Gestión de ciberincidentes and some other comments on the CERT.PT taxonomy should be used during the first

meeting of the CERT.PT governance structure to evaluate the input these studies could provide for the current version of the CERT.PT taxonomy.

2.5 Proposal for a sharing mechanism for the selected taxonomy

A clear distinction should be made between a **taxonomy**, a **sharing mechanism** and a **sharing platform** to avoid any possible confusion. While a taxonomy is a way of describing information through classification, a sharing mechanism structures the way the information is encoded. For example, a sharing mechanism might provide rules for names and positions of XML tags to allow a file to be treated automatically. Finally, a sharing platform is a tool allowing to share information. It is not mandatory to have such a platform – files containing information structured according to a standard and classified according to a taxonomy could simply be sent by e-mail, for example. Nevertheless, the use of a sharing platform allows users to easily share information in a structured way.

While a taxonomy allows classification of the information, it does not provide a format for the representation or the sharing of the information. This section presents the different requirements for the sharing mechanism obtained through desk research and interviews, and observes how sharing mechanisms taken into consideration for this study meet these requirements. **The last part justifies the choice of STIX as the proposed sharing mechanism and possibilities of future alignment with the OAP 4.1 working group.** However, the choice of STIX as the sharing mechanism is not yet fully supported by both communities, as explained in section 2.5.3.

2.5.1 Requirements for the sharing mechanism highlighted by the desk research

Based on the desk research, information and recommendations for sharing mechanisms for the exchange of information is detailed here. This information is not always focused on CSIRTs and LEAs but more generally speaking about information exchange. These requirements and the requirements highlighted through the interviews (in section 2.5.2) have been supported by the vote of the attendees of the 4th ENISA/EC3 workshop where the feedback about them was positive – 83% of voters found these requirements 'likely representative' and 17% of them found the requirements 'very much representative'.

2.5.1.1 Requirement 1: The new sharing mechanism should not be a new standard [54]

Considering the amount of already existing initiatives, creating a new standard for the exchange of information between CSIRTs and LEAs could hinder the acceptance of the mechanism by CSIRTs and LEAs, and later on by third parties (considering that the OAP 4.1 working group is also targeting the use of the taxonomy and the sharing mechanism by the private sector).

Therefore, this study was directed towards the proposal for the use of an existing mechanism instead of the creation of a new one.

[54] Good practice guide for addressing NIS aspects of cybercrime: https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime/at_download/fullReport

2.5.1.2 Requirement 2: The source of the data of the sharing mechanism should be referenced, including the originating organisation, the transport mechanism and the data format[55]

For information to be actionable, there must be a clear indication of its origin. Based on the source of the data, the receiver of the information can decide to trust or not to trust the information received. The sharing mechanism should therefore allow its users to indicate the details of the source of the information transmitted.

2.5.1.3 Requirement 3: The sharing mechanism should have a level of acceptance among the business[56]

Until recently, none of the mechanisms available to structure information exchange were considered popular among the private sector. Nowadays, STIX is growing in popularity and is progressively turning into a de facto standard. It is considered as a reliable and exhaustive tool to structure information, and it is conveniently provided with the specification for a sharing mechanism, TAXII.

2.5.2 Requirements for the sharing mechanism highlighted through interviews

2.5.2.1 Requirement 1: The sharing mechanism should be considered as an appropriate tool for the exchange of information between CSIRTs and LEAs

Through the interviews, it appeared that CSIRTs and LEAs consider STIX as an appropriate tool for the exchange of information between CSIRTs and LEAs. Although some of the CSIRTs and the LEAs pointed out its complexity, most of them considered it as adaptable for information sharing.

The respondents also mentioned that, to be able to use STIX for information sharing, profiles would have to be defined for LEAs. The profiles allow users to describe how they use STIX – what kind of information they need, which parts of it should or should not be indicated in the information transmitted. For example, if a user of STIX just wants to receive information about spam e-mails, he could specify that the type of information he wants to receive is about spam, that he only needs the observables and indicators in the information and does not need details about the target, the attacker etc.

2.5.2.2 Requirement 2: The lack of human resources should not be an obstacle for the implementation of a standard

While some CSIRTs and LEAs said that implementing a standard to share information would not be a problem, some others mentioned that, considering their lack of human resources, implementing such a tool would be rather resource intensive.

[55] Actionable information for security: https://www.enisa.europa.eu/activities/cert/support/actionable-information/actionable-information-for-security/at_download/fullReport
[56] Standards and tools for exchange and processing of actionable information: http://www.enisa.europa.eu/activities/cert/support/actionable-information/standards-and-tools-for-exchange-and-processing-of-actionable-information/at_download/fullReport

2.5.3 Why STIX could be an appropriate sharing mechanism

Although multiple standards exist for the sharing of information, STIX appears to be the preferred mechanism for the exchange mechanism, also recognised by the CSIRT and LEA communities as a suitable candidate for a sharing mechanism, although its use for the exchange of information between CSIRTs and LEAS is still under discussion. Indeed, using STIX would avoid rebuilding a standard from scratch, which would represent a huge amount of work. It is also a mechanism that is widely known and becoming a de facto standard according to the ENISA study 'Standards and tools for exchange and processing of actionable information'[57].

STIX allows for a very close description of information – including the detailed description of the source of the data exchanged, which is a requirement that has been pointed out during the desk research. In addition, as STIX is a structured language to describe information, it can be implemented together with any cyber incidents taxonomy. Besides, the STIX model is constituted of different elements that relate to each other, which makes it feasible to use a step-by-step approach in its implementation, by implementing the different parts of the model. In this process, the basic parts of the STIX model could be implemented first, such as observables (the lowest element of the Pyramid of Pain[49]), and then grown in complexity by adding other elements of the model when feasible.

Regarding the lack of resources mentioned by some of the Member States, there might be ways to overcome the complexity of the implementation of the tool, like cooperation between CSIRTs and LEAs to implement it, specific help from ENISA or EC3, centralisation of a platform, etc. However, these situations should be treated on a case-by-case basis.

Although a sharing mechanism would offer advantages, the use of sharing mechanisms and a sharing platform is not supported by all stakeholders. It appeared through the 4th ENISA/EC3 workshop feedback session that some members of the community are not inclined to use STIX due to its complexity, but also that some of them might prefer to use independent sharing mechanisms on a case-by-case basis by taking into account the needs of the receiver of the information exchanged – such as using a CSV file to send information to an ISP. Therefore, a separate study should be set-up once the taxonomy has been implemented to see if there is sufficient demand for a common sharing mechanism or if the local existing mechanisms in place should be kept. Alternatively, if a unique sharing mechanism would be chosen, STIX is a 'good enough' solution according to the feedback received during the workshop. If needed, it might also be implemented step-by-step to reduce the complexity of the mechanism.

2.6 Proposed model to adapt the selected taxonomy to new phenomena

For the taxonomy to be used by the CSIRT and LEA communities, it should be regularly updated to respond to the new needs of each community and the new phenomena appearing. This section details the requirements for this update process that were highlighted by the interviews and the proposed model for the regular update of the taxonomy.

[57] Source: http://www.enisa.europa.eu/activities/cert/support/actionable-information/standards-and-tools-for-exchange-and-processing-of-actionable-information

2.6.1 Requirements for maintaining a taxonomy highlighted by the interviews

This section presents requirements obtained through the interviews of CSIRTs and LEAs that should be met by the model to adapt the chosen taxonomy.

2.6.1.1 Requirement 1: The update of the taxonomy and the exchange of information should be supported by informal personal meetings

This is one of the pieces of justified information – all the CSIRTs and LEAs mentioning personal meetings agreed that these meetings were necessary to maintain trust and keep the exchange of information alive. While this is not a requirement directly addressed to the update of the taxonomy, it adds to the following requirement ('the update of the taxonomy should be performed regularly by doing meetings with the stakeholders'). See below section.

Indeed, since personal meetings are considered vital to keep the exchange of information going, these meetings could also be used to discuss the taxonomy and the need to update it to new phenomena.

2.6.1.2 Requirement 2: The update of the taxonomy should be performed regularly by regular meetings with the stakeholders

A number of CSIRTs and LEA mentioned that, to ensure that the taxonomy is updated and kept in line with the requirements of the communities, meetings should take place regularly (at least once a year) to ensure that the taxonomy stays 'alive'. The more that input is received from the users of the taxonomy, the more that the taxonomy will be adapted to the needs and, therefore, used.

2.6.2 Model to adapt the taxonomy based on the requirements

Based on our observations, we can divide the process of updating taxonomies into two models: 'dynamic' and 'unidirectional'.

The **dynamic update of a taxonomy** is done through meetings happening at regular intervals. During these meetings, the stakeholders (owners, users, etc.) meet and share their experience and their wishes regarding the evolution of the taxonomy. These meetings can be physical but online meetings are also sufficient to update the taxonomy.

The **unidirectional update of a taxonomy** is usually in place when the taxonomy is owned by an entity: users send a request for an update of the taxonomy and the owner of the taxonomy accepts them and integrates them into the taxonomy or simply refuses them.

Regarding the update of the proposed common taxonomy for the exchange of information between CSIRTs and LEAs, considering the low amount of stakeholders and the intention to be adapted to the needs of the stakeholders, we recommend to implement a dynamic update of the taxonomy by setting up regular meetings.

Also, a structure should be put in place to allow exceptional reviews of the taxonomy. In case of an urgent need, this would allow the users of the taxonomy to request a change to the taxonomy outside of the regular meetings, to meet new urgent needs.

The OAP 4.1 working group also considers regular meetings of the stakeholders to adapt the taxonomy as a good way to proceed for its updates. They were setting up such meetings at the time of writing of this report (2015).

During the 4th ENISA/EC3 workshop, this 'update model' based on regular meetings of the stakeholders was supported by the majority of the voters. However, a concern about the costs for such meetings was also expressed, but these could be avoided by co-locating meetings with another meeting addressing the same communities, such as the ENISA/EC3 workshops.

3 Proposal for a roadmap for the use of the taxonomy in a sharing solution

Once a common taxonomy has been agreed, endorsed by ENISA and EC3 and accepted by the CSIRT and LEA communities, the classification of the information proposed by the taxonomy can be effectively used in the exchange of information between both communities. The taxonomy should be used to further assist CSIRTs and LEAs in improving the information exchange and in accessing information if the taxonomy has been effectively 'implemented' by them, or assigned to content, in some way.

To achieve that goal, a mechanism to exchange the information based on the taxonomy classification should be chosen, refined and further applied by the CSIRT and LEA communities.

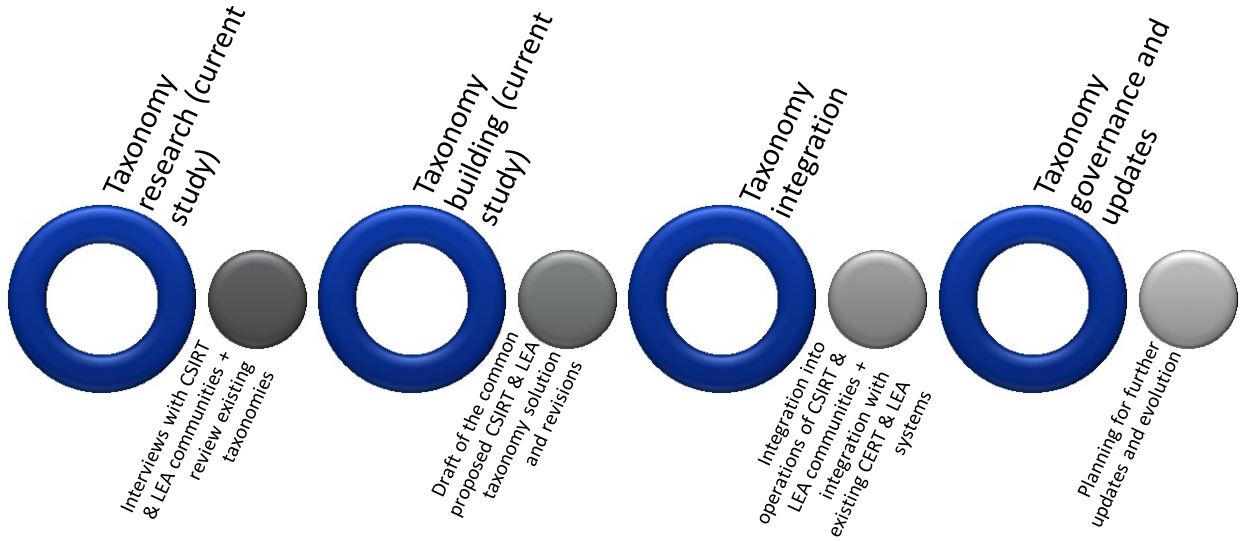
Such a mechanism can be either supported by existing or further systems and technologies in place at the CSIRTs and LEAs – with anticipated long-terms benefits in terms of decreasing necessary effort/cost for exchanging information – or can be based only on agreements and protocols that implement the taxonomy.

Based on our observations, without an agreed-upon mechanism, the exchange of data, even with a common language, would remain unstructured and therefore could not be automatically processed.

For example, if a LEA and a CSIRT have an agreement on the taxonomy to use for the exchange of information between them but have no agreement on a sharing mechanism, the LEA might send information to the CSIRT in a simple text format. The CSIRT would be able to understand the information the same way as the LEA thanks to the taxonomy, but they would not be able to automatically enter this information into their systems without transforming it into the right format. Having a common exchange mechanism would ensure that the format of the file that is exchanged is the same, and therefore can easily be integrated in the tools of every receiver.

3.1 Key tasks to perform for the implementation of the taxonomy

Based on the desk research, the interviews and the goals of the OAP 4.1 working group, this section presents a roadmap, consisting of a set of short-term and long-term actions proposed for the implementation of an information exchange between CSIRTs and LEAs communities. Conceptually, these short-term and long-term actions can be grouped in the following categories, corresponding to the typical phases of implementation for the taxonomies:



Key success factors for the implementation of the proposed roadmap consist of:

- Integration into the day-to-day operations of CSIRTs and LEAs, eventually supported by a sharing platform allowing for integration with the existing technical systems and technologies in place is critical for the success of the taxonomy adoption. It is key that once the taxonomy has been validated by end-users, it needs to be completely integrated into the systems and technologies that are in place, or in the planned new ones (e.g. common sharing platform). Changes and refinements to the taxonomy are usually further needed at this stage – in order to allow for integration adjustments for multiple technical systems and technologies in place.

- Good governance of the taxonomy is critical to maintain its long-term stability and growth. For this, creating clear policies to allow the community of CSIRT and LEA stakeholders to effectively manage the taxonomy and its changes is a key success factor. This needs to be supported by a simple and transparent governance plan.

- Achieving a well-managed roll-out of a common taxonomy can emphasise a number of benefits for CSIRTs and LEAs, in terms of lower efforts / costs for information exchange, creation and retrieval.

- Awareness and a proper training to involved CSIRTs and LEAs for the roll-out and effective use of the taxonomy.

- Further linking the taxonomy with an existing legislation of the Member States (e.g. based on the demand of the Member States) may contribute to a faster speed of adoption of the taxonomy – by overcoming limitations of the CSIRT and LEA mandates and possible other limits coming from the legislative framework.
- A well-defined and well-organized system for adoption of the taxonomy allows to connect the relevant CSIRT and LEA content and experts while improving information exchange, ensuring a proper information security and data compliance.

3.1.1 Roadmap summary

This section presents an overview of the proposed roadmap to implement the sharing of information between CSIRTs and LEAs by using the defined taxonomy. The numbering of the actions corresponds to the sequence in which the actions must be performed. Each element is detailed in the next section (see: 'Description of the roadmap actions').

NR.	PROPOSED ACTION	COMPLEXITY	WHO	DEPENDENCIES	RESOURCES	TIMELINE[58]
1.	Creation of a governance structure for the update of the taxonomy to new phenomena – supported by a simple and transparent governance plan. Diffusion of the taxonomy to the CSIRT & LEA communities. Identification of the participants for each CSIRT & LEA. Organisation and planning of the meetings.	Low	EC3 and ENISA	-	Medium	Short term
2.	Carry out a study to assess the need for a sharing mechanism	Medium	ENISA	-	Medium	Short to medium term
3.	Adaptation of the chosen sharing mechanism(s) to the taxonomy.	High	EC3, CERT EU, LEAs and CSIRTs	Need for a sharing mechanism	Medium	Medium term
4.	If there is a demand for a common sharing mechanism: choice of a sharing platform and an implementation model (distributed or global platform) for the exchange of messages across Member States.	High	EC3 and ENISA	Adapting the chosen sharing mechanism to the taxonomy	High	Medium term

[58] 'Short term' means one to two years, 'medium term' means two to three years and 'long term' means three to five years.

NR.	PROPOSED ACTION	COMPLEXITY	WHO	DEPENDENCIES	RESOURCES	TIMELINE[58]
5.	Creation of a documentation on integration, use and examples of the exchange of information with (the sharing mechanism and) the taxonomy.	Low	ENISA	Adapting the chosen sharing mechanism to the taxonomy	Medium	Medium term
6.	Organisation of an online workshop to present the taxonomy (and the sharing mechanism) to CSIRTs and LEAs.	Low	EC3 and ENISA	-	Medium	Medium term
7.	Linking the taxonomy with the legislation of the Member States based on the demand of the Member States.	Medium	ENISA and/or the Member States	-	Low	Long term
8.	Providing help to CSIRTs and LEAs for the integration of the taxonomy (and the sharing mechanism) into the CSIRTs and LEAs operations	Low	EC3 and ENISA	-	Low	Medium term

Table 4 - Roadmap actions

3.1.2 Description of the key roadmap actions

This section details the actions presented in the roadmap.

3.1.2.1 Action 1. Creation of a governance structure for the update of the taxonomy

To be able to adapt the taxonomy to a new phenomenon encountered by the communities and also to meet new requirements that they might have in the future, a simple but effective governance structure should be put in place by Europol and ENISA to organise regular meetings for the update of the taxonomy. Europol and ENISA are the most appropriate organisers of this governance structure due to the fact that they are EU agencies and that they represent both communities.

The first step for the creation of such a structure should be the identification of the stakeholder representatives. If possible, each CSIRT and LEA from all EU Member States should be represented in the governance structure that will update the taxonomy. Since Europol has access to the EUCTF mailing list and ENISA has a mailing-list of national and governmental CSIRTs in EU Member States, Europol should contact the LEAs of the Member States while ENISA should contact CSIRTs, to ask them to collaborate in such meetings.

The second step is to plan regular meetings of this governance structure to ensure a regular review of the taxonomy, with proper consideration of the balance between meeting of the requirements of the communities and ensuring the stability of the taxonomy. Based on the information collected so far, it seems that having meetings once or twice a year would be a good compromise. Once again, due to their roles and contacts lists, Europol and ENISA should be responsible for the organisation of such meetings (choosing the dates, making the agenda and sending invitations).

In parallel with the creation of the governance structure, the selected taxonomy should be promoted amongst both LEA and CSIRT communities, to raise awareness about the taxonomy and to incline both communities to use its classification for the exchange of information between CSIRTs and LEAs. Having them use the taxonomy before the choice of a sharing mechanism might provide feedback to be processed by the governance structure, allowing it to begin updating the taxonomy to the needs of the users. As a result, when a sharing mechanism and a sharing platform are chosen (which are the following actions), there may be an accelerated adoption of the taxonomy, the sharing mechanism and the sharing platform. The promotion of the taxonomy should be performed by ENISA and Europol, since they have the appropriate contact list for this action (the EUCTF for Europol and a global CSIRT mailing list for ENISA).

3.1.2.2 Action 2. Adapting the chosen sharing mechanism to the taxonomy

As explained previously, the taxonomy itself needs to be accompanied by a sharing mechanism to make the exchange of information efficient. The sharing mechanism that will be selected has to be adapted to the taxonomy. A simple example is to define which fields contains the types of events and which other contains the types of incidents.

Therefore, to integrate the taxonomy into a sharing mechanism, the fields that will contain the classification provided by the taxonomy should be determined and the mandatory information specified (in the case of high-level taxonomies like the CERT.PT taxonomy, the specification should define all fields as mandatory). This task should be executed by Europol, in cooperation with ENISA and the members of the OAP 4.1 working group since they are the main actors in the selection of this taxonomy and are knowledgeable on

the matter. CERT-EU[59] should provide technical support when needed since they already implemented the CERT.PT taxonomy in information exchange tools.

The kind of information to be exchanged depending on the receiver should be determined as well. In STIX, this is done by creating profiles, which allow users to define what kind of information they want to receive (in other words, what part of the data they are interested in). This step could enable the use of the sharing mechanism together with the taxonomy. Some profiles already exists for CSIRTs which could be reused as default profiles. The focus of this step should therefore be on the LEAs. Europol, as the EU agency, should define a LEA profile (in STIX, this is done by modifying the default profile[60]) with the cooperation of the members of the OAP 4.1 working group and the LEAs. CSIRTs and LEAs that have specific needs regarding a common profile and prefer using a specific profile created should also build a profile adapted to their needs.

3.1.2.3 Action 3. Choice of a sharing platform and an implementation model (distributed or global platform) for the exchange of messages across Member States

As explained in the section 'Proposition for a sharing mechanism for the selected taxonomy', three elements are used for the sharing of information between CSIRTs and LEAs: a taxonomy, a sharing mechanism and a sharing platform. Once the first two are selected, the third one should be chosen or created. The platform to exchange information might be simply e-mails, or specific tools could be used, such as MISP[61] or AbuseHelper[62], which allows the use of a level of classification (such as TLP[63], which was mentioned during the interviews).

Therefore, selecting a sharing platform that would fit the needs of both communities might allow the stakeholders to exchange information more easily. Europol and ENISA should execute this step in collaboration with the OAP 4.1 working group since they have knowledge about the taxonomy and also know the needs of the CSIRTs and the LEAs.

3.1.2.4 Action 4. Creation of a documentation set on integration, use and examples of the exchange of information with the sharing mechanism and the taxonomy

Since not all CSIRTs and LEAs are familiar with the use of such tools (a taxonomy, sharing mechanisms and platforms), the creation of documentation and examples on how to implement these to share information at a local and EU level could help them through the process. ENISA should create this documentation since they have an extensive experience in such documentation.

3.1.2.5 Action 5. Organisation of an online workshop to present the taxonomy and the sharing mechanism to CSIRTs and LEAs

To present the tools (the taxonomy, the sharing mechanism and the sharing platform) to both communities, demonstrate the use of the tools and gather comments and feedback from CSIRTs and LEAs, a workshop should be organised to show how the exchange of information could be structured and the objectives and advantages of such an approach.

---

[59] CERT-EU: https://cert.europa.eu
[60] STIX profile template: https://stix.mitre.org/language/profiles/stix_1.2_profile_template_r1.xlsx
[61] Malware Information Sharing Platform, http://www.misp-project.org/
[62] AbuseHelper, http://abusehelper.be/
[63] The Traffic Light Protocol (TLP) is a mechanism widely used in information sharing communities to indicate the allowed distribution of information. https://en.wikipedia.org/wiki/Traffic_Light_Protocol

To be able to provide that information to all CSIRTs and LEAs and ensure a high participation to the workshop, Europol and ENISA should organise such a workshop together and handle also invitations to CSIRTs and LEAs.

3.1.2.6 Action 6. Linking the taxonomy with the legislation of the Member States based on the demand of the Member States

Some Member States might need the taxonomy to be linked to their national legislation to help them adopt the taxonomy to overcome limitations of their mandates and other possible limits from the legislative framework (especially for the LEAs since their way of working is more procedural).

ENISA should provide help to Member States that would need assistance to create this mapping between the taxonomy and their national legislation since it is an EU agency and it can provide such an advice through their experience and knowledge about the taxonomy.

3.1.2.7 Action 7. Providing help to CSIRTs and LEAs for the integration of the taxonomy and the sharing mechanism

Since the implementation of the taxonomy, the sharing mechanism and potentially a sharing platform might be relatively complex for some CSIRTs or LEAs, ENISA and Europol should provide support (awareness raising and, resources or documentation) to the entities that would require it based on their knowledge about the taxonomy and the sharing mechanism.

Training requirements and the approach for training on the taxonomy will have to be further identified and detailed. These will in-turn drive the development of training schedules and materials that are critical to the actual delivery of support to the CSIRTs and LEAs for taxonomy implementation. This might help them put such a mechanism in place.

It is recommended that CERT-EU should also be involved in this task in order to provide additional support for the implementation, based on their experience with implementing the taxonomy.

4 Conclusion

During this study, key elements for the exchange of information between CSIRTs and LEAs have been identified, more specifically regarding:

- A taxonomy to use for the exchange of information
- A sharing mechanism to structure the exchange
- A model to adapt the taxonomy to new requirements

Based on this, a roadmap has been proposed for the implementation of a taxonomy in the exchange of information. This section describes the conclusions for each part of this study.

4.1 Common taxonomy for the exchange of information between CSIRTs and LEAs

Based on the desk research and the information gathered from interviews of CSIRTs and LEAs of EU Member States, requirements for a common taxonomy have been obtained. Based on these requirements and the possibilities of alignment with the OAP 4.1 working group, this study proposes **the CERT.PT taxonomy as a common taxonomy for the exchange of information between CSIRTs and LEAs**. This taxonomy answers the requirements provided and is easy to use and implement, while also offering opportunities for future updates, to evolve to a higher level of detail. It is also based on the Budapest Convention and the Cybercrime Directive, and provides a definition of the incidents and events it describes.

4.2 Sharing mechanism for the selected taxonomy

While a taxonomy allows to classify the information exchanged, it does not provide a format for the exchanged data. Using a common sharing mechanism could offer advantages such as automation of the analysis of the data and the creation of statistics.

Based on the research performed, STIX would be a good candidate for the format of the data. It has a high level of recognition by business and the stakeholders (CSIRTs and LEAs). STIX can be used together with any taxonomy and offer a model of which the parts can be implemented separately, allowing a step-by-step approach.

Although a sharing mechanism could offer advantages for the exchange of information, it also has drawbacks: it complexity might hinder its use, and some CSIRTs and LEAs might prefer to keep ad-hoc sharing mechanisms such as CSV files. Therefore, the use of a sharing mechanism should be studied further based on the needs of the CSIRTs and LEAs.

4.3 Model to adapt the taxonomy to new requirements

To enhance the use of a taxonomy, it should also be kept up-to-date and evolve according to the requirements of the CSIRTs and LEAs. Therefore, an update model should be in place to ensure the evolution of the taxonomy. Based on the information collected from the interviews and the possibilities of alignment with the OAP 4.1 working group, **a dynamic update of the taxonomy through regular meeting of the stakeholders seems to be best suited.**

4.4 Roadmap for the implementation of the taxonomy

This study proposes a roadmap that defines the main elements of the implementation of the common taxonomy through the CSIRT and LEA communities.

The CERT.PT taxonomy is an important step towards improving the cooperation between CSIRTs and LEAs. It should allow both communities to share information more easily and improve the efficiency of the communication. Furthermore, based on the evolution of the taxonomy, it should allow CSIRTs and LEAs to adapt the classification to their convenience, making it grow based on their needs.

Towards this end, the most important short term activities include setting up a governance structure to continuously update the taxonomy to new phenomena, disseminating the taxonomy to the CSIRT and LEA communities, identifying the participants for the CSIRTs and LEAs in each Member State of the EU and organising the governance meetings.

ENISA

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

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP0215981ENN

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

ISBN: 978-92-9204-163-2
DOI: 10.2824/189989