Common Taxonomy for Law Enforcement and The National Network of CSIRTs

Executive Summary

The objective of this document is to support the Computer Security Incident Response Teams (CSIRTs) and the Public Prosecutors in their dealing with Law Enforcement Agencies in cases of criminal investigations, by providing a common taxonomy for the classification of incidents, named **Common Taxonomy for Law Enforcement and The National Network of CSIRTs**.

The Common Taxonomy for Law Enforcement and The National Network of CSIRTs bridges the gap between the CSIRTs and international Law Enforcement communities by adding a legislative framework to facilitate the harmonisation of incident reporting to competent authorities, the development of useful statistics and sharing information within the entire cybercrime ecosystem.

To guarantee that this taxonomy remains relevant for the CSIRT as well as the Law Enforcement community alike, amendments and regular updates to its text and indicators are to be expected on a continuous basis.

The Taxonomy Governance Group was established as a working group engaged in maintaining and updating this taxonomy to maximise collaboration between Law Enforcement and CSIRTs, stepping up coordination of efforts, exchange of information and building prevention and detection capabilities.

In this new version (v1.3 – December 2017) of the taxonomy several changes have been performed, such as a definition of the scope of the taxonomy, a new simplified taxonomy structure, inclusion of new international legislation linked to each incident and semantic and structure changes in the Class of Incidents, Type of Incidents and Descriptions of the taxonomy.

Table of Contents

1 Introduction

The objective of this document is to support the Computer Security Incident Response Teams (CSIRTs) and the Public Prosecutors in their dealing with Law Enforcement Agencies in cases of criminal investigations, by providing a common taxonomy for the classification of incidents, named **Common Taxonomy for Law Enforcement and The National Network of CSIRTs**.

This Common Taxonomy for Law Enforcement and The National Network of CSIRTs which will be referred to as the "Common Taxonomy" or the "Taxonomy", it is based on the CERT.PT taxonomy, considered by the European Multidisciplinary Platform Against Criminal Threats (EMPACT) Operational Action Plan 4.1 as an appropriate candidate for the exchange of information and currently in use within The National Network of CSIRTs. The report "*Information sharing and common taxonomies between CSIRTs and Law Enforcement*" (ENISA, 2015) also observed that the CERT.PT Taxonomy was the best fitting for the exchange of information between the CSIRTs and LEAs.

This decision was based on the suitable implementation of several of the taxonomies' good practices identified in the CSIRT community, such as the simple top level categorisation, the mutually exclusive categories, an appropriate level of ease of use, and ease of understanding by external non-CSIRT entities, among others.

The Common Taxonomy bridges the gap between the CSIRTs and international Law Enforcement communities by adding an international legislative framework to facilitate the harmonisation of incident reporting to competent authorities, the development of useful statistics and sharing information within the entire cybercriminal ecosystem.

In this new version several changes have been made, such as:

- Clear definition of the scope of the taxonomy, focused on the cybercrime ecosystem.
- New simplified Taxonomy structure: reduced to a single table where all the Classes and Types of Incidents are shown.
- New international legislation included, linked with each Type of Incident.

- Semantic and structure changes regarding the Class of Incidents, Type of Incidents and their Descriptions, improving the previous version of the Taxonomy.

2 Taxonomy Structure

The Taxonomy will be presented in one table, as below:

1. Describing the variety of incidents that fall under the taxonomy;
2. Grouping those incidents according to their class and type;
3. Mapping each type of incident with the pertinent article of the international legislative framework.

This way, any incident categorised in this Taxonomy can be matched to the relevant and appropriate legislative framework and subsequently mapped to relevant national legislation.

3 Taxonomy Scope

For the purpose of this Taxonomy it is important to have a clear concept of the different scopes of an event, an incident and a crime.

An **event** can be defined as any observable occurrence that happened at a point in time in a system or network, especially one of importance. Thus, **an event does not necessarily imply an adverse situation or a malicious activity**.

For instance, *"to send an email"* or "*to make a phone call*" are events with no malicious implication.

On the other hand, a **security incident necessarily implies a human-cause adverse event**, usually with a malicious nature, which is oriented to cause a disruption of any system or network.

It is important to underline that incidents arising from **negligence**, as well as **attempts** that fail, also fall under the concept of a security incident. Examples of security incidents are "*SQL injection*" or "*Cross-Site Scripting*" attacks.

As can be observed below in Figure 1, **any security incident is considered an event but not any event is considered a security incident**.

Also not every security incident has a crime penalty, therefore only the security incidents able to be criminally prosecuted will be the ones falling under the scope of this Taxonomy. To clarify this, see the Figure 1 below.

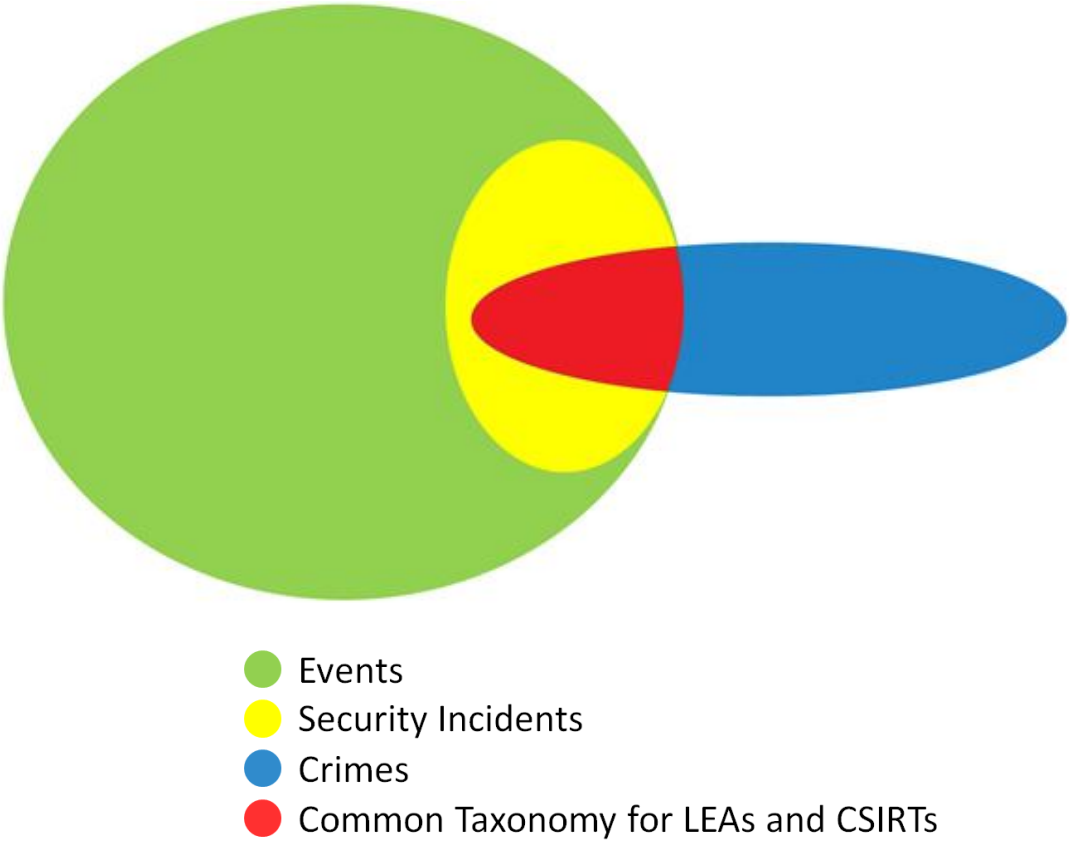

Figure 1: Events, Security incidents, Crimes and Common Taxonomy ecosystem.

This Taxonomy is limited to those incidents related with **human-cause cyber offences** and **attempted offences.**

Natural disasters or any other adverse event not directly related with information security and human activities are outside of the scope.

4 Taxonomy Legislative Framework

To make sure that this Taxonomy fits the needs of all EU Member States and Third parties alike, the reference legislative framework is international. For that purpose, this Taxonomy is linked with the main international and European legislations:

A. Council of Europe Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention (ETS 185)[1]
B. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201)[2]
C. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS 189)[3]
D. Berne Convention for the Protection of Literary and Artistic Works[4]
E. Universal Convention on Copyright[5]
F. Directive 2013/40/EU of the European Parliament and of the Council of 12th August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Directive 2013/40/EU) – NIS Directive [6]
G. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) – GDPR [7]
H. Directive 2000/31/EC of the European Parliament and of the Council of 8th June 2000 on certain legal aspects of information society services, in particular

[1] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[2] https://rm.coe.int/168046e1e1
[3] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081601
[4] http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=283693
[5] http://portal.unesco.org/en/ev.php-URL_ID=15381&URL_DO=DO_TOPIC&URL_SECTION=201.html
[6] http://data.europa.eu/eli/dir/2013/40/oj
[7] ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf : The Taxonomy refers to the principles of the GDPR, as named in art. 5, art. 25 and the proposal for an ePrivacy regulation: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

electronic commerce, in the Internal Market (Directive 2000/31/EC) – eCommerce Directive [8]

I. Directive 2001/29/EC of the European Parliament and of the Council of 22nd May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Directive 2001/29/EC) – InfoSoc Directive [9]
J. Directive 2001/84/CE of the Parliament and the Council of the 27th September on the resale right for the benefit of the author of an original work of art[10]
K. Directive n 2004/48/CE, of the Parliament and the Council of the 29th April on the enforcement of intellectual property rights (Directive n 2004/48/CE)[11]

5 Taxonomy Maintenance

The participants in the initial development of the Common Taxonomy for Law Enforcement and The National Network of CSIRTs were:

Figure 2: Participants in the development of the Common Taxonomy for LEAs and CSIRTs.

[8] http://data.europa.eu/eli/dir/2000/31/oj
[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML
[10] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0084&from=EN
[11] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0048R(01)&from=EN

To guarantee that this Taxonomy remains relevant for the CSIRT as well as the Law Enforcement community alike, amendments and regular updates to its text and indicators are to be expected on a continuous basis.

The **Taxonomy Governance Group (TGG)** was established as a working group to maintain and update this Taxonomy, acting as liaison and promoting common standards and procedures in the exchange of intelligence. It aims to develop new avenues for the practical use of the Common Taxonomy to stimulate cooperation between the Law Enforcement and CSIRT communities.

The Taxonomy Governance Group member organisations are represented by the subject matter expert of the organisation or in exceptional circumstances by a senior officer.

The current members of the TGG are:

- European Cybercrime Centre (EC3)/EUROPOL
- European Cyber Task Force (EUCTF)
- ENISA
- CERT-EU
- Selected CSIRTs

Additional members will be subject to approval of the Group.

The Taxonomy Governance Group will meet **every year** for a Regular Group meeting.

6 Taxonomy Classification:

Class of Incidents	Description of Class of Incidents	Type of Incidents	Description of Type of Incidents	Legislative Framework
Malware	Infection of one or various systems with a specific type of malware.	**Infection**	Malware detected in a system.	System(s) or software(s) infected with malware allowing remote access, monitoring of system activities and gathering of information: - Art. 2 and 6 [A] - Art. 3 and 6 [F]
		Distribution	Malware attached to a message or email message containing link to malicious URL or IP.	Dissemination of malware through various communication channels: - Art. 7 [F] - Art. 6 [A]
		Command & Control (C&C)	System used as a command-and-control point by a botnet. Also included in this field are systems serving as a point for gathering information stolen by botnets.	C&C server hosting: - Art. 2 and 6 [A] - Art. 4 and 7 [F]
	Connection performed by/from/to (a) suspicious system(s)	**Malicious connection**	System attempting to gain access to a port normally linked to a specific type of malware.	Connection to (a) suspicious system(s) or port(s) linked to specific malware: - N/A

Class of Incidents	Description of Class of Incidents	Type of Incidents	Description of Type of Incidents	Legislative Framework
			System attempting to gain access to an IP address or URL normally linked to a specific type of malware, e.g. C&C or a distribution page for components linked to a specific botnet.	Connection to (a) suspicious system(s) linked to specific malware: - N/A
Availability	Disruption of the processing and response capacity of systems and networks in order to render them inoperative.	**Denial of Service (DoS)/ Distributed Denial of Service (DDoS)**	Single source using specially designed software to affect the normal functioning of a specific service, by exploiting vulnerability.	Exploit or tool (individual or distributed) aimed at exhausting resources (network, processing capacity, sessions, etc.): - Art. 5 and 6 [A] - Art. 7 [F]
			Mass mailing of requests (network packets, emails, etc.) from one single source to a specific service, aimed at affecting its normal functioning.	Flood of requests (individual or distributed): - Art. 5 and 6 [A] - Art. 4 [E]
	Premeditated action to damage a system, interrupt a process, change or delete information, etc.	**Sabotage**	Logical and physical activities which – although they are not aimed at causing damage to information or at preventing its transmission among systems – have this effect.	Vandalism: - Art. 4 and 5 [F] - Art. 5 and 6 [A]
Information Gathering	Active and passive gathering of information on systems or networks.	**Scanning**	Single system scan searching for open ports or services using these ports for responding.	System probe: - N/A
			Scanning a network aimed at identifying systems which are active in the same network.	Network scanning: - N/A

Class of Incidents	Description of Class of Incidents	Type of Incidents	Description of Type of Incidents	Legislative Framework
			Transfer of a specific DNS zone.	DNS zone transfer: - N/A
	Unauthorised monitoring and reading of network traffic.	**Sniffing**	Logical or physical interception of communications.	Wiretapping: - Art. 3 and 6 [A] - Art. 6 and 7 [F]
	Attempt to gather information on a user or a system through phishing methods.	**Phishing**	Mass emailing aimed at collecting data for phishing purposes with regard to the victims.	Dissemination of phishing emails: - Art. 7 [H] - Art. 7 [G]
			Hosting web sites for phishing purposes.	Hosting of phishing sites: - Art. 7 [F]
Intrusion Attempt	Attempt to intrude by exploiting vulnerability in a system, component or network.	**Exploitation of vulnerability attempt**	Unsuccessful use of a tool exploiting a specific vulnerability of the system.	Exploit attempt: - Art. 2, 6 and 11 [A] - Art. 3, 7 and 8 [F]
			Unsuccessful attempt to manipulate or read the information of a database by using the SQL injection technique.	SQL injection attempt: - Art. 2, 6 and 11 [A] - Art. 3, 7 and 8 [F]
			Unsuccessful attempts to perform attacks by using cross-site scripting techniques.	XSS attempt: - Art. 2, 6 and 11 [A] - Art. 3, 7 and 8 n 1 [F]
			Unsuccessful attempt to include files in the system under attack by using file inclusion techniques.	File inclusion attempt: - Art. 5 and 11 [A]

Class of Incidents	Description of Class of Incidents	Type of Incidents	Description of Type of Incidents	Legislative Framework
				- Art. 3, 7 and 8 [F]
			Unauthorised access to a system or component by bypassing an access control system in place.	Control system bypass: - Art. 2 [A] - Art. 3 and 7 [F]
	Attempt to log in to services or authentication / access control mechanisms.	**Login attempt**	Unsuccessful login by using sequential credentials for gaining access to the system.	Brute-force attempt: - Art. 2, 6 and 11 [A] - Art. 3,7 and 8 [F]
			Unsuccessful acquisition of access credentials by breaking the protective cryptographic keys.	Password cracking attempt: - Art. 2, 6 and 11 [A] - Art. 3,7 and 8 [F]
			Unsuccessful login by using system access credentials previously loaded into a dictionary.	Dictionary attack attempt: - Art. 2, 6 and 11 [A] - Art. 3,7 and 8 [F]
Intrusion	Actual intrusion by exploiting vulnerability in the system, component or network.	**(Successful) Exploitation of vulnerability**	Unauthorised use of a tool exploiting a specific vulnerability of the system.	Use of a local or remote exploit: - Art. 2 and 6 [A] - Art. 3 and 7 [F]
			Unauthorised manipulation or reading of information contained in a database by using the SQL injection technique.	SQL injection: - Art. 5 and 6 [A] - Art. 3 and 7 [F]
			Attack performed with the use of cross-site scripting techniques.	XSS: - Art. 5 and 6 [A]

Class of Incidents	Description of Class of Incidents	Type of Incidents	Description of Type of Incidents	Legislative Framework
				- Art. 3 and 7 [F]
			Unauthorised inclusion of files into a system under attack with the use of file inclusion techniques.	File inclusion: - Art. 5 and 6 [A] - Art. 3 and 7 [F]
			Unauthorised access to a system or component by bypassing an access control system in place.	Control system bypass: - Art. 2 [A] - Art. 3 and 7 [F]
	Actual intrusion in a system, component or network by compromising a user or administrator account.	**Compromising an account**	Unauthorised access to a system or component by using stolen access credentials.	Theft of access credentials: - Art. 6 [A] - Art. 3 and 7 [F]
Information Security	Unauthorised access to a particular set of information	**Unauthorised access**	Unauthorised access to a system or component.	Unauthorised access to a system: - Art. 2 [A] - Art. 3 and 7 [F]
			Unauthorised access to a set of information.	Unauthorised access to information: - Art. 2 [A] - Art. 3 and 7 [F] - Art. 5, 6 and 25 [G]
			Unauthorised access to and sharing of a specific set of information.	Data exfiltration: - Art. 2 [A]

Class of Incidents	Description of Class of Incidents	Type of Incidents	Description of Type of Incidents	Legislative Framework
	Unauthorised change or elimination of a particular set of information.	**Unauthorised modification/deletion**	Unauthorised changes to a specific set of information.	Modification of information: - Art. 4, 7 and 8 [A] - Art. 5 [F]
			Unauthorised deleting of a specific set of information.	Deleting of information: - Art. 4 [A] - Art. 5 [F]
Fraud	Loss of property caused with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Misuse or unauthorised use of resources**	Use of institutional resources for purposes other than those intended.	Misuse or unauthorised use of resources: - N/A
		False representation	Unauthorised use of the name of an institution.	Illegitimate use of the name of an institution or third party: - N/A
Abusive Content	Sending SPAM messages.	**SPAM**	Sending an unusually large quantity of email messages.	Email flooding: - Art. 7 [H]
			Unsolicited or unwanted email message sent to the recipient.	Sending an unsolicited message: - Art. 7 [H]

Class of Incidents	Description of Class of Incidents	Type of Incidents	Description of Type of Incidents	Legislative Framework
	Distribution and sharing of copyright protected content	**Copyright**	Unauthorised distribution or sharing of content protected by Copyright and related rights.	Distribution and sharing of copyright protected content: - Art. 10 [A] - [D] - [E] - [I] - [J] - [K]
	Dissemination of content forbidden by law.	**Child Sexual Exploitation, racism or incitement to violence**	Distribution or sharing of illegal content such as child sexual exploitation material, racism, xenophobia, etc.	Dissemination of content forbidden by law (Publicly prosecuted offences): - Art. 9 [A] - Art. 18 to 23 [B] - Art. 3 to 6 [C]
Other	Incidents not classified in the existing classification	**Unclassified incident**	Incidents which do not fit the existing classification, acting as an indicator for the classification's update.	Unclassified incident. - N/A
		Undetermined incident	Unprocessed incidents which have remained undetermined from the beginning.	Undetermined incident. - N/A