

RESISTO: D2.2_Cyber-physical threat/risk scenarios and pre-assessment - first

RESISTO

D2.2 – CYBER-PHYSICAL THREAT/RISK SCENARIOS AND PRE-ASSESSMENT - FIRST

Document Manager:	Mirjam FEHLING-KASCHEK	Fraunhofer	Editor
--------------------------	------------------------	------------	--------

Project Title:	RESilience enhancement and risk control platform for communication infraSTructure Operators
Project Acronym:	RESISTO
Contract Number:	786409
Project Coordinator:	LEONARDO
WP Leader:	BTC

Document ID N°:	RESISTO_D2.2_190117_01	Version:	1.0
Deliverable:	D2.2	Date:	16/05/2019
		Status:	APPROVED

Document classification	Public
--------------------------------	---------------

Approval Status	
Prepared by:	Mirjam FEHLING-KASCHEK, Katja FAIST (Fraunhofer)
Approved by: (WP Leader)	Zhan CUI (BTC)
Approved by: (Coordinator)	Federico FROSALI (LDO)
Advisory Board Validation (Advisory Board Coordinator)	Carmen PATRASCU (ORO)
Security Approval (Security Advisory Board Leader)	Alberto BIANCHI (LDO)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Mirjam Fehling-Kaschek, Jörg Finger, Katja Faist	Fraunhofer	Scientific Researcher
Ioan Constantin	ORO	Cyber Security Expert
Rodoula Makri, Nikolaos Uzunoglu, Panos Karaivazoglou, Apostolos Papafragkakis	ICCS	Telecommunication experts, Senior Researchers
Andrei Avadanei Lucian Nitescu Florina Dumitrache	BSS	Cyber Security Specialists, Communication Specialist
Xiao-Si Selina Wang Zhan Cui	BTC	Senior Researcher Chief Researcher
Sylvia Bach	BUW	Scientific Researcher
Maria Belesioti Ioannis Chochliouros	OTE	Telecommunication experts, Senior Researchers

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
PMT	RESISTO CONSORTIUM	NA
Markus MULLER	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.1	29.10.2018	All	All	First complete draft
0.2	06.11.2018	All	All	Comments from WP2 review
0.3	14.11.2018	All	All	Release for AB review
0.9	17.01.2019	All	All	Release for SAB review
1.0	16.05.2019	All	All	Final release

COPYRIGHT STATEMENT



© 2018-2021 This document and its content are the property of the RESISTO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the RESISTO Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the RESISTO Partners. Each RESISTO Partner may use this document in conformity with the RESISTO Consortium Grant Agreement provisions.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Program, under the Grant Agreement No 786409.

The views and opinions in this document are solely those of the authors and contributors, not those of the European Commission.

PROJECT CONTACT



LEONARDO
Via delle Officine Galileo 1 – Campi Bisenzio (FI) –
50013 – Italy
Tel.: +39 055 5369640, Fax: +39 055 5369640
E-Mail: frederico.frosali@leonardocompany.com

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the CIs. Thus they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and gains. Also extreme weather events and natural disasters represents a challenge due to their increase in frequency and intensity requiring smarter resilience of the Communication CIs, which are extremely vulnerable due to the ever-increasing complexity of the architecture also in light of the evolution towards 5G, the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. RESISTO platform is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters. Through RESISTO Communications Operators, will be able to implement a set of mitigation actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences, and cascading effects in particular by bouncing efficiently back to original and forward to operational states of operation.

EXECUTIVE SUMMARY

This deliverable reports the current status of Task 2.2 “Cyber physical threat, hazard and disruption ranking ontology”. The work is ongoing and the final results will be presented in the concluding report at the end of the runtime of Task 2.2.

Main objective is the deployment of a living threats, hazards and disruptions list for the communication infrastructures. The setup of the list should follow a resilience driven approach and cover the event properties of main interest for the telecom operators. Furthermore, it should contain cyber, physical and combined cyber-physical threats. Final goal will be to define an event ranking ontology.

As a first step, existing and publically available threat databases, e.g. ENISA, have been studied and evaluated. A summary of them is given in this report.

To capture the properties of interest specifically for this project, a tabular template for the threats list was developed. It contains not only a table listing the threats and disruptions, but also tables listing system components, system functions and possible mitigation actions. This setup was chosen to follow the risk and resilience management approach.

The structure of the tabular template is described in detail in this report. Input to the lists is currently collected from telecom operators. The input is needed for further evaluation and to perform the risk ranking. Those results will be subject of the final report of Task 2.2.

CONTENTS

ABBREVIATIONS	10
1. INTRODUCTION	11
2. BACKGROUND AND RELATED WORK.....	12
2.1. Introduction to risk and resilience management.....	12
2.2. Current telecommunication infrastructures, assets and networks – security concerns..	14
2.3. Overview on threat classification and example classifications.....	16
2.3.1. Overview of threat standards and models.....	17
2.3.2 Definition of security threats in telecom infrastructures.....	25
2.3.3 The European Union Agency for Network and Information Security – ENISA.....	36
2.3.4 Malware classifications and examples	38
2.3.5 Cyber-Physical System Security classifications and examples	40
2.3.6. Other classification schemes.....	41
2.4. Existing threat databases.....	51
3. DEFINITION OF PROFILE TEMPLATE FOR POTENTIAL DISRUPTIONS.....	54
3.1. Aim of the threats and hazards template	54
3.2. General setup of the template: Tabular Excel document.....	54
3.3. Identification of information needed for the risk and resilience assessment.....	55
3.4. Context of the tabular template with respect to the resilience management approach ...	56
4. FIRST IMPLEMENTATION AND TESTING OF THE TEMPLATE.....	57
4.1. Implementation details	57
4.2. First testing and results	58
5. SUMMARY AND CONCLUSIONS	61
5.1. Next steps	61

Figure 1: Risk and resilience management processes [1]. The risk management process (right) follows the definition of ISO 31000 (2009) Risk management – Principles and guidelines ¹ . The definition of the resilience management process (left) is taken from [1].	12
Figure 2: Generic resilience management process that consists of nine steps and covers resilience quantification and development [1].	13
Figure 3: Typical Layouts of a local access network (left) and a mobile network (right).	15
Figure 4: Typical arrangement and routing to the core network – accessing the internet.	15
Figure 5: CVSS v3.0 Metric Groups	19
Figure 6: CVSS v2.0 Metrics	20
Figure 7: Website defacement statistics ⁴	23
Figure 8: Website defacement statistics, Single IPs only ⁴	23
Figure 9: Screenshot of the AbuseIPDB website	24
Figure 10: Statistic by number of unique attackers (Screenshot of the AbuseIPDB website ⁵)	24
Figure 11: Statistic by number of unique reporters (Screenshot of the AbuseIPDB website ⁵)	25
Figure 12: Submissions to VirusTotal [18] in October 2018.	25
Figure 13: Chart of percentage of significant incidents per root cause category, development 2011-17.	37
Figure 14: Chart of percentage of affected services, development 2011 - 2017	37
Figure 15: Chart of duration of incidents per root cause category in hours, development 2011 - 2017	38
Figure 16: Malware infections by type in Q1 2013, Panda Security	40
Figure 17: Screenshot of the tabular template for the hazard list	56
Figure 18: Screenshot of the Hazard specific part of the Definitions sheet of the threats and hazards template	57

ABBREVIATIONS

2G, 3G, 4G	Second, third and fourth generation of mobile phone systems
APT	Advanced Persistent Threat
DSL	Digital Subscriber Line
DoS	Denial of Service
ENISA	European Network and Information Security Agency
EU	European Union
GSM	Global System for Mobile communications
ID	Identifier
IP	Internet Protocol
ISP	Internet Service Provider
LTE	Long Term Evolution (= 4G)
MAC	Media Access Control
MSC	Mobile Switching Center
OSI	Open Systems Interconnection
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
TCP	Transmission Control Protocol
UE	User Equipment
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WP	Work Package

1. INTRODUCTION

The aim of WP2 is the refinement and specification of user expectations and requirements for the RESISTO platform. It was designed to collect the necessary inputs for the implementation of the tools and methods throughout the other work packages. The following tasks are included in WP2:

Task 2.1 Communication operators requirements refinement

Task 2.2 Cyber physical threat, hazard and disruption ranking ontology

Task 2.3 Holistic socio-technical communication infrastructure system modelling

Task 2.4 RESISTO reference architecture for long term preparation and short term disruptions

Task 2.5 Operational use cases and validation plan

This report summarizes the status and results of Task 2.2. Aim of the task is to define a template for threats and hazards for the communication infrastructures. By collecting input from all telecommunication operation partners, a top-level resilience driven threats and hazards list is generated. A focus is set on covering not only physical or cyber threats standalone but also combined cyber-physical threats.

The report is structured as follows. A brief introduction and overview on the topics covered in this report is given in Section 2: introduction to risk and resilience management (2.1), a short introduction to communication infrastructures (2.2), an overview on threat classification (2.3) and existing threat databases (2.4). The threats and hazards template is specified and defined in Section 3. The implementation and first tests/results are described in Section 4. Finally, a summary is given in Section 5, summarizing the results of this report and giving an overview on the next steps that will be followed towards the final report (5.1).

2. BACKGROUND AND RELATED WORK

2.1. Introduction to risk and resilience management

In this project, a sophisticated risk and resilience management approach is applied. The ISO 31000 standard for risk management is therefore extended to define the long term analytical assessment and improvement process for the RESISTO platform.

A detailed introduction and description for a joint risk and resilience management process is given in [1]. A key output of this paper is the definition of an iterative resilience management cycle. It consists of nine sequential steps, as shown in Figure 1 on the left side. For comparison, also the five steps following the ISO 31000 (2009)¹ risk management process are presented in Figure 1 on the right side and assigned to the corresponding steps of the extended resilience management process.

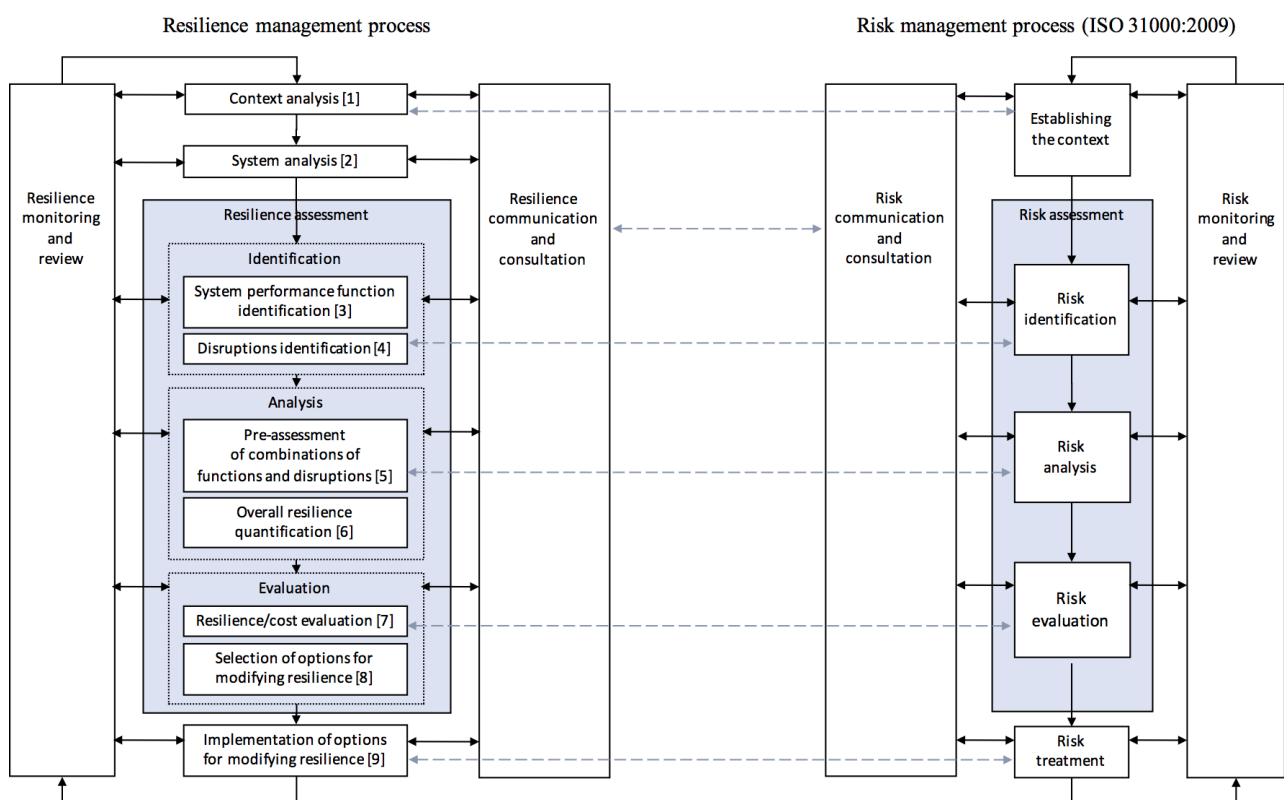


Figure 1: Risk and resilience management processes [1]. The risk management process (right) follows the definition of ISO 31000 (2009) Risk management – Principles and guidelines¹. The definition of the resilience management process (left) is taken from [1].

¹ ISO 31000 was updated in 2018, thus ISO 31000:2009 is replaced by ISO 31000:2018. The work presented in this section was originally developed based on the 2009 version. The extension of the risk management steps to the risk and resilience management steps is still valid. An update of the scheme shown in Fig.1 is planned for the final version of the report D2.3.

The risk management process (right) follows the definition of ISO 31000 (2009) Risk management – Principles and guidelines. The definition of the resilience management process (left) is taken from

The full resilience management process is further defined and implemented within the Long Term Control Loop in WP3 (see deliverables D3.1 and D3.2). Most of the direct input needed to assess the resilience of a system in the different steps of the resilience management process is gathered in WP2. A second scheme showing the nine steps iterative resilience management process is shown in Figure 2.

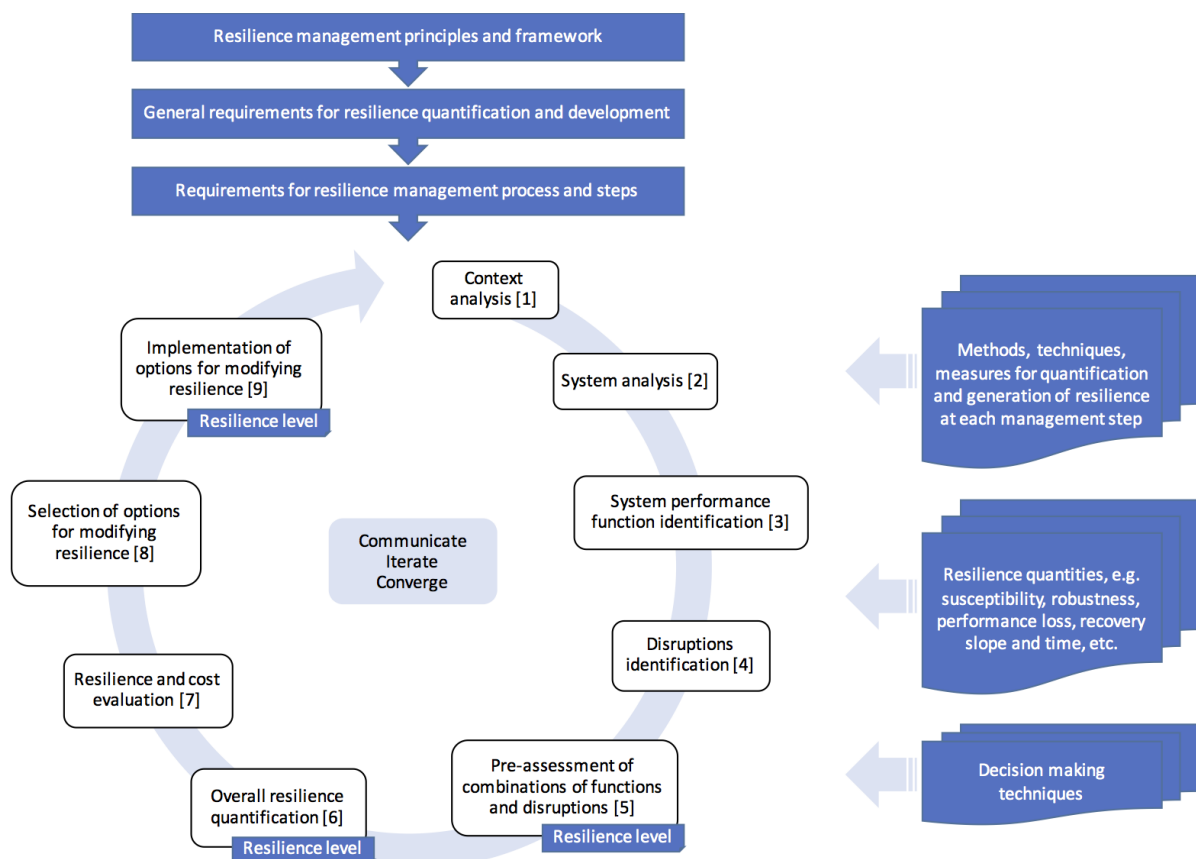


Figure 2: Generic resilience management process that consists of nine steps and covers resilience quantification and development [1]

The threats and hazards list that is prepared by Task 2.2 is the main input for Step 4 (Disruptions identification), which consists of seven ordered sub-steps [1]:

1. Threats / Hazards / Disruptions identification (possible root causes), classical risk events
2. Identification of service function disruptions
3. Elicitation of means to cover (as far as possible) unexampled (unknown unknown, black swan) events, e.g. in terms of their effects on system (service) functions
4. Identification of loss of (technical) resilience capabilities

5. Consideration of potentially affected system layers, e.g. physical, technical, cyber, organizational, etc.
6. Summary / Inventory of disruptions space relevant for resilience
7. Assessment of uncertainty of disruptions identification

For this approach, the threats and hazards list is needed as initial input (sub-step 1). The following sub-steps (especially sub-steps 2, 3 and 5) are strongly related to the other phases of the main resilience management process, in particular the identification of system performance functions (Step 3) and system components (Step 2). In addition, possible mitigation strategies evaluated in the resilience process (Step 8) are directly linked to the threats. In total, complementing information about the system components, system functions and mitigation options is needed in addition to the pure threat list in order to follow the resilience management process. A proposal for a combined inquiry of all information was therefore developed and is presented in Section 3.

2.2. Current telecommunication infrastructures, assets and networks – security concerns

Telecommunications networks are essential for the day-to-day running of all nations businesses and public services, but concerns have been raised in recent years over their security. Private businesses, government agencies and other bodies are dependent on telephone and internet services provided by telecommunications (telecoms) networks to carry out daily operations. Telecoms networks also provide services integral to the health and social life of the population. In this respect, telecoms have been recognized as one of the main critical national infrastructure sectors – since they are pivotal infrastructures to the functioning of a state or country.

Telecommunications networks face a range of physical and cyber threats that may be malicious, non-deliberate or naturally occurring. The Communications Act 2003 requires telecom companies to maintain the security and resilience of their networks [2]. While there is no mandated security and resilience standard for telecommunications, current resilience mainly includes investing in duplicates of infrastructure (i.e. disaster centers, double networks) and installing back-up power supplies.

Telecom networks and telecom providers

Telecom networks rely on infrastructure to connect users to others within a state and internationally. Networks comprise two main parts: a 'core' and an 'access' network. A core (or 'backbone') network connects telecom networks and carries large volumes of communication data across the country. There may be several different but interconnected core networks owned by various telecommunication providers (including mobile operators) while core network infrastructure can also be provided by third parties. Access networks connect customers to the core network in a local area, either via cables or wirelessly using radio signals. Figures 3 and 4 show typical layouts of different networks.

Fixed-Line Networks: Fixed-line networks provide telephone, TV and broadband internet services. Fixed-line core networks are made up of telephone exchanges that contain a system of switches to route communications, usually connected by fibre optic cables. Access

networks typically use a mixture of fibre optic and copper cables to connect customers' premises to the core network, while often there are regulatory obligations to share their access network infrastructure with other companies.

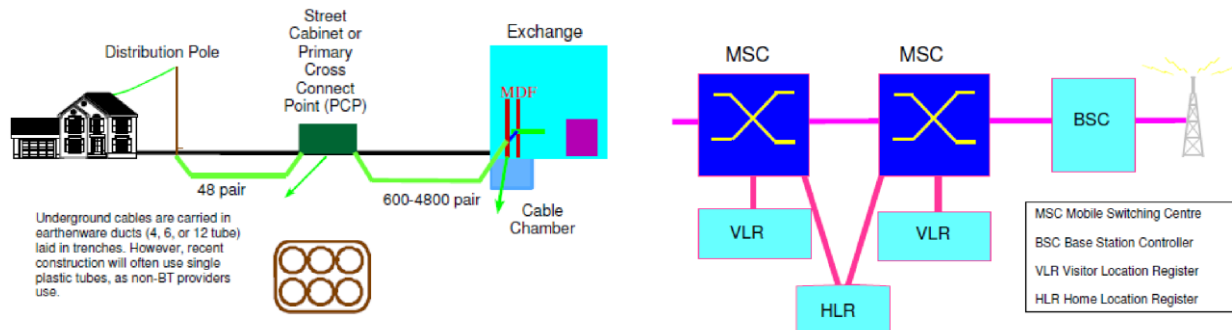


Figure 3: Typical Layouts of a local access network (left) and a mobile network (right).

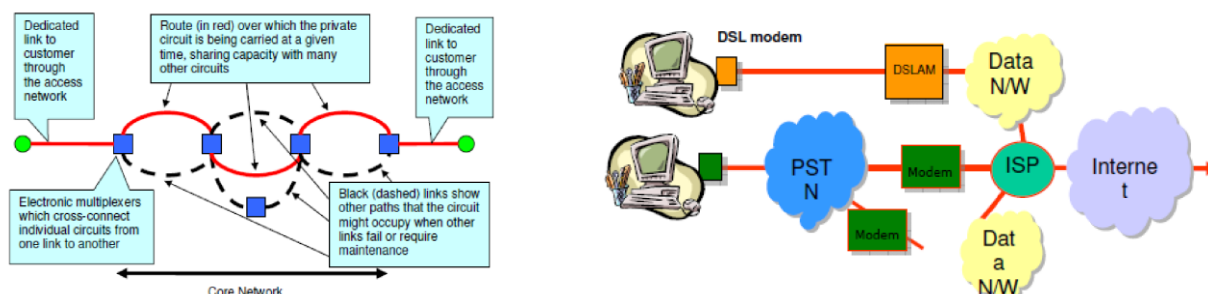


Figure 4: Typical arrangement and routing to the core network – accessing the internet.

Mobile Networks: Like fixed-line networks, mobile networks have a core network consisting of exchanges (e.g. 'mobile switching centres'), normally connected by fibre optic cables. Mobile access networks differ from fixed-line ones, as they comprise base stations (connected to the exchanges) that communicate with handsets using radio signals. Mobile operators use fixed-line (and in some instances radio) infrastructure to connect base stations and exchanges together. Base stations provide access to the network over a limited area, so many are required to achieve nation-wide coverage. Mobile network providers must obtain licenses from national telecoms regulator authorities to use certain parts of the radio frequency spectrum. Various mobile network operators may operate in a country which in certain cases own additional fixed-line networks or hire them from the fixed-line operators, as described above. In many cases, the emergency services currently communicate using dedicated networks, where plans are made to migrate them to commercial networks.

International interconnections - Undersea Cables and Satellites: The core networks of different countries are connected using fibre optic cables that run along or are buried in the sea bed. For example, there are around 40 active undersea cables connecting the UK to the rest of the world. Undersea cables come ashore at landing sites that connect the cables to the core network. Furthermore, satellites can send and receive radio signals over large

distances to antennae on the ground, and provide connectivity to remote communities where there is no fixed-line infrastructure. The part of the radio frequency spectrum they use and the paths of their orbits are registered by the International Telecommunication Union (ITU). Telecoms networks also rely on information from global positioning system (GPS) satellites to synchronize with each other. Despite the relatively small part of the radio frequency spectrum assigned, satellites do make the most efficient usage of it connecting billions of end-users; showing in many cases capacity equivalent to fiber connecting oil rigs, ships and airplanes with high power data all over the world or often providing back up capacity to fiber networks.

Concerns have recently been raised (2017) about the security of both the undersea cables and the satellites that carry a large amount of global communications² (i.e. their ground segment and or concerns related to cyber threats), which is also another aspect to be taken into account for security and resilience mechanisms.

2.3. Overview on threat classification and example classifications

Threats classifications help to identify and understand threat characteristics and sources. These help to detect, understand and evaluate threats, and thus help to propose appropriate security solutions, to protect systems assets and services, and to be resilient under attacks and disasters. Moreover, it articulates the security risks that threaten these systems and assists in understanding the capabilities and selection of security solutions. In fact, security threats can be observed and classified in different ways by considering different aspects of the system like its source code, or its users, or their impacts. A comprehensive view of existing threat classifications helps to examine the coverage of the RESISTO platform and validate its solutions by studying how these threats/hazards are addressed. By examining potential vulnerabilities/weaknesses of components and systems, RESISTO solutions can identify measures to minimize attacks and to stop exploits.

This section overviews publically available threats/hazards classifications for RESISTO project. It covers a wide range of threats/hazards affecting Communication Infrastructures (CIs) including physical structures, services as well as devices used by or connected to communication networks, and information systems. Apart from a list of existing threat classifications, this section also covers key terminologies used when people talk about, analyze and deal with security threats. As security could be dealt with on many levels, by different frameworks and in different contexts, many terminologies overlap. It's important to understand in what context they are used.

In the following, a brief overview of the current knowledge concerning the various kinds of threats and resilience actions in existing telecom infrastructures is given, starting from the current telecommunication networks and resulting in existing threats classification as this can be found in related literature or reports from national or international Agencies. The whole analysis will help identify relevant gaps and needs that will act as the baseline in order the added value that will be brought by the RESISTO project to be substantiated.

² <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>

Section 2.3.1 overviews commonly used threats standards and models. Then, Section 2.3.2 covers security threats in telecom infrastructures including physical, cyber, and cyber-physical threats and hazards. Afterwards, Section 2.3.3 discusses ENISA threat taxonomy. Section 2.3.4 introduces malware classifications and examples. Section 2.3.5 gives examples of combined cyber-physical threats. Finally, Section 2.3.6 includes other classification schemes briefly.

2.3.1. Overview of threat standards and models

As mentioned before, threats/hazards could be classified according to different purposes. Thus there are many different threat classification schemes using a variety of criteria. The papers [3, 4] include quite good coverages of existing classification frameworks. This section briefly overviews some of those commonly found in literature and well-known frameworks.

Open Systems Interconnection (OSI) model is a reference model for understanding data communications between any two networked systems. It is developed by the International Organization for Standardization (ISO) under OSI project. It divides network communication into seven layers. Each layer performs specific functions to support the layers above it and offers services to the layers below it. It covers all aspects of networks from physical layers to application layers including all protocols used. Naturally, threats/hazards could be looked at and grouped by these layers. It also helps to include measures at each layer against these threats.

OSI 7 layers:

- Application (layer 7)
- Presentation (layer 6)
- Session (layer 5)
- Transport (layer 4)
- Network (layer 3)
- Data link (layer 2)
- Physical (layer 1)

The advantage of grouping threats by these layers is that they help practitioners to focus on security measures against threats affecting those layers their applications are on. Some example classifications can be found in these papers [5–8].

STRIDE Model developed by Microsoft [9, 10] is an impact-based one. It models threats by the intention of the attacker such as:

- Spoofing of user identity: attackers pose as other users
- Data tampering: malicious modification of data by any means
- Repudiation: making applications/systems lose controls to properly track and log users' actions

- Information Disclosure (privacy breach or data leak): disclose of information to those who are not supposed to have it
- Denial of Service: make systems or network resources unavailable to its intended users by disrupting services
- Elevation of Privilege: unprivileged users gain privileged access

The ISO model [11] is another impact based model. There are five major security threats impacts and services:

- (1) Destruction of information and/or other resources,
- (2) Corruption or modification of information,
- (3) Theft, removal or loss of information and/or other resources,
- (4) Disclosure of information; and
- (5) Interruption of services.

Common Vulnerabilities and Exposures (CVE) [12] is a list of well-known and common identifiers for publicly known cybersecurity vulnerabilities. Use of CVE Entries, which are assigned by **CVE Numbering Authorities (CNAs)** from around the world, ensures confidence among parties when used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.

CVE Numbering Authorities (CNAs) [13] are organizations and companies from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. Those CVE IDs are provided to researchers, vulnerability disclosures, and information technology vendors in order to have a publicly available reference.

The Common Vulnerability Scoring System (CVSS) [14] provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its model ensures repeatable accurate measurement while enabling users to see the vulnerability characteristics that were used to generate the scores.

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
		None	0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Table 1: Score ratings for CVSS v2.0 and v3.0

CVSS v3.0 Rating Methodology, shown in Figure 5, adds some important modification to CVSS v2.0 Rating Methodology, shown in Figure 6, such as:

- New Physical attack vector
- New field for User Interaction (i.e. do we need the mark to visit a page?)
- New field for Scope (i.e. changing execution environment)

It also allows the base score to be adjusted to be more thoughtful of the environment (which will be useful if the beneficiaries have a full risk management function). For example, changing the complexity of an attack because the environment has extra protective measures.

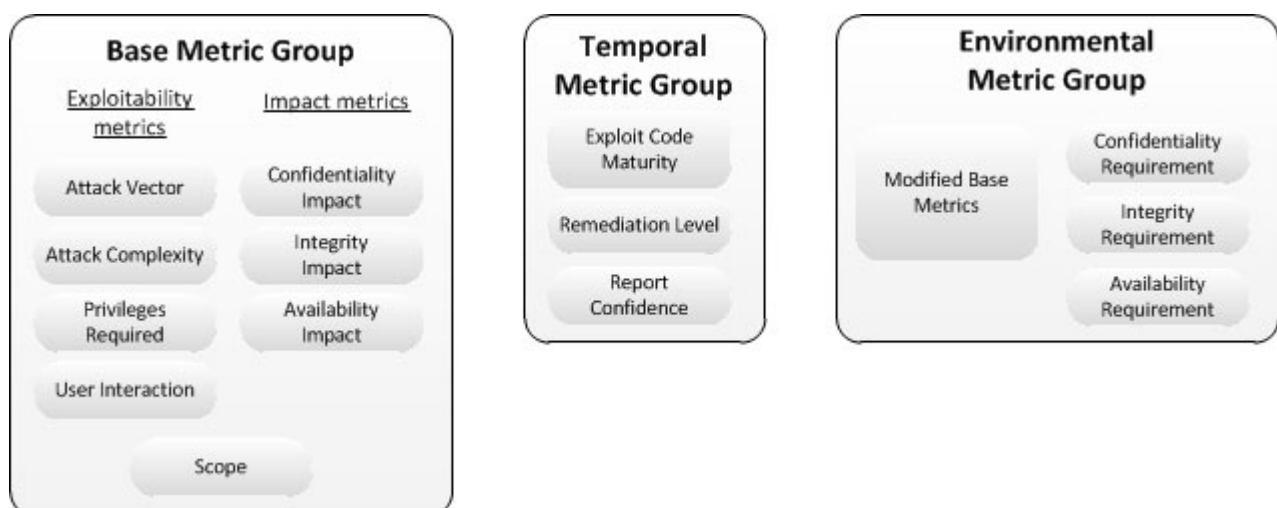


Figure 5: CVSS v3.0 Metric Groups³

³ CVSS v3.0 Metrics: <https://www.first.org/cvss/specification-document>



Figure 6: CVSS v2.0 Metrics⁴

NIST (National Institute of Standards and Technology) (SP 800-30, 2012) [15] is **Classification by Threat Sources as well as by Significance**. NIST's comprehensive overview of threat sources includes:

- Cyber or physical attacks
- Human errors
- Failure of resources
- Environmental disasters, accidents, or failures

By significance, NIST distinguishes the following types of security threats:

- **Errors and Omissions:** They are caused by intentional human mistakes. Errors and omissions are caused in the same way by daily transactions data entry clerks processing and by all types of users who create and edit data.
- **Fraud and Theft:** They can be performed by simply automating traditional forms of fraud and theft. For example, employer can use the computer (and program) for stealing small amounts of money from financial accounts with presumption that the small financial transaction will not be checked as suspicious.
- **Employee Sabotage:** For example, destroying hardware of facilities, planting logic bombs that destroy programs or data, entering data incorrectly, changing data.
- **Loss of Physical and Infrastructure Support:** They include power failures (outages, spikes, and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes.
- **Malicious Hackers:** It refers to those who break into computers without authorization and it comes either from outsiders or insiders.
- **Industrial Espionage:** The act of gathering proprietary data from private companies or the government for the purpose of aiding another company.

⁴ CVSS v2.0 Metrics: <https://www.first.org/cvss/v2/guide>

- **Malicious Code:** It refers to viruses, worms, Trojan horses and logic bombs.
- **Foreign Government Espionage:** It includes threats posed by foreign government intelligence services. Like travel plans of senior officials, civil defense and emergency preparedness, manufacturing technologies, satellite data, personnel and payroll data, and law enforcement, investigative, and security files.
- **Threats to Personal Privacy:** They arise from many sources. It comes, for instance, from the accumulation of vast amounts of electronic information about individuals by governments, credit bureaus, and private companies.
- **Disruption:** Circumstance or event that interrupts or prevents the correct operation of services and functions.
- **Usurpation:** Circumstance or event that results in control of services or functions by a threat source.
- **Disclosure:** Circumstance or event in which a threat source gains unauthorized access to data.

OWASP Risk Rating Methodology [16] addresses risk using the following standard risk model:

$$\text{Risk} = \text{Likelihood} * \text{Impact}$$

In order to determine factors that define “likelihood” and “impact” for application security, those factors are broken down in 6 unique steps as follows:

- Step 1: Identifying a Risk
- Step 2: Factors for Estimating Likelihood
- Step 3: Factors for Estimating Impact
- Step 4: Determining Severity of the Risk
- Step 5: Deciding What to Fix
- Step 6: Customizing Your Risk Rating Model

Step 4: Determining the Severity of the Risk: the likelihood estimate and the impact estimate are put collectively to determine an overall severity for this risk. This is accomplished by figuring out whether the likelihood is low, medium, or high and then do the equivalent for impact. The 0 to 9 scale is split into three parts as follows:

- Likelihood and Impact Levels

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

- Determining Severity

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Statistical classification on type of attacks

The **Zone-H Website**⁵ represents an online publicly available database which works as an archive for enlisting resources affected website defacement, see Figure 7 and Figure 8.

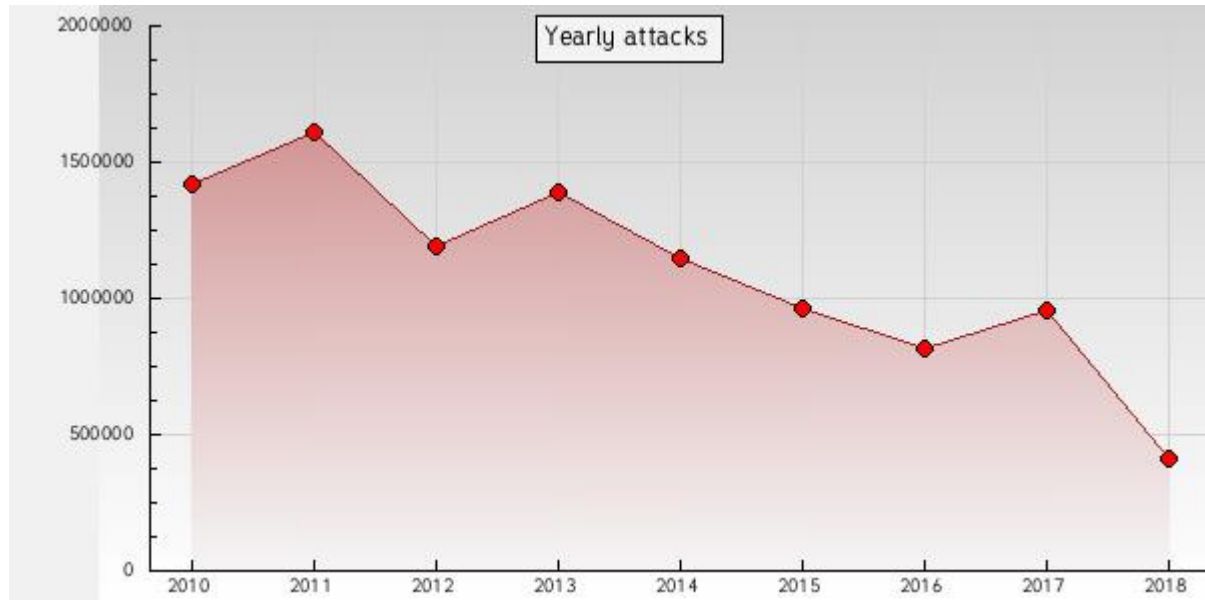


Figure 7: Website defacement statistics⁵

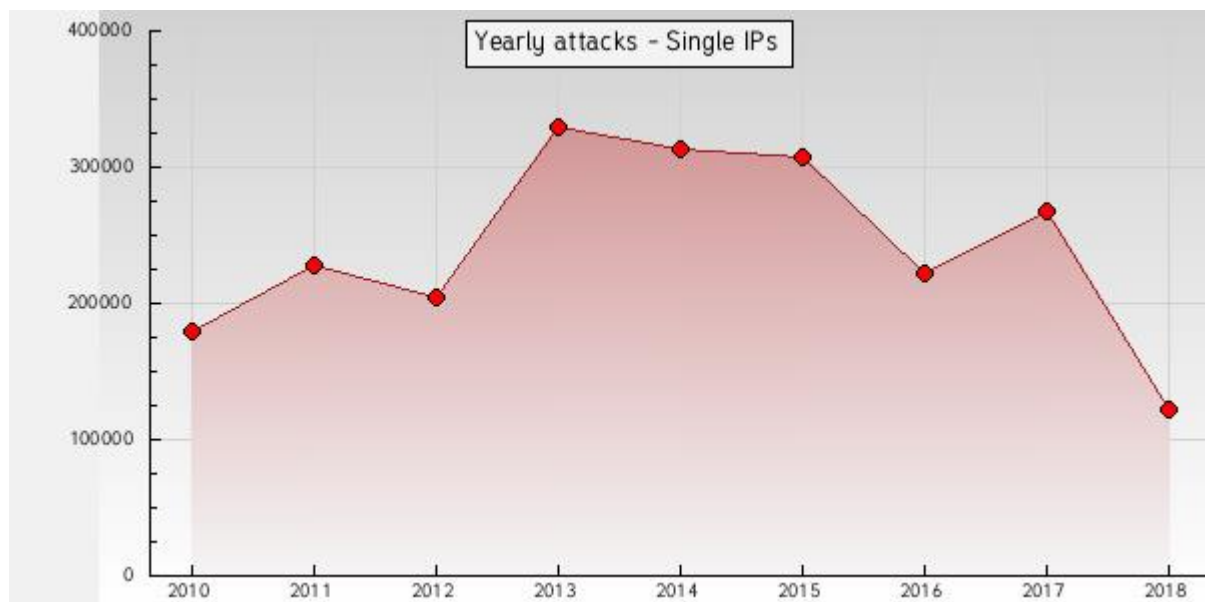


Figure 8: Website defacement statistics, Single IPs only⁵

⁵ <http://www.zone-h.org>

AbuseIPDB [17] is a project committed to helping combat the spread of hackers, spammers, and abusive activity on the internet. Screenshots of the AbuseIPDB statistics website are shown in Figure 9, Figure 10 and Figure 11.

AbuseIPDB — Reporting Statistics

Number of IP Address Reported in the last:

1,944

1 Hour

49,073

24 Hours

375,443

7 Days

1,577,896

30 Days

Figure 9: Screenshot of the AbuseIPDB website⁶

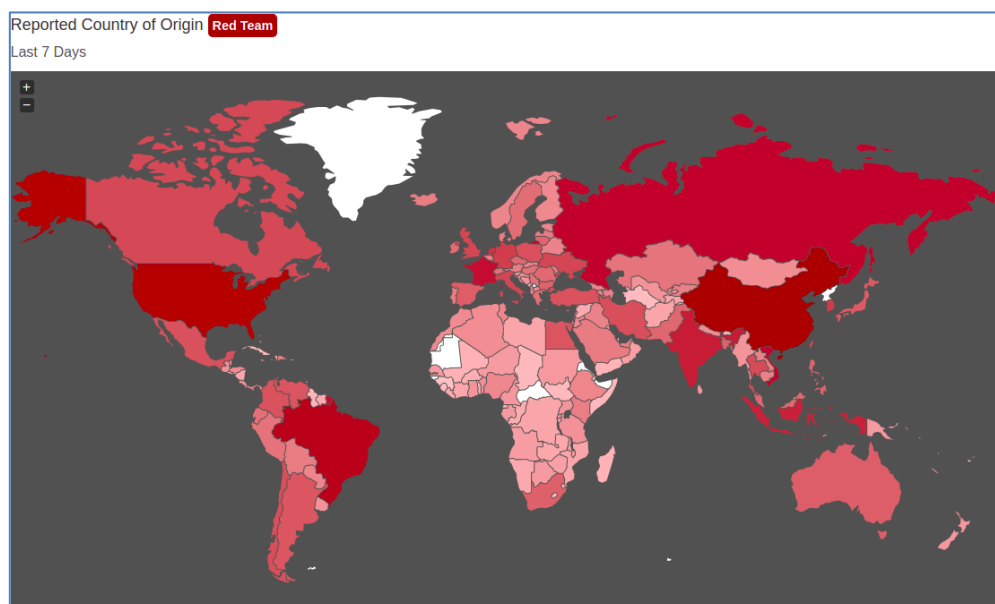


Figure 10: Statistic by number of unique attackers (Screenshot of the AbuseIPDB website⁶)

⁶ <https://www.abuseipdb.com/statistics> (accessed October 2018)

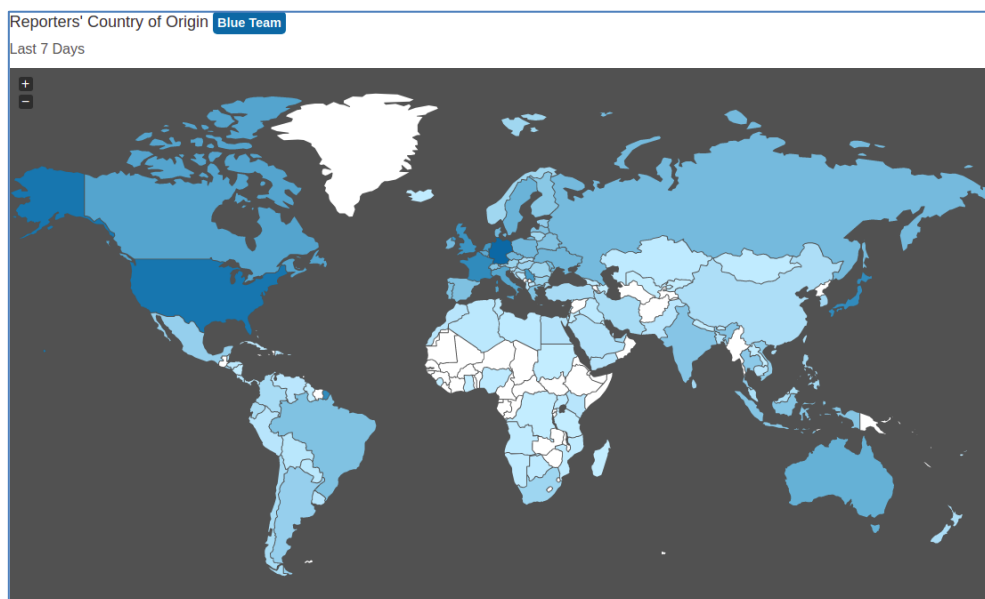


Figure 11: Statistic by number of unique reporters (Screenshot of the AbuseIPDB website⁶)

VirusTotal [18] aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus may have missed, or to verify against any false positives.

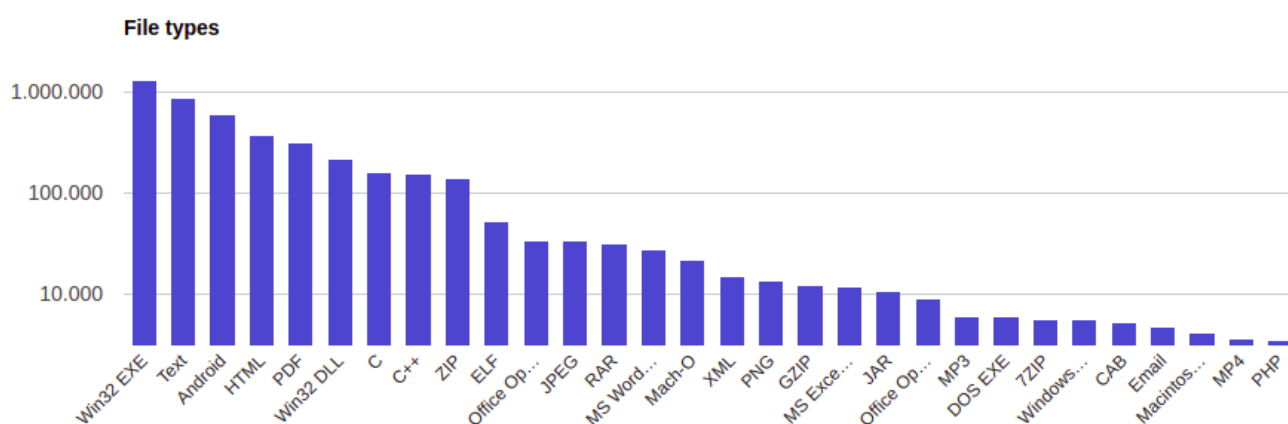


Figure 12: Submissions to VirusTotal [18] in October 2018.

2.3.2 Definition of security threats in telecom infrastructures

Various classification types are used for telecommunication security threats and related risks. In order to be able to provide a comprehensive threats overview for the resilience analysis that will be performed within the RESISTO project, an initial definition of security threats

related to the telecom infrastructures is given herein. Then, the existing threat databases will be presented, so that to highlight the need for the RESISTO classification.

According to ITU-T [19], a comprehensive review of security requirements must take into account: the parties involved; the assets that need to be protected; the threats against which those assets must be protected; the vulnerabilities associated with the assets and the environment; and the overall risk to the assets from those threats and vulnerabilities.

According to ITU-T, in general terms, there is a need to protect assets for:

- customers / subscribers who need confidence in the network and the services offered, including availability of services (especially emergency services);
- public community/authorities who demand security by directives and/or legislation, in order to ensure availability of services, privacy protection, and fair competition; and
- network operators and service providers who need security to safeguard their operation and business interests and to meet their obligations to customers, their business partners and the public.

The assets to be protected include:

- communication and computing services;
- information and data, including software and data relating to security services;
- personnel; and
- equipment and facilities.

A security threat is defined as a potential violation of security; a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm. Examples of threats include:

- unauthorized disclosure of information;
- unauthorized destruction or modification of data, equipment or other resources;
- theft, removal or loss of information or other resources;
- interruption or denial of services; and
- impersonation, or masquerading as an authorized entity.

Threats may be accidental (also sometimes called inadvertent) or intentional and may be active or passive, man-made or caused by natural phenomena. An accidental threat is one with no premeditated intent such as a system or software malfunction or a physical failure. An intentional threat is one that is realized by someone committing a deliberate act. Intentional threats may range from casual examination, using easily-available monitoring tools, to sophisticated attacks using special system knowledge. When an intentional threat is realized it is called an attack. An active threat is one that results in some change to the state or operation of a system, such as alteration of data or destruction of physical equipment. A passive threat involves no change of state. Eavesdropping and wiretapping are examples of passive threats.

A security vulnerability is a flaw or weakness that could be exploited to violate a system or the information it contains. If a vulnerability exists, then it is possible for a threat to be realized successfully unless effective countermeasures are in place. ITU-T recommendations recognize four types of vulnerability:

- threat model vulnerabilities, which result from failure to foresee possible future threats;

- design and specification vulnerabilities, which result from errors or oversights in the design of a system or protocol and make it inherently vulnerable;
- implementation vulnerabilities, which are introduced by errors or oversights during system or protocol implementation; and
- operation and configuration vulnerabilities, which originate from improper usage of options in implementations or weak deployment policies and practices (such as failure to use encryption in a wireless network).

With the development of Information and Communication Technologies and increasing accessibility to the Internet organizations become vulnerable to various types of threats. In fact, their information becomes exposed to cyber-attacks and their resulting damages. Threats come from different sources, like employees' activities or hacker's attacks.

Vulnerabilities consist of weaknesses or faults in a system which can be exploited by the attackers that may lead to dangerous impact. When vulnerabilities exist in a system, a threat may be manifested via a threat agent using a particular penetration technique to cause undesired effects [20]. Telecommunication network security also demands extensive cooperation between service providers. Recommendation ITU-T E.408 [21] provides an overview of security requirements and a framework that identifies security threats to telecommunication networks in general (both fixed and mobile; voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats. Recommendation ITU-T X.1205 [22] provides a taxonomy of security threats from an organizational point of view along with a discussion of the threats at the various layers of a network.

Depending on their source, threats can be man-made or natural and when causality is considered threats can be intentional, accidental or natural disaster. As for the affected system types, in general the following types are defined:

- physical threats that affect physical systems, buildings and infrastructure and
- cyber-threats that exploit vulnerabilities in computer systems and cause possible harm in the digital realm,
- cyber-physical threats that exploits vulnerabilities and can cause possible harm in systems controlled and monitored by computer-based algorithms (CPSs – i.e. – smart grids, autonomous automobile systems, robotics, medical monitoring etc.).

In addition, according to the context promoted in ITU-T X.800 [23], threats can also be classified as “accidental” or “intentional” and may be assessed as “active” or “passive”. In this context, accidental threats are those that happen with no premeditated intent. Examples of realized accidental threats comprise system malfunctions, operational blunders and software bugs. The intentional threats may vary from casual examination, using easily available and accessible monitoring tools, to sophisticated sort of attacks using special system knowledge. An intentional threat, if realized, may be considered to be a sort of an “attack”. Passive threats are those which, if taken place, would not result in any modification to any information contained in the system(s), and where neither the operation nor the state of the system is changed. The use of passive wire tapping to observe information being transmitted over a communications line is a realization of a passive threat. Active threats to a system involve the

alteration of information contained in the system, or changes to the state or operation of the system. A malicious change to the routing tables of a system by an unauthorized user is an example of an active threat⁷.

The X.800 security threats also apply to the cyber environment. According to the ITU-T X.800 conceptual approach, security features usually increase the cost of a system and may make it “harder to use”. Before designing a secure system, therefore, a recommended practice is to identify the specific threats against which protection is needed. This approach is known as the threat assessment. A system is vulnerable in many ways, but only some of them are exploitable because the attacker lacks the opportunity, or because the result does not justify the effort and risk of detection.

Threats are against assets, so the first step is to list out the assets that require protection. The next step of the assessment is a threat analysis, then a vulnerability analysis (including impact assessment), countermeasures and security mechanisms. In a broader concern, this process also implicates for: (i) identifying the vulnerabilities of the system; (ii) analysing the likelihood of threats aimed at exploiting these vulnerabilities; (iii) assessing the consequences if each threat were to be successfully carried out; (iv) estimating the cost of each attack; (v) costing out potential countermeasures, and; (vi) selecting the security mechanisms that are justified (possibly by using cost benefit analysis).

As it will be seen in the following section, quite many classification types exist already in literature or operational systems. However, based on the above assumptions, the above definition will be used as the primary reference point to describe the physical and cyber threats, and their combined impact dealt within RESISTO project. This reference baseline of defining threats is briefly described in the following, while further classification analysis will continue in the following section.

Threats classification principles

A literature review [24] shows the following principles for information security classification should be respected:

- **Acceptability:** the classification of logical and practices easy to be accepted by the majority.
- **Mutually exclusive:** Every threat classified in one category excludes all others because categories do not overlap. Every specimen should fit in at most one category.
- **Scalability:** classification method can adapt to technology, the ability to accurately define new types.
- **Certainty:** the characteristics of each category description are accurate.
- **Exhaustive:** The categories in a classification must include all the possibilities (all threat specimens).
- **Unambiguous:** All categories must be clear and precise so that classification is certain. Every category should be accompanied by unambiguous classification criteria defining what specimens to be placed in that category.

⁷ The Appendix I of the ITU-T X.800 Recommendation provides a brief summary of some specific types of attacks.

- **Repeatable:** Repeated applications result in the same classification, regardless of who is classifying.
- **Universality:** Can be adapted to different application requirements.
- **Usefulness:** It can be used to gain insight into the field of inquiry; it can be adapted to different application needs.
- **Availability:** classification of the different fields of practical value

These principles can be used in order to evaluate threat classifications. A well-established threat classification should support the most presented principles⁸ [25].

Physical Threats

The physical threats that could impact telecoms networks, include malicious attacks, non-deliberate threats, and natural hazards^{9, 10}.

Malicious Attacks:

These actions refer to damage caused by accidents, vandalism, internal sabotage and terrorism, including any kind of intentional or unintentional attacks, like land and airborne threats. Motivations for malicious intentional attacks can include financial gain (e.g. through metal theft) or causing disruption for the purpose of vandalism, espionage or terrorism. In 2007, telecoms infrastructures were the target of an attempted terrorist attack when Al-Qaeda reportedly planned to bomb a key internet exchange in London. Attacks of this kind can range from those using sophisticated military weaponry to those that don't use any specialized equipment as in the following examples:

- **Airborne and land threats:** hostile drones and UAVs bearing weaponry along with direct weaponry used in the vicinity of the critical telecom infrastructure. Nowadays, the telecom pillars, the antenna parks or the telecom buildings and rooftops are vulnerable to airborne threats and malicious attacks from the air and/or the vicinity of the telecom CI. Drones and UAVs present a dramatically increasing commercial use, making it easy and cheap to add dangerous payload.
- **Signal jammers:** signal jammers are used to disrupt mobile networks by transmitting interfering radio signals. Handheld signal jammers can be purchased cheaply online and their effects are localized (typically tens of meters) while more powerful devices are considered as deliberate actions of attack.
- **Cable damage:** copper or fiber optics cabling is either stolen or damaged from the access network and disrupts emergency service communications, resulting in higher costs for the telecom providers.

⁸ Howard MD. LeBlanc, Writing Secure Code 2nd ed., Redmond, Washington: Microsoft Press; 2003.

⁹ Security of UK Telecommunications, Houses of Parliament, Parliamentary Office of Science and Technology, UK, PostNote No 584, August 2018.

¹⁰ Telecommunications Networks – a vital part of the Critical National Infrastructure Version 1.1, EC-RRG (Electronic Communications Resilience and Response Group, Protecting Communications, 2004.

Non-Deliberate Threats

Examples of non-deliberate threats to telecoms networks include losses of key inputs due to unintentional actions, amongst which the most critical are:

- **System failures:** can occur in both hardware and software. System failures were identified as the most common cause of network disruption reported by ENISA annually since 2012 (see Section 2.3.3).
- **Power failures:** telecoms infrastructure is dependent on a continuous supply of power. Power failures were the second most common reason for network disruption reported by ENISA. These include electrical power, fuel (for backup generators and vehicle fleet) and material, as well as non-deliberate damages caused by human access (to operational installations).
- **Cable damage:** Excavation machines can cause damage to land-based cables, while damages to undersea cables caused by the anchors of fishing vessels or ships could also be counted.

Not only is the telecoms industry wholly dependent on electrical power, but the electrical power industry depends on telecoms to manage their extensive network of generators and grid distribution.

Natural Hazards

Annual reports from ENISA since 2012 show that these lead to the most prolonged disruption (30 hours on average in 2016, see Figure 13). Hazards of this kind include:

- **Severe weather:** flooding, strong winds, lightning, cold weather, and heatwaves have the potential to disrupt telecoms. Severe weather can cause disruption either through direct damage to infrastructure or loss of power, resulting in loss of mobile and internet connections. Furthermore, space weather (changes in the near-earth space environment) events can also disrupt telecoms and power infrastructure on the ground.
- **Seismic activity:** Earthquakes can also damage land-based infrastructure, especially in countries with intense seismic activity like Greece (OTE) or Italy (TEI).
- **Fire:** which is a self-evident threat
- **Accidental explosions:** in particular those caused by natural gas leaks.

Cyber Threats

Cyber threats can be quite many, different in type and manner, affecting the whole telecom operation as a software system and service. Telecom companies underpin many vital services and hold their customer's personal data, making them a cybercrime target growing dramatically nowadays. Cybercriminals can target telecoms companies directly or target customers through the network. Cyber threats can be intentional (i.e. hacking activities) or accidental (i.e., a computer malfunctioning). Indicative examples include:

- **Malicious cyber actions:** where deliberate breaches of the system or a service take place i.e. hacking actions, spoofing of user identity, information disclosure (privacy breach or data leak) and many other of similar types.
- **System/Logical failings:** To prevent being vulnerable to the failure of a single part of the system, telecommunications companies invest, where practical, in duplicate or triplicate back-ups for their equipment (redundancy) and diverse transmission routings. Thus, the 'logical' architecture of the service will be more resilient than the simple physical layout. But sometimes, due often to human error, these logical configurations can themselves fail to provide the expected level of resilience. The key is to avoid, wherever possible, 'single points of failure'. However, not all parts of the network can be made resilient and in these cases, the complementary processes of restoration and repair have to be strengthened.
- **Software failures:** All telecommunications networks are reliant on software-controlled equipment, and no software is immune from errors and operational failings. Unlike personal computers, it is not acceptable for a telecommunications network to crash and stop responding altogether. A particularly worrying form of software failure is called a 'systemic' or 'common-mode' failure, where a software error in one network node causes the same fault to occur in other connected nodes, leading to a 'runaway' failure of an entire network.
- **Device compromise:** devices used in telecoms networks (such as home routers) can be targeted in cyber-attacks. Once they are compromised, hackers can launch anonymous attacks or access services.
- **Vulnerabilities:** A weakness in system security procedures, hardware design, internal controls, software code, etc., which could be exploited to gain unauthorized access, to manipulate the integrity or to affect the availability of both classified or sensitive information and non-sensitive information.
- **Man-in-the-middle attacks:** communication between two parties may be covertly intercepted, recorded, and even altered by an attacker. Information collected may then be used for identity or data theft.
- **Denial-of-service attacks:** cyber-attacks in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a **distributed-denial-of-service (DdoS) attack**
- **Backdoor attacks:** attacks in which software development companies or hardware providers leave a single point of failure in order to obtain access to a system or application found in production.
- **Semantic attack:** modification and dissemination of correct and incorrect information to set someone into the wrong direction or to cover tracks or malicious activities.

- **Legacy protocols:** protocols describe the software that telecoms networks use to communicate with each other. Some protocols are decades old and were designed without considering future security issues.
- **Malicious code:** includes execution of viruses, worms, Trojan horses, and active Web scripts with intent to destroy or steal information. Perhaps the most well-known computer security threat, a computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to a personal computer in the process.
- **Phishing:** Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyber threat.
- **SQL injection:** A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.
- **Zero-day exploit:** A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time.

The Stages of the cyber-attacks include the following:

- **Survey:** Investigating and analyzing available information about the target in order to identify potential vulnerabilities
- **Delivery:** getting to the point in a system where a vulnerability can be exploited
- **Breach:** exploiting the vulnerability to gain some form of unauthorized access
- **Affect:** carrying out activities within a system that achieve the attacker's goal

Cyber-Physical Threats

As denoted earlier, cyber-physical threats include disruptions to information systems, which directly affect physical infrastructure services. In a more general term, exploited vulnerabilities can cause possible harm in systems controlled and monitored by computer-based algorithms (i.e. smart grids). Indicative examples include the following:

- **Electronic 'interference':** Telecommunications networks, especially those increasingly using IP technology, can be vulnerable to conditions entering the system via the network itself. Increasingly, these can be malicious in intent. A wide range of types of threat fall into this category, including:
 - Inappropriate signals injected by users, either too high a voltage or at the wrong frequency;
 - Similar signal pickup problems caused by radio interference, e.g. from amateur radio transmissions;

- Traffic overloads, often stimulated by advertising campaigns and TV based promotions;
- Denial of Service attacks – malicious attempts to damage a service, sometimes by traffic overload, sometimes by the transmission of ‘malware’ (malicious software);
- ‘Malware’, such as viruses, worms and Trojans;
- Hacking, including attempts to subvert the proper operation of the billing system in networks;
- The transmission of specifically crafted signaling messages, designed to cause disoperation of the network

Additionally to the above, in the following an important type of threats is provided, as a result of the complexity of the telecom systems and services offered nowadays:

Advanced Persistent Threat (APT)

Advanced Persistent Threats (APTs) are considered and are often defined as the threats that are the most challenging to detect and defend against. Conventional threats tend to be to a large extent opportunistic. However, whatever their motivation (financial, reputation, intellectual property, political, etc.), the actors behind an APT have the capability and determination to achieve a specific target.

An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. An APT usually targets either private organizations, states or both for business or political motives. APT processes require a high degree of covertness over a long period of time. As the name implies, APT consists of three major components or processes, that is: advanced, persistent and threat: The “advanced” process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The “persistent” process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The “threat” process indicates human involvement in orchestrating the attack¹¹. Definitions of precisely what an APT is can vary, but can be summarized by their named requirements below, approached by an operator’s point of view¹²:

Advanced: Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques such as telephone-interception technologies and satellite imaging. While individual components of the attack may not be classed as particularly “advanced” (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily

¹¹ More details can also be found at: https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT

¹² More information can be found, inter-alia, at: https://en.wikipedia.org/wiki/Advanced_persistent_threat

procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from “less advanced” threats.

Persistent: Operators give priority to a specific task, rather than opportunistically seeking information for financial or other gain. This distinction implies that the attackers are guided by external entities. The targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a “low-and-slow” approach is usually more successful. If the operator loses access to their target they usually will reattempt access, and most often, successfully. One of the operator’s goals is to maintain long-term access to the target, in contrast to threats who only need access to execute a specific task.

Threat – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well-funded.

APTs often breach entities via Internet, infected media, external exploitation, or internal exploitation. Internet breach may take place by sending malicious payload via email attachments, peer-to-peer file sharing, or spear phishing; on the other hand, media infection may consist of infected Universal Serial Bus (USB) memory sticks, infected memory cards, or infected appliances; furthermore, external exploitation may occur through rogue WiFi penetration, zero day attack, or smart phone bridging. Internal exploitation, on the other hand, can be encountered by a rogue employee, social engineering, or funded placement.

APT frequently refers to a group, such as a government, with both the capability and the intent to target, persistently and effectively, a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information¹³, but applies equally to other threats such as that of traditional espionage or attacks. Other recognized attack vectors include infected media, supply chain compromise, and social engineering. The purpose of these attacks is to place custom malicious code on one or multiple computers for specific tasks and to remain undetected for the longest possible period. Knowing the attacker artifacts, such as file names, can help a professional make a network-wide search to gather all affected systems¹⁴. Individuals, such as an individual hacker, are not usually referred to as an APT, as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.

Bodmer, Kilger, Carpenter and Jones defined the following APT criteria [26]:

Objectives – The end goal of the threat, the adversary.

¹³ Also see: <https://www.secureworks.com/resources/sb-advanced-threat-protection>

¹⁴ For further informative details also see: <https://www.maliciousfilehunter.com/feature-live-search.php>

Timeliness – The time spent probing and accessing the system.

Resources – The level of knowledge and tools used in the event (skills and methods will weigh on this point).

Risk tolerance – The extent the threat will go to in order to remain undetected.

Skills and methods – The tools and techniques used throughout the event.

Actions – The precise actions of a threat or numerous threats.

Attack origination points – The number of points where the event originated.

Numbers involved in the attack – How many internal and external systems were involved in the event, and how many people's systems have different influence/importance weights.

Knowledge source – The ability to discern any information regarding any of the specific threats through online information gathering.

For the target specialized, what matters is not how secure it is in comparison with the competition, but how secure it is in absolute terms. The Operation Aurora APT led Google to rapidly lose 18% of the online search market share in China¹⁵, Stuxnet caused Iran to decommission 1,000 Uranium enrichment centrifuges¹⁶, while EMC's security division spent US\$66 Million to undo the damages brought about by an APT exfiltrating data from its network over several months¹⁷.

More recently, the world's first global ransomware attack, Wannacry, which was estimated to reach a cost of €3.4 Billion in addition to almost disabling the National Health System in the UK¹⁸, was shown to be based on code produced by a known APT. Following on from two years of rapidly increasing number and sophistication of APT attacks, ENISA's threat landscape report predicts that high-capability agents will specialize in the future on more off-the-shelf campaigns rather than custom techniques, so as to enhance stealthiness and further improve APT effectiveness¹⁹, showing that APTs exemplify the advanced cyber threat due to increasing frequency, increasing importance and increasing difficulty in countering. The overall picture of the APT product landscape is fragmented and limited, which explains the steady increase in APT breaches and the damages caused. From the commercial exploitation perspective, the APT protection market is growing rapidly (20% per year, in contrast to the 6% growth of the rest of the cyber security sector), expected to reach €6.4 billion by 2020 and it has been noted specifically that there are "no mature players in this market" yet. This makes APT protection an extremely attractive area for growth of the European cyber security sector, which is severely underrepresented, as currently no key player in this market is European.

¹⁵ Mandiant, "APT1: Exposing one of China's Cyber Espionage Units.," Mandiant Corporation, Alexandria, VA, 2013.

¹⁶ D. Albright, P. Brannan and C. Walrond, "Stuxnet malware and Natanz: Update of ISIS," Institute for Science and International Security, vol. 15, pp. 739883-3., 22 December 2010.

¹⁷ TrendMicro, "Connecting the dots," [Online]. Available:
<http://www.trendmicro.co.uk/infographics/connecting-the-apt-dots/index.html>

¹⁸ J. Berr, "'WannaCry' ransomware attack losses could reach \$4 billion. CBS News," 16 5 2017. [Online]

¹⁹ ENISA., "ENISA Threat Landscape Report 2016.," ENISA, 2017.

2.3.3 The European Union Agency for Network and Information Security – ENISA

The telecommunication infrastructure providers have to report security incidents with a significant impact on the provided services to the national telecom regulatory authorities (NRAs) which subsequently have to report a part of those to the ENISA, based on EU-wide thresholds. This procedure is defined in the European Directive 2009/140/EC on a common regulatory framework for electronic communications networks and services, art. 13 a.

“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.”

ENISA produces “Annual Incident Reports” for the telecommunications sector which are published yearly by the ENISA since 2011. Each year, 28 to 30 countries contribute to this report.

Telecom companies are required to report to the NRAs security breaches and incidents that have a significant impact on the availability of their network. For an incident to be reported, it needs to be above a threshold related to number of customer-hours lost. However, this does not take into account unsuccessful attacks. An analysis of the reported incidents is published annually, however, a breakdown of the number of hours lost for each incident is not provided. For example, of the 678 incidents reported from September 2016 to August 2017, 93% were caused by hardware and software system failures.

The following graphs show the development of the reported incidents (per root cause category, percentage of affected services and duration of incidents) during the years 2011 to 2017²⁰.

²⁰ <https://www.enisa.europa.eu/publications/annual-incident-reports-2011-up-to-2017>

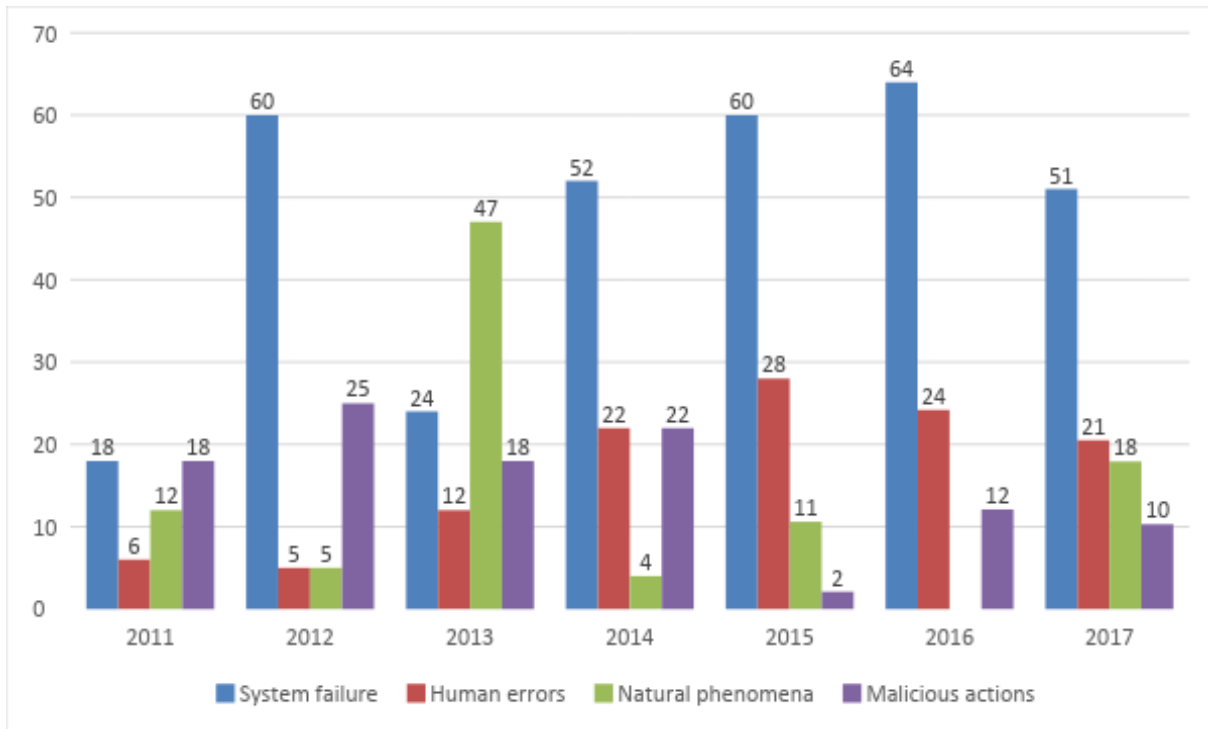


Figure 13: Chart of percentage of significant incidents per root cause category, development 2011-17

Figure 13 shows that in the first two years of reporting, “third party failure” has been used as one of five main root causes. Since 2013, reporting was reduced to the four root causes shown in graph 1 with “third party failures” displayed separately. All “third party failures” had to be assigned to one of the other four causes since then.

Obviously, system failures have been the reason for most significant incidents throughout the reporting years. Malicious actions seem to be decreasing slightly whereas human errors show a rather great significance in the last years.

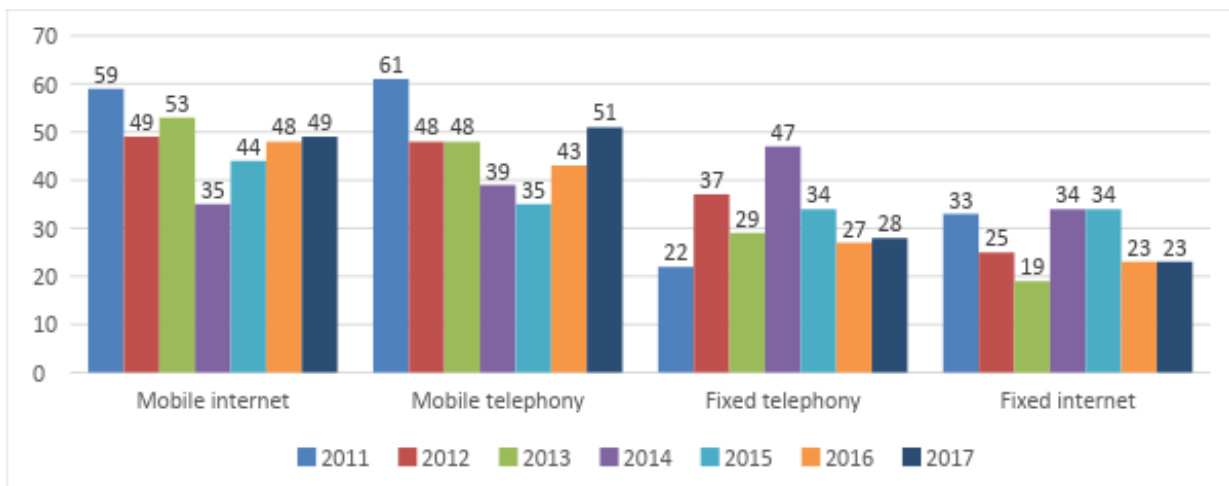


Figure 14: Chart of percentage of affected services, development 2011 - 2017

In Figure 14, the services affected by the incidents are shown as a percentage of all incidents. The mobile services are more affected by incidents than the fixed ones (except for 2014, where fixed telephony was the most affected service). In 2014 and 2015, the numbers for fixed and mobile services are noticeable more similar in comparison to the other years.

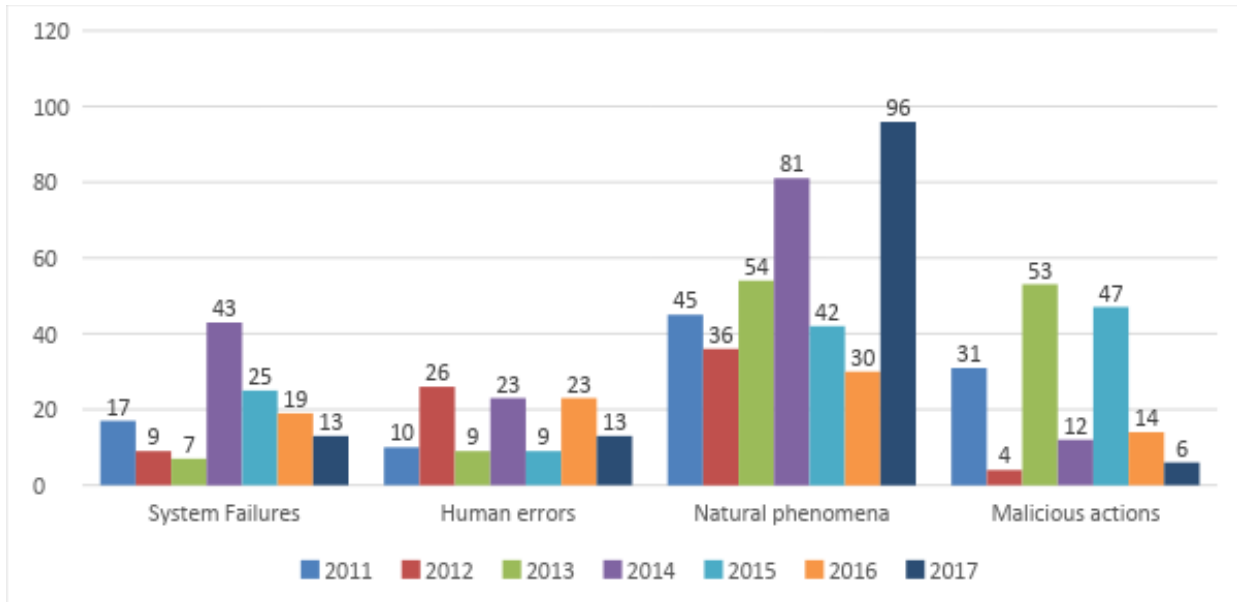


Figure 15: Chart of duration of incidents per root cause category in hours, development 2011 - 2017

Figure 15 displays the duration of the incidents throughout the years 2011 to 2017. It does not seem as if there is a trend in the duration of the incidents in any root cause category. In 2017 and 2014, “natural phenomena” caused longer lasting incidents than “usual”, as well as “malicious actions” did in 2013 and 2015.

Concluding from the non-existing obvious trends in the displayed contexts, the RESISTO platform should take into account all mentioned threats. It is seen that system failures, human errors, natural phenomena and malicious actions are referred as incidents; however, each of the above category involves a set of security threats, either physical or cyber ones which needs to be taken into account in a resilience analysis like the one to be performed in RESISTO. Furthermore, the level of detail in the ENISA incidents reports is not sufficient for RESISTO.

In this respect, in the following, an initial identification of the related various kinds of threats will be provided, in order to enable the reader to have a comprehensive overview of the inherent security risks related to the telecom critical infrastructures.

2.3.4 Malware classifications and examples

Before proceeding to further existing classifications the following description and explanations concerning malware are also provided for a more comprehensive overall approach.

Malware is a common name given to a software which is malicious to computing systems. According to a very recent report on cost of cybercrimes, malwares is the most costly type of all cybercrimes and on average companies spend \$2.4 million on malware attacks.²¹

Malware classifications are not consistent across the industry, but one commonly used classification methodology divides malwares into three generic types by the different ways they spread: Trojans, worms and viruses.

- **Trojans are malicious programs pretending to be legitimate.** Trojans do not self-replicate. The users are usually tricked into activating these malicious programs on their computing systems through social engineering. In recent years, Trojans became the most incidental and prevalent malwares. It is estimated that Trojans comprise 70%-80% of all the malware attacks on an annual basis. Within Trojans, there are different types based on functionalities, e.g. a backdoor allowing hackers to gain access and control of the user's system, a downloader allowing different parts of the malicious components to be downloaded, a keylogger allowing the hackers to access all the information the user typed on the keyboard, a ransomware allowing the hackers to encrypt all the data on the user's system and then ask for ransom to be paid to get the data back. The propagation of Trojans is usually done through the user's social network.
- **Worms are malwares that can self-replicate.** Worms can spread automatically through computer networks. The propagation of a worm is generally very fast and aggressive because worms utilise the actual computing network rather than waiting for the user to fall into the trap to activate it. The prevalence of worms is not as high as Trojans in recent years, but if any malware packages include a worm component, e.g. WannaCry, NotPetya, the propagation can be very fast and the scale of attack damages can be huge.
- **Viruses are another type of malwares** that can self-replicate but need to insert or attach themselves into other mediums to make the infection happen. Viruses include file infectors, boot sector viruses and interpreted viruses. File viruses also include prepending and appending viruses and inserting viruses. Viruses are not as common as worms or Trojans but are still seen in recent years.

Increasingly, successful modern malware attacks do not 100% rely on one single type of malwares but often package multiple different types of malwares into a malware toolkit to maximize the chance of success. For example, WannaCry and NotPetya both have Trojan components and worm components to realise different functionalities. These ransomwares used the Trojan components to first infiltrate the organization which were targeted and then used the worm components to spread rapidly through the network.

Here is an example of the malware incidence by generic classifications listed above²²:

²¹ Cost of Cyber Crime Study, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

²² Malware statistics by type, Panda Security, <https://www.pandasecurity.com/mediacenter/press-releases/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record>

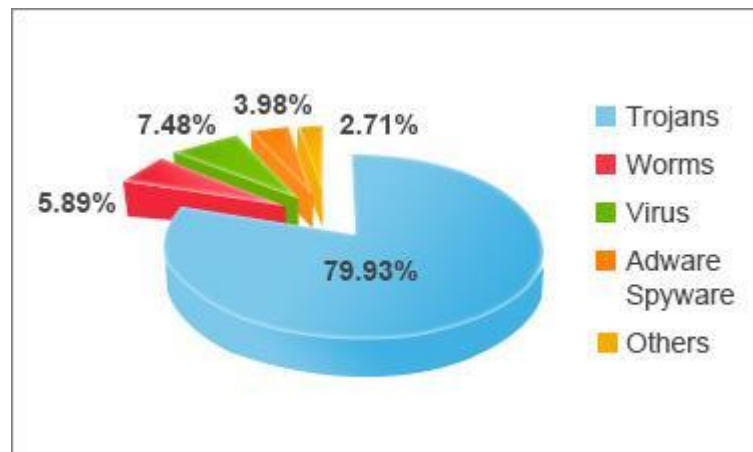


Figure 16: Malware infections by type in Q1 2013, Panda Security

2.3.5 Cyber-Physical System Security classifications and examples

A Cyber-Physical System (CPS) is a computing system or algorithm used to monitor and control physical systems²³. In recent years, CPSs are developed and deployed at massive scale in many different areas. Industrial Control Systems (ICS), Smart Grid, IoT systems, quite often as part of the critical infrastructure, heavily rely on CPSs. Because of the importance of CPSs, they should be as resilient as possible and have zero vulnerabilities, but unfortunately that is not the case. Recent damages include Stuxnet attack on ICS²⁴, Medjak on medical devices²⁵ and Mirai on IoT devices²⁶. End of 2017, a new malware called HATMAN or TRITON surfaced and it was the first publically identified industrial safety system malware²⁷.

According to a recent study on CPS classification, there are four representative types of CPS threats and security by application area [27]:

- **ICS** are control systems used in different industries. ICS are generally a very important component in critical infrastructure and because of its importance, generally they are not connected to the internet. But any weakness of the system itself or any human error in using ICS could see a catastrophic damage and loss of human wealth and lives.
- **Smart grid systems** are systems enabling control and optimization of power grid at the local and national level. Compared to the traditional grid, a smart grid provides optimized power and load control at national, local and household levels. Any attack on the smart grid

²³ Cyber-physical system, https://en.wikipedia.org/wiki/Cyber-physical_system

²⁴ Stuxnet attack, <https://en.wikipedia.org/wiki/Stuxnet>

²⁵ Medical device hijack, https://en.wikipedia.org/wiki/Medical_device_hijack

²⁶ Mirai (malware), [https://en.wikipedia.org/wiki/Mirai_\(malware\)](https://en.wikipedia.org/wiki/Mirai_(malware))

²⁷ Triton (Hatman), <https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/>

systems could result in either power blackout at the household level and/or local level, or even blackout at the national level. And blackouts subsequently result in enormous loss and damage.

- **Smart medical device:** Modern medical devices have the advantage of delivering better health care through monitoring and control functions which can have a positive impact on the patients. Attacks on smart medical devices can compromise patient privacy and can pose huge risk on patients' lives.

- **Smart cars** are cars equipped with modern information and control technologies to make the cars easier and more comfortable to drive and control. Human safety by far is the most important issue in smart car development and deployment. If the attackers take control of the communication systems and components of the cars, human lives are put under huge risks.

2.3.6. Other classification schemes

As it is seen hereafter, various threat classification schemes and databases can be found either in the literature or in national and international agencies reports or related assessments of the private sector. As it seems, each taxonomy presents also specific gaps and weaknesses highlighting the requirement of developing a classification tailored to the need and scope of the RESISTO project.

The already existing threat classification schemes and databases are briefly described herein:

Applying OSI layer [28] to model network security is an example of classification by OSI layers. It includes some typical threats found at each layer:

- **Physical Layer**

- Physical Layer Vulnerabilities: Loss of power, loss of environmental control, physical theft of data and hardware, physical damage or destruction of data and hardware, unauthorized changes to the functional environment (data connections, removable media, adding/removing resources), disconnection of physical data links, undetectable interception of data, keystroke & other input logging
- Physical Layer Controls: Locked perimeters and enclosures, electronic lock mechanisms for logging & detailed authorization, video & audio surveillance, PIN & password secured locks, biometric authentication systems, data storage cryptography, electromagnetic shielding

- **Data Link Layer**

- Link Layer Vulnerability Examples: MAC address spoofing (station claims the identity of another), VLAN circumvention (station may force direct communication with other stations, bypassing logical controls such as subnets and firewalls). Spanning tree errors may be accidentally or purposefully introduced, causing the layer two

environment to transmit packets in infinite loops. In wireless media situations, layer two protocols may allow free connection to the network by unauthorized entities, or weak authentication and encryption may allow a false sense of security. Switches may be forced to flood traffic to all VLAN ports rather than selectively forwarding to the appropriate ports, allowing interception of data by any device connected to a VLAN.

- Link Layer Controls: MAC address filtering - identifying stations by address and cross-referencing physical port or logical access. Do not use VLANs to enforce secure designs. Layers of trust should be physically isolated from one another, with policy engines such as firewalls between. Wireless applications must be carefully evaluated for unauthorized access exposure. Built-in encryption, authentication, and MAC filtering may be applied to secure networks.

- **Network Layer**

- Network Layer Vulnerabilities: Route spoofing - propagation of false network topology, IP Address Spoofing - false source addressing on malicious packets, identity & resource ID vulnerability - Reliance on addressing to identify resources and peers can be brittle and vulnerable
- Network Layer Controls: route policy controls - use strict anti-spoofing and route filters at network edges, firewalls with strong filter & anti-spoof policy, ARP/Broadcast monitoring software, implementations that minimize the ability to abuse protocol features such as broadcast

Transport layer

- Transport Layer Vulnerabilities: Mishandling of undefined, poorly defined, or “illegal” conditions. Differences in transport protocol implementation allow “fingerprinting” and other enumeration of host information. Overloading of transport-layer mechanisms such as port numbers limit the ability to effectively filter and qualify traffic. Transmission mechanisms can be subject to spoofing and attack based on crafted packets and the educated guessing of flow and transmission values, allowing the disruption or seizure of control of communications.
- Transport Layer Controls: Strict firewall rules limiting access to specific transmission protocols and sub-protocol information such as TCP/UDP port number or ICMP type. Stateful inspection at firewall layer, preventing out-of-state packets, “illegal” flags, and other phony packet profiles from entering the perimeter. Stronger transmission and layer session identification mechanisms to prevent the attack and takeover of communications.

- **Session and Presentation layers**

- Session Layer Vulnerabilities: Weak or non-existent authentication mechanisms. Passing of session credentials such as user ID and

password in the clear, allowing intercept and unauthorized use. Session identification may be subject to spoofing and hijack. Leakage of information based on failed authentication attempts. Unlimited failed sessions allow brute-force attacks on access credentials.

- Session Layer Controls: Encrypted password exchange and storage. Accounts have specific expirations for credentials and authorization. Protect session identification information via random/cryptographic means. Limit failed session attempts via timing mechanism, not lockout.
- **Application Layer**
 - Application Layer Vulnerabilities: Open design issues allow free use of application resources by unintended parties. Backdoors and application design flaws bypass standard security controls. Inadequate security controls force “all-or-nothing” approach, resulting in either excessive or insufficient access. Overly complex application security controls tend to be bypassed or poorly understood and implemented. Program logic flaws may be accidentally or purposely used to crash programs or cause undesired behavior.
 - Application Layer Controls: Application level access controls to define and enforce access to application resources. Controls must be detailed and flexible, but also straightforward to prevent complexity issues from masking policy and implementation weakness. Standards, testing, and review of application code and functionality. A baseline is used to measure application implementation and recommend improvements. IDS systems to monitor application inquiries and activity. Some host-based firewall systems can regulate traffic by application, preventing unauthorized or covert use of the network.

Classification by Chidambaram, 2004

This paper [29] includes a classification by three categories: network threats, server or host threats, and application threats. The following are examples of the threats included in each of the categories:

- **Network Threats:** We can cite as a major network threats denial of service attack, Trojan horses, worms, IP spoofing, SYN flooding, connection hijacking, and faulty configuration of firewall rules which allow outsiders to get access to a database and change the data.
- **Server Threats:** They represent threats that allow crackers to exploit known servers vulnerabilities like lack of clearly defined trust boundaries, improper server hardening guidelines resulting in a mismatch between the server configuration and the security context in which it's placed.
- **Application Threats:** For instance: code that's prone to buffer overflows, SQL injection, or cross-site scripting, defective or missing data encryption resulting in password compromise. This classification is simple and it presents an exhaustive list of threats (it covers all threats).

However, it is based on one criterion for classification. This classification did not provide a mutually exclusive classification scheme. For example, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users and thus it affects hosts, servers and networks and we cannot classify it easily. In addition to that, misconfigured servers and hosts can serve as network security threats as they unnecessarily consume resources.

STIX (Structured Threat Information Expression)

STIX [30] was a language developed by the US Department of Homeland Security (DSH) and the MITRE corporation, now by OASIS in the newly formed Cyber Threat Intelligence Technical Committee. The STIX language has a number of constructs or components, including the following:

- **Observable:** A dynamic event or stateful property, represented in Cyber Observable eXpression (CybOX).
- **Indicator:** An observable with context. An indicator can contain a time range, information source, intrusion detection system rules, etc.
- **Incident:** A set of activity associated with the same adversary along with context.
- **Tactics, Techniques and Procedures (TTP):** Represents the modus operandi of the adversary.
- **Exploit Target:** A weakness of a victim in light of a TTP.
- **Course of Action (COA):** Defensive actions against a threat (prevention, remediation, mitigation).
- **Campaign:** A set of related TTPs, indicators, incidents and exploit targets.
- **Threat Actor:** The cyber adversary.

Common Weakness Enumeration (CWE) List Version 3.1²⁸ classification system and is based on a community initiative aimed at creating a list of specific and succinct definitions for each common type of weaknesses. They can be split in three categories:

Category #1: Research Concepts, a view that is intended to classify threats and weaknesses mainly organized according to abstractions of software behaviors. This classification ignores the detection, the location in the code or when they are introduced in the SDLC (software development life cycle). The following table presents the Research Concepts components.

²⁸ Common Weakness Enumeration (CWE): <https://cwe.mitre.org/data/>

Research Concepts	Incorrect Calculation
	Incorrect Access of Indexable Resource ('Range Error')
	Use of Insufficiently Random Values
	Improper Interaction Between Multiple Correctly-Behaving Entities
	Improper Control of a Resource Through its Lifetime
	Insufficient Control Flow Management
	Protection Mechanism Failure
	Incorrect Comparison
	Improper Check or Handling of Exceptional Conditions
	Improper Enforcement of Message or Data Structure
	Improper Adherence to Coding Standards

Category #2: Development Concepts is a view that organizes threats and weaknesses around concepts that are frequently used or encountered in software development. This view is usually used by developers and assessment vendors. This view also provides a variety of categories that are intended to simplify navigation, browsing, and mapping such as the following:

Development Concepts	Configuration
	Data Processing Errors
	Pathname Traversal and Equivalence Errors
	Numeric Errors
	7PK ²⁹ – Security Features
	7PK – Time and State
	Error Conditions, Return Values, Status Codes
	Resource Management Errors
	Channel and Path Errors
	Handler Errors
	Behavioral Problems
	Business Logic Errors
	Web Problems
	User Interface Security Issues
	Initialization and Cleanup Errors
	Pointer Issues
	Mobile Code Issues
	Often Misused: Arguments and Parameters
	Expression Issues
	Violation of Secure Design Principles
	Bad Coding Practices

Category #3: Architectural Concepts is a way to assist architects in identifying potential mistakes that can be made when designing software. The following

²⁹ 7PK: Seven Pernicious Kingdoms (<http://www.fortify.com/vulncat/>).

table describes main types of mistakes or weaknesses that can be made in this phase of development.

Architectural Concepts	Audit
	Authenticate Actors
	Authorize Actors
	Cross Cutting
	Encrypt Data
	Identify Actors
	Limit Access
	Limit Exposure
	Lock Computer
	Manage User Sessions
	Validate Inputs
	Verify Message Integrity

The 2011 CWE/SANS Top 25 Most Dangerous Software Errors³⁰ contains a curated list of the most widespread and critical errors and threats that can lead to serious vulnerabilities in software.

The Top 25 list is a tool having a wide spectrum of study cases, including:

- a) **for education and awareness**, to help programmers to prevent most common types of vulnerabilities
- b) **for software customers**, this list can help them to ask for more secure software
- c) **for researchers in software security**, can be used to focus on a subset of all known security weaknesses.
- d) **for software managers and chief information officers**, can be used to measure progress in their efforts to secure software
- e) **for RESISTO**, this list, along with others, can help the partners to define, analyse and prioritise most common threats on existing technologies

³⁰ The 2011 CWE/SANS Top 25 Most Dangerous Software Errors <https://cwe.mitre.org/data/definitions/900.html>

Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3]	79	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75	CWE-798	Use of Hard-coded Credentials
[8]	75	CWE-311	Missing Encryption of Sensitive Data
[9]	74	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)
[13]	69.3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[14]	68.5	CWE-494	Download of Code Without Integrity Check
[15]	67.8	CWE-863	Incorrect Authorization
[16]	66	CWE-829	Inclusion of Functionality from Untrusted Control Sphere
[17]	65.5	CWE-732	Incorrect Permission Assignment for Critical Resource
[18]	64.6	CWE-676	Use of Potentially Dangerous Function
[19]	64.1	CWE-327	Use of a Broken or Risky Cryptographic Algorithm
[20]	62.4	CWE-131	Incorrect Calculation of Buffer Size
[21]	61.5	CWE-307	Improper Restriction of Excessive Authentication Attempts
[22]	61.1	CWE-601	URL Redirection to Untrusted Site ('Open

			Redirect')
[23]	61	CWE-134	Uncontrolled Format String
[24]	60.3	CWE-190	Integer Overflow or Wraparound
[25]	59.9	CWE-759	Use of a One-Way Hash without a Salt

OWASP Top Ten 2017 Project³¹ is another popular and accepted by the industry classification project maintained mainly by Open Web Application Security Project (OWASP) community and is used as a powerful awareness document for web application security, especially for most critical security risks to web applications. This project is also accepted by many security specialists as a methodology for security testing, such as code review or penetration testing, against applications. The following list summarizes the top:

- A1:2017-Injection
- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure
- A4:2017-XML (eXtensible Markup Language) External Entities (XXE)
- A5:2017-Broken Access Control
- A6:2017-Security Misconfiguration
- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization
- A9:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging & Monitoring

ISO/IEC 27002³² is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), titled Information technology – Security techniques – Code of practice for information security controls.

ISO/IEC 27002 classifies all security controls needed for all weaknesses (as in vulnerabilities or disturbances) and threats to 14 main topics as follows:

- Information Security Policies
- Organization of Information Security

³¹ OWASP Top Ten 2017 Project: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

³² ISO/IEC 27002: <http://www.iso27001security.com/html/27002.html>

- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and environmental security
- Operation Security
- Communication security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Cyber-Physical Attacks by George Loukas is a book which is not strictly a classification scheme, but contains various attacks under different categories.³³

³³ <https://www.elsevier.com/books/cyber-physical-attacks/loukas/978-0-12-801290-1>

2.4. Existing threat databases

This section briefly overviews and lists existing hazards and threats databases we have found and reviewed. Only brief descriptions are given. For details, refer to the given urls.

1. VDC – Vulnerability Database Catalog³⁴

This catalog initially contains a set of vulnerability databases (VDBs) that were surveyed by the Vulnerability Reporting and Data eXchange Special Interest Group (VRDX-SIG) to observe differences in identifiers, coverage and scope, size, abstraction and other characteristics. VDBs are loosely defined as sites that provide vulnerability information, such as advisories, with identifiers. Included VDBs are free to access, substantially public, and have broad scope and coverage (not limited to a single vendor or research organization).

2. CVE – Common Vulnerabilities and Exposures³⁵

This is a dictionary of common names (ie. CVE identifiers) for publicly known information security vulnerabilities. It's maintained by MITRE.

3. NVD – National Vulnerability Database^{36 37}

NVD is the US government repository of standards based vulnerability. It provides a list of common vulnerabilities and exposures (CVE) with over 77,000 entries predominately for, but not exclusive to software used within the United States. Each CVE is composed of: identifier (CVE-2013-1234), a description and references. The database is maintained by MITRE.

4. US-CERT – Vulnerability Notes Database³⁸

VND is maintained by United States Computer Emergency Response Team (US-CERT). It publishes a wide variety of vulnerabilities. It includes summaries, technical details, remediation information and lists of affected vendors. Most Vulnerability Notes are the result of private coordination and disclose efforts. Each Note has identifier (VU#581311), overview, description (CWE-306: Missing Authentication for critical function – CVE-2018-5393), impact and solution.

5. CERT-EU – Vulnerability alerts/news³⁹

CERT-EU is a permanent Computer Emergency Response Team for the EU institutions, agencies and bodies. The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the Member States and beyond as well as with specialized IT security companies.

³⁴ <https://www.first.org/global/sigs/vrdx/vdb-catalog>

³⁵ <https://cve.mitre.org/>

³⁶ <https://www.cvedetails.com>

³⁷ <https://cve.mitre.org/>

³⁸ <https://www.kb.cert.org/vuls>

³⁹ <https://cert.europa.eu/cert/filterededition/en/VulnerabilitiesApplications.html>

It includes alerts/news by product vulnerabilities, threats and incidents, hacking/techniques, and a category called Vulnerabilities in applications, database management systems, operating systems, firmware, cryptography, VOIP, network and hardware.

6. CNNVD – China National Vulnerability Database of Information Security⁴⁰

CNNVD is maintained by China Information Security Evaluation Center for the effective performance of the functions of vulnerability analysis and risk assessment, responsible for building operation and maintenance of the national information security vulnerabilities library, for our information security to provide basic services. Each entry includes ID (CA20181017-01: Security Notice for CA Identity Governance), description, risk rating, platform, affected products, etc.

7. Exploit Database⁴¹

The Exploit database is a CVE compliant archive of public exploits and corresponding vulnerability software, developed for use by penetration testers and vulnerability researchers. It's maintained by Offensive Security – an information security training company (<https://www.offensive-security.com/>)

8. Packet Storm⁴²

Packet Storm Security is a popular information security website offering current and historical computer security tools, exploits, and security advisories. It is operated by a group of security enthusiasts that publish new security information and offer tools for educational and testing purposes.

9. Vulners⁴³

Vulners.com is a security database containing descriptions for a large amount of software vulnerabilities in machine-readable format. Cross-references between bulletins and continuously updating of the database keeps the reader abreast of the latest information security threats.

10. Open Bug Bounty Community⁴⁴

Open Bug Bounty's coordinated vulnerability disclosure platform allows any security researcher reporting a vulnerability on any website as long as the vulnerability is discovered without any intrusive testing techniques and is submitted following responsible disclosure guidelines.

11. XSSed – Cross Site Scripting (XSS) attacks information and archive⁴⁵

The XSSed project provides information on all things related to cross-site scripting vulnerabilities and is the largest online archive of XSS vulnerable websites.

⁴⁰ <http://www.cnvd.org.cn/>

⁴¹ <https://www.exploit-db.com/>

⁴² <https://packetstormsecurity.com/>

⁴³ <https://vulners.com/>

⁴⁴ <https://www.openbugbounty.org/>

⁴⁵ <http://www.xssed.com>

12. Shodan⁴⁶

Shodan is a search engine that lets the user find specific types of computers (webcams, routers, servers, etc.) connected to the internet using a variety of filters. Some have also described it as a search engine of service banners, which are metadata that the server sends back to the client. This can be information about the server software, what options the service supports, a welcome message or anything else that the client can find out before interacting with the server.

These databases provide a good overview on identified threats. It will serve to validate our threat list generated by the template presented in the following section.

⁴⁶ <https://www.shodan.io/>

3. DEFINITION OF PROFILE TEMPLATE FOR POTENTIAL DISRUPTIONS

3.1. Aim of the threats and hazards template

The existing threat databases discussed in Section 2.4 provide a general overview on common threats and hazards for communication infrastructures. However, these sources mostly focus on providing general lists of threats without including much context information. For a thorough resilience analysis as introduced in Section 2.1, it is necessary to

- know which system components and system functions are affected in which way in order to identify the critical threat-system function combinations,
- further analyze the threats and possible protection and mitigation processes, e.g. via network simulation,
- quantify the impact of the threat in order to rank the threats and find critical combinations of threats.

In addition, the direct feedback from the RESISTO end users within the project ensures that the most important threats experienced currently are considered. Since not many examples of combined cyber-physical threats were found on the publicly available threat databases, we hope that a few examples for this class of hazards will be provided by our telecommunication partners.

The results obtained in Section 2.4 will serve as an important feedback to validate the completeness of the hazard list generated with our template.

3.2. General setup of the template: Tabular Excel document

Several options to gain input for the threats and hazards list were considered, including

- the addition of specific questions to a more general Questionnaire that is used for interviews of the telecommunication partners in Task 2.1, *Communication operators requirements refinement*
- a separate Word document with questions about the hazards to be filled by the telecommunication partners
- a tabular form (Excel sheet) to be filled by the telecommunication partners
- a Web-Interface guiding through the different aspects

The third option, an Excel sheet, was chosen as main input format for the following reasons. The tabular form enhances a structural and systematic setup. In addition to a plain text file, it allows for an easy implementation of pre-defined options to categorize the threats and to further evaluate the data by using e.g. macros. All these points could also be accomplished via a Web-Interface (e.g. Shiny application). However, the Excel format is used since it is a common format that all partner are familiar working with.

Furthermore, the first option of adding questions to the Questionnaire of Task 2.1 is used to gain information on a few general questions that do not fit in the tabular form.

3.3. Identification of information needed for the risk and resilience assessment

The threats and hazards template contains input from all three categories of physical, cyber and cyber-physical threats and hazards. This information on the hazard type belongs therefore to the class of general information, which is summarized in the following.

General classification:

- ID: a unique identifier per hazard
- Name: a short name related to the hazard cause, e.g. earthquake
- Description: further information about the hazard
- Type: a classifier to identify the event as *physical*, *cyber* or *cyber-physical*
- Cause: a classifier to identify the general source as either *man-made (accidental)*, *man-made (attack)*, *technical/system failure*, or *natural*

In order to rank the threats, the impact of the threats needs to be evaluated. The impact is assessed with respect to the occurrence frequency and duration on one hand and the estimated economic and social impact on the other hand. Also, possible direct impacts on the society are retrieved.

Threat impact:

- Frequency: a classifier to rank the occurrence of the event from *very frequent* ($\geq 10/\text{week}$) to *rare* ($\leq 1/\text{year}$)
- Duration: approximate mean time the system is affected
- Economic impact: classifier (*high*, *medium*, *low*, *no*)
- Impact on society: list observed and possible impacts on the society

The input gathered so far allows to compute a ranked threat list needed as direct input for Step 4 of the resilience management process. However, the following resilience cycle steps require a linking of the threats to system components and system functions. This is for example needed to quantify the resilience via system simulations and evaluate possible mitigation processes. Therefore, several columns are added to the table to identify the affected components and functions.

Effects on the system:

- System components affected directly
- System components affected indirectly
- System functions affected
- Subsystems affected (*radio network*, *optical network*, *satellite network*, *core network*, *data center*)
- Impact on other critical infrastructures: can be needed to simulate cascading effects or as another indicator for the threat impact

In Figure 17 a screenshot of the tabular template for the hazard list is shown. A column for comments was added to allow the end users to give specific information that does not fit any of the other categories.

Threats (hazard list)														
ID	Name	Description	Hazard type	Hazard cause	Frequency	Duration	Economic impact	Impact on society	SCs affected directly	SCs affected indirectly	SFs affected	Subsystems affected	Impact on other CIs	Comments
T1														
T2														
T3														
T4														

Figure 17: Screenshot of the tabular template for the hazard list

3.4. Context of the tabular template with respect to the resilience management approach

As mentioned in the previous section, a linkage of the threats to system components and system functions is crucial. In context of the resilience management steps, information about the system components and system functions contribute to Step 2 (System analysis) and Step 3 (System performance function identification), respectively. It was decided to add two specific tables to the Excel document to collect this information. Another aspect directly related to the threats in the implementation of improvement measures. Therefore, a fourth table was added to collect information on implemented or possible improvement measures, which contributes to the resilience management Step 8 (Selection of options for improving resilience).

In summary, the following four tables are included in the full excel template:

1. System components (→ Step 2)
2. System functions (→ Step 3)
3. Threats (→ Step 4)
4. Improvement measures (→ Step 8)

The advantage of having all four tables in one document is that the contents of the four tables can be linked to each other (via drop-down menus, see Section 4.1). The interlinkages of the tables allow for an easy computation of correlation matrices, e.g. the critical combinations of threats and system functions (→ Step 5).

More detailed descriptions on the other tables (apart from 3. Threats, which is described in this report) will be given in the deliverables of Task 2.3 (1. System components) and WP3.

4. FIRST IMPLEMENTATION AND TESTING OF THE TEMPLATE

4.1. Implementation details

The tabular template is set up as a Microsoft Excel document. Each of the four tables introduced in Section 3.3 (1. *System components (SC)*, 2. *System functions (SF)*, 3. *Threats*, 4. *Improvement measures (IM)*) is predefined on a separate sheet. The information in the tables can be filled by using provided drop-down menus or direct text input depending on the context. An extra sheet, *Definitions*, was added to pre-define the drop-down menus.

The drop-down menus defined to fill the table 3. *Threats* are:

- Hazard type: cyber, physical, cyber-physical
- Hazard cause: man-made (accidental), man-made (attack), technical/system failure, natural
- Hazard frequency: rare: $\leq 1/\text{year}$, modest: several per year, frequently: several per month, very frequently: $\geq 10/\text{week}$, never (hypothetical hazard)
- Economic impact: high, medium, low, no
- Subsystems affected: Radio Network, Optical Network, Satellite Network, Core Network, Data Center, Applications, Internal Network

Hazard Definitions

Hazard type
cyber
physical
cyber-physical

Hazard cause
man made (accidental)
man made (attack)
technical/system failure
natural

Hazard frequency
rare: ≤ 1/year
modest: several per year
frequently: several per month
very frequently: ≥ 10/week
never (hypothetical hazard)

Economic impact	Range
high	
medium	
low	
no	

Figure 18: Screenshot of the Hazard specific part of the Definitions sheet of the threats and hazards template

Each drop-down menu is defined as a separate table on the Definitions sheet. A screenshot of the tables is depicted in Figure 18. The end user can modify these tables, e.g. adding a category, when working on the document. Also the fields *SCs affected directly*, *SCs affected indirectly*, *SFs affected* are filled via drop down menus. Here, the dropdown menus are using the ID columns of the 1. *System components (SC)* and 2. *System functions (SF)* tables. The ID columns are the only fields that are filled in the template, e.g. T1, T2 in case of the 3. *Threats* table.

Some of the fields allow multiple selections from the drop-down menus (e.g. System Components affected). Since this option is not available in basic Excel documents, VBA scripts are used to implement the option.

4.2. First testing and results

First testing of the Tabular Template is based on the 7th revision of the Excel Document. It was done in a one week time frame and it involved the participation of several people with roles in

- Cyber Security
- Core Network/IP Network Architecture and Operation
- Radio and Fiber Optics Network
- Information Security, Risk Management and Compliance
- Physical Security
- Mobile Network Architecture and Operation

We gathered data from OROs Monitoring Platforms and Incident Reporting and Management Systems.

We used ORO's taxonomy for the classification and enumeration of System Functions and System Components and we input data for the most important (as of ORO's Business Requirements) 10 System Components⁴⁷ and 6 System Functions:

System Components: in OROs taxonomy, the following SCs were taken into consideration in respect to Threats that may affect it:

SC1 – Border Routers: Carrier Grade Routers, provides resources access to subscribers

SC2 – Fiber Optics Infrastructure – Nation-Wide F.O. Infrastructure

SC3 – Mobile Switching Centers (MSCs) – Primary service delivery nodes for GSM/CDMA, responsible for routing voice calls and SMS as well as other services

SC4 – Radio Infrastructure (BTS, BSC, RNC, NodeB) – Provides Radio Connectivity for legacy (2G+3G) and current (4G) services, both voice and data

SC5 – Network Security Equipment – Deployed network security infrastructure including Firewalls, IPS, WAFs

⁴⁷ In Orange Romania (ORO), satellite network are used only for DTH services. This component, together with associated components (head-end, CAS), are completely separated from the rest of the network, and there will be no interdependencies/correlations, so adding a SC on Satellite Network would not add value to the analysis. Moreover, ORO will NOT use satellite networks as backup to its communication networks, that could be affected by cyber/cyber-physical attacks. However it is not excluded that other Operators from consortium operate also a satellite network and could complete the excel with valuable information.

SC6 – Workstations and Servers – All Servers, internal and public –facing, all end-points in all of the Microsoft Security Domains

SC7 – Microsoft Security Domains – All devices, users, policies and data in one of the Microsoft Windows Security Domains

SC8 – Business Applications – Applications such as CRM, ERP, SSO/MultiAuth Tools, Databases, Internal Web Services (Intranet), Billing Apps, Monitoring Apps, VPN access

SC9 – Equipment Shelters – Build Structures that houses and provides weather and human-tampering protection to sensitive equipment

SC10 – Mobile Core Network

The System Components described above were grouped into the given Subsystems as follows, based on the destination, usage and business policies of each component

Core Network: SC1, SC3, SC5, SC10

Radio Network: SC4, SC9

Optical Network: SC2

Internal Network: SC6, SC7

Applications: SC8

Several System Components are grouped, as per functionality as a system in a System Function (SF). OROs System functions are derived from Business Requirements and Technical Requirements and are classified and labelled pertinent to their destination (i.e. – the Business Functionality it provides).

All system Functions are reliant on at least one system component although most of them depend on more than one.

SF1 – Voice Services – Provides Voice Communication Capabilities for all subscribers.

Has the following Linked System Components: SC1, SC2, SC3, SC4, SC9, SC10

SF2 – OSI Layer 1 Connectivity – Provides L1 radio and FO links between equipment

Has the following Linked System Components: SC4, SC9, SC10

SF3 – Mobile Data Services – Provides data connectivity for subscriber's mobile end-points (cell phones, modems etc.), including Internet connectivity

Has the following Linked System Components: SC1, SC2, SC3, SC4, SC5, SC10

SF4 – Fixed Data Services – Provides data connectivity for subscriber's fixed devices such as home or business terminals – routers, ONTs etc., including Internet Connectivity

Has the following linked System Components: SC1, SC2, SC3, SC4, SC5

SF5 – OSI Layer 3 Connectivity – Provides IP L3 Connectivity between devices in a network

Has the following linked System Components: SC1, SC2, SC3, SC4

SF6 – Security Functions and Policies – Information Security, Cyber and Physical Security equipment, personell and policies.

Has the following linked System Components: SC5

After inputting the above data in the Tabular Template, we inputted 4 different threats that impacted ORO in the past, as it was monitored and logged by OROs Incident Management Systems. We chose cyber and physical threats as we have not yet registered a cyber-physical incident as of now.

5. SUMMARY AND CONCLUSIONS

A living threat list is one of the main inputs for the risk and resilience management approach followed in the RESISTO project. The setup and definition of this list is the goal of Task 2.2, which status is summarized in this deliverable.

It was decided to set up an Excel template to collect the input for the threat list. This allows correlating threats to additional information, such as system components, needed to follow the main path of the project, the risk and resilience management process. The setup of the template is described in this deliverable, but the collection of input is still ongoing.

The RESISTO threat list needs to comply with current standards used in the telecom sector. Therefore a special emphasis in this deliverable was given to the review of existing threat classification schemes and available threat lists and databases. The evaluation of the compliance still needs to be assessed.

This deliverable reports the status at mid-interval of the runtime of Task 2.2. The steps described in the following subsection are planned in order to finish the task.

5.1. Next steps

As a next direct step, the output of the Excel template needs to be assessed, regarding completeness and comparability of the collected data. The following points need to be addressed:

1. First assessment of the input collected by the Excel template:
 - Is data collected from all telecommunication partners?
 - Can we combine the input from different partners into one document?
 - Did we gather input for all combinations requested, in particular: did we receive examples of cyber physical threats?
2. Compliance with existing threat lists:
 - Does the collected data represent the most common and important threats listed in existing databases, or are we missing certain kind of event classes important for the RESISTO project?
3. Evaluation of the event classification:
 - Is our classification scheme adequate for the collected events, or do we need to add e.g. sub-classes?
 - Does our classification scheme comply with current standards?

Finally, the resulting threat list will support the first analytical risk and resilience assessment by providing a threat, hazard and disruption ranking ontology.

6. REFERENCES

- [1] Häring I et al 2017 Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies *Resilience and Risk (NATO Science for Peace and Security Series C: Environmental Security)* ed I Linkov and J M Palma-Oliveira (Dordrecht: Springer Netherlands) pp 21–80
- [2] Parliamentary Office of Science and Technology 2018 *PostNote No 584*
- [3] Jouini M, Rabai L B A and Aissa A B 2014 *Procedia Computer Science* 32 489–96
- [4] Jouini M and Rabai L B A 2016 Threats Classification *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security (Advances in Information Security, Privacy, and Ethics)* ed M Gupta et al (IGI Global) pp 368–92
- [5] 2014 *DDoS Quick Guide* <https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf> (accessed 10/2018)
- [6] *Layer 1: The Physical Layer* <http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Layer-1-The-Physical-Layer.pdf>
- [7] Damon Reed 2003 *Applying the OSI Seven Layer Network Model To Information Security* <https://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309> (accessed 10/2018)
- [8] Glenn Surman 2002 *Understanding Security Using the OSI Model* <https://www.sans.org/reading-room/whitepapers/protocols/understanding-security-osi-model-377> (accessed 10/2018)
- [9] Meirer J, Mackman A, Vasireddy S, Dunner M, Escamilla R, Murukan A 2013 *Satyam Computer Services*
- [10] Swiderski F and Snyder W 2004 *Threat modeling: Includes index* (Redmond, Wash.: Microsoft Press)
- [11] ISO 1989 information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture (7492-2:1989)
- [12] *CVE: Common Vulnerabilities and Exposures* <https://cve.mitre.org/>
- [13] [Der Titel "Common Vulnerabilities and Exposures CVE" kann nicht dargestellt werden. Die Vorlage "Literaturverzeichnis - Zeitschriftenaufsatz - (Standardvorlage)" beinhaltet nur Felder, welche bei diesem Titel leer sind.]
- [14] *Common Vulnerability Scoring System SIG* <https://www.first.org/cvss/>
- [15] Joint Task Force Transformation Initiative 2012 *Guide for conducting risk assessments* (Gaithersburg, MD: National Institute of Standards and Technology)
- [16] *OWASP Risk Rating Methodology* https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (accessed 10/2018)
- [17] *AbuseIPDB* <https://www.abuseipdb.com/> (accessed 10/2018)
- [18] *VirusTotal* <https://en.wikipedia.org/wiki/VirusTotal>
- [19] 2015 *Security in Telecommunications and Information Technology*
- [20] Alhabeeb M, Almuhaideb A, Le P D and Srinivasan B 2010 - 2010 Information Security Threats Classification Pyramid 2010 *IEEE 24th International Conference on Advanced Information Networking and Applications Workshops 2010 IEEE 24th International*

Conference on Advanced Information Networking and Applications Workshops (Perth, Australia, 20.04.2010 - 23.04.2010) (IEEE) pp 208–13

- [21] International Telecommunication Union, Geneva, Switzerland 2004 ITU-T Recommendation E.408 (05/2004): Telecommunication Networks Security Requirements.
- [22] International Telecommunication Union, Geneva, Switzerland ITU-T Recommendation X.1205 (04/2008): Overview of Cybersecurity
- [23] International Telecommunication Union, Geneva, Switzerland ITU-T Recommendation X.800 (04/2008): Security Architecture for Open Systems Interconnection for CCITT Applications
- [24] Lindqvist U and Jonsson E 1997 How to systematically classify computer security intrusions *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097) Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097) (Oakland, CA, USA, 4-7 May 1997) (IEEE Comput. Soc. Press)* pp 154–63
- [25] Farahmand F, Navathe S B, Sharp G P and Enslow P H 2005 *Inf Technol Manage* 6 203–25
- [26] Kilger M 2012 *Reverse Deception Organized Cyber Threat Counter-Exploitation* (McGraw-Hill Publishing)
- [27] Humayed A, Lin J, Li F and Luo B 2017 *IEEE Internet Things J.* 4 1802–31
- [28] SANS Institute 2004 *Applying the OSI Seven Layer Network Model To Information Security* <https://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309> (accessed 10/2018)
- [29] Technologies I 2004 *Technologies, Infosys*
- [30] STIX <https://oasis-open.github.io/cti-documentation/> (accessed 10/2018)