Horizon 2020 Program (2014-2020)

Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

Cyber security cOmpeteNCe fOr Research anD InnovAtion[†]

Work package 4: *Policy and the European dimension*

Deliverable D4.1: *1st year report on cybersecurity threats*

Abstract: Deliverable D4.1 presents a first overview of the cybersecurity threat landscape, focusing on the current state-of-the-art in the domains of interest of CONCORDIA, namely, network-centric, system-centric, application-centric, data-centric, user-centric, and IoT/Device-centric security. The landscape is primarily designed for supporting awareness and information exchange initiatives, but takes into account also threat categorizations for meta-data design. The deliverable also provides an outlook of emerging threats and evolving attacks, in the form of key takeaways. All activities involved in threat reporting process described in this deliverable are considered from technological, legal, and economics perspectives.

Contractual Date of Delivery	*31 December 2019*
Actual Date of Delivery	*31 December 2019*
Deliverable Dissemination Level	*Public*
Editors	*Claudio Ardagna, Ernesto Damiani, Marco Anisetti, Marco Cremonini (UMIL)*
Contributors	*Arthur van der Wees, Dimitra Stefanatou, Prakriti Pathania (ALBV), Luciana Costa (TI), Claudio Ardagna, Ernesto Damiani, Marco Anisetti, Marco Cremonini (UMIL), Muriel Franco, Bruno Rodrigues, Geetha Parangi, Simon Miescher, Burkhard Stiller (UZH)*
Quality Assurance	*Roberta D'amico, Paolo De Lutiis (TI) Luis Barriga (Ericsson) Tatjana Welzer, Lili Nemec Zlatolas, Urška Kežmah (UM) Aiko Pras, Mattijs Jonker (UT)*

[†] This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

The CONCORDIA Consortium

UniBW/CODE	University Bundeswehr Munich / Research Institute CODE (Coordinator)	Germany	
FORTH	Foundation for Research and Technology - Hellas	Greece	
UT	University of Twente	Netherlands	
SnT	University of Luxembourg	Luxembourg	
UL	University of Lorraine	France	
UM	University of Maribor	Slovenia	
UZH	University of Zurich	Switzerland	
JACOBSUNI	Jacobs University Bremen	Germany	
UI	University of Insubria	Italy	
CUT	Cyprus University of Technology	Cyprus	
UP	University of Patras	Greece	
TUBS	Technical University of Braunschweig	Germany	
TUDA	Technical University of Darmstadt	Germany	Termination 29.02.2020
MUNI	Masaryk University	Czech Republic	
BGU	Ben-Gurion University	Israel	
OsloMET	Oslo Metropolitan University	Norway	
Imperial	Imperial College London	UK	
UMIL	University of Milan	Italy	
BADW-LRZ	Leibniz Supercomputing Centre	Germany	
EIT DIGITAL	EIT DIGITAL	Belgium	
TELENOR ASA	Telenor ASA	Norway	
AirbusCS-GE	Airbus Cybersecurity GmbH	Germany	
SECUNET	secunet Security Networks AG	Germany	
IFAG	Infineon Technologies AG	Germany	
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands	
SURFnet bv	SURFnet bv	Netherlands	
CYBER-DETECT	Cyber-Detect	France	
TID	Telefonica I+D SA	Spain	
Ruag Schweiz AG	RUAG Schweiz AG	Switzerland	
BITDEFENDER	Bitdefender SRL	Romania	
ATOS	Atos Spain S.A.	Spain	
SAG	Siemens AG	Germany	
Flowmon	Flowmon Networks AS	Czech Republic	
TÜV TRUST IT	TUV TRUST IT GmbH	Germany	
TI	Telecom Italia SPA	Italy	
Efacec Energia	EFACEC Energia	Portugal	
ARTHUR'S LEGAL	Arthur's Legal B.V.	Netherlands	

eesy-inno	eesy innovation GmbH	Germany	
DFN-CERT	DFN-CERT Services GmbH	Germany	
CAIXABANK SA	CaixaBank SA	Spain	
BMW Group	Bayerische Motoren Werke AG	Germany	Termination 29.02.2020
GSDP	Ministry of Digital Policy, Telecommunications and Media	Greece	
RISE	RISE Research Institutes of Sweden AB	Sweden	
Ericsson	Ericsson AB	Sweden	
SBA	SBA Research gemeinnutzige GmbH	Austria	
IJS	Institut Jozef Stefan	Slovenia	
UiO	University of Oslo	Norway	
ULANC	University of Lancaster	UK	
ISI	ATHINA-ISI	Greece	
UNI PASSAU	University of Passau	Germany	
RUB	Ruhr University Bochum	Germany	
CRF	Centro Ricerche Fiat	Italy	Starting 01.01.2020

Document Revisions & Quality Assurance (Original Submission)

Internal Reviewers

1. Telecom Italia (review lead)
2. Ericsson
3. University of Twente
4. University of Maribor

Revisions

Ver.	Date	By	Overview
0.1	*June 2019*	*WP4*	*Deliverable Structure and Methodology*
0.2	*July 2019*	*UZH*	*Economic Perspectives (Sec. 5 and 6.3)*
0.3	*July 2019*	*UMIL*	*Technical Perspective (first draft)*
0.4	*September 2019*	*UMIL, TI*	*Technical Perspective (advanced draft)*
0.45	*October 2019*	*ALBV*	*Input under Chapter 1 and 5, subject to further revisions.*
0.5	*October 2019*	*UMIL*	*Restructuring*
0.7	*November 2019*	*UMIL,ALBV,UZH, TI*	*New version of Sections 3, 4, 5, Conclusions*
1	*November 2019*	*UMIL*	*Final version for internal review ready*
2	*December 2019*	*UMIL*	*First round of internal review*
3	*December 2019*	*UMIL*	*Second round of internal review*

Document Revisions & Quality Assurance (Revision)

Internal Reviewers

1. Telecom Italia (review lead)
2. Ericsson
3. University of Twente
4. University of Maribor

Revisions

Ver.	Date	By	Overview
0.1	*21-02-2020*	*UMIL*	*Review report received and relevant partners informed*
0.2	*28-02-2020*	*UMIL*	*New validation section drafted, discussion about working groups added*
0.3	04-03-2020	UMIL	*List of attacks moved to appendix, first draft of the new section including most significant findings/key takeaways (technical threats)*
0.5	08-03-2020	UMIL	*Clarifications added in the first part of the deliverable, about methodology, relationship with ENISA and EUROPOL documents*
0.7	12-03-2020	ALBV, UMIL, UZH	*Pre-final draft of the new section including most significant findings/key takeaways (technical threats – Section 3.9). Integration of all contributions from partners*
0.9	16-03-2020	ALBV, UMIL, UZH	*New executive summary, pre-final version of validation section (Section 3.10), and startup of activities for next validation round (HTML version of the deliverable, dissemination of the new survey, involvement of CONCORDIA Stakeholder Group)*
1	19-03-2020	UMIL	*Deliverable released for first internal review*
1.5	27-03-2020	UMIL	*Revised version released for second internal review*
2.0	06-04-2020	UMIL	*Final version ready to be submitted*

Requests for revision

The following table provides a description of the activities made to address comments from reviewers.

Request	Actions
Make the deliverable more codified and consistent	*A restructuring of the deliverable has been implemented. Attacks have been moved to the appendix, new sections "Technical Validation" (Section 3.9) and "Key Takeaways" (Section 3.10) have been added*
Discuss the difference with ENISA and include EUROPOL documents	*The introduction of the deliverable and the introduction of chapter 3 on technical aspects of threats have been extended to clarify the role of ENISA and EUROPOL documents*
Distinguish between state of the art and novelty	*Paper restructuring aimed to distinguish the two aspects, clearly separating state-of-the-art (threat description, attacks) and novelty (asset and threat taxonomy, key findings/takeaways, validation)*
Further validation of the threat landscape	*A substantially revised section on validation (Section 3.10) has been presented and new activities started (e.g., HTML version of the deliverable, new questionnaire for CONCORDIA stakeholder group, new communication activities)*
Executive summary to be improved	*Executive summary has been extended according to reviewers' suggestion*
Add 10 pages of the most significant findings/key takeaways	*A new section on "Key Takeaways" (Section 3.9) has been added*
Details on working groups formation	*Section 3.1.3 has been extended with a description on working groups formation*
Minor comments (e.g., structure of the document, revision and quality assurance, threats/attacks, typos)	*Minor comments have been addressed in the text*

Executive Summary

Workpackage 4 (WP4) aims to outline the landscape of (i) current and emerging threats and evolving attacks, by providing an end-to-end overview of cybersecurity threats, highlighting security gaps and challenges, existing countermeasures and future research actions (technological perspective in Task 4.1), (ii) the most relevant regulations that are currently applicable as well as other proposed regulation at EU level (legal perspective in Task 4.2), and (iii) economic aspects of cybersecurity threats, especially from an economic analysis approach (economics perspective in Task 4.3). D4.1 is the first in a series, as the outcomes of the above-mentioned tasks will be discussed in three consecutive deliverables (D4.1, D4.2 and D4.3) focusing on cybersecurity threat analysis. These three deliverables, and more in general WP4, will contribute to the overall cybersecurity roadmap envisioned under T4.4.

More in detail, D4.1 presents a first overview of the cybersecurity threat landscape, focusing on the domains of interest of CONCORDIA, namely: network-centric, system-centric, application-centric, data-centric, user-centric, and IoT/device-centric security. It provides an outlook of emerging threats and evolving attacks (technological perspective), of current regulations and upcoming initiatives (legal perspective), and of some European cybersecurity economics projects, selecting common threads of relevance in the context of economics (economic perspective).

The deliverable is structured as follows: Chapter 1 introduces the methodology used in the deliverable and Chapter 2 the definition of the CONCORDIA areas of interest: network, system, device/IoT, data, application and user.

Chapters 3 (technical perspective) focuses on emerging threats and attacks providing an overview of threats in the areas of interest of CONCORDIA. To this aim, relevant documents in literature, provided by sources like ENISA, Europol, CSA, IETF, OWASP, to name but a few, have been collected and integrated to produce a snapshot of the status of cybersecurity. Integration aims to harmonize knowledge coming from different organizations to provide a “one-stop-shop” threat landscape suitable for awareness and information exchange initiatives. Threats are organized in a *cybersecurity threat map* that represents relations between identified threat groups and individual threats, in the CONCORDIA areas of interest. The map shows that while threat groups are shared and horizontal across multiple areas, differences do exist due to the peculiarities of each area. Specifically, threats in the data and user areas are mostly cross-domain due to the fact that often data represent the target of an attack, while users appear in the map both as a target and as a threat agent.
In addition to the threat landscape, Chapter 3 also provides a taxonomy of the assets targeted by attacks. Assets cover the entire spectrum of IT systems, from infrastructure and

platforms, to data and applications, including network components, middleware, devices, and people/roles.
Elaborating on the threat landscape and asset taxonomy, 21 key technical takeaways for decision makers have been identified. These takeaways show that architectural innovations driving new threats are the increasing complexity of the information and communication architectures, their distribution and stratification in multiple layers, the miniaturization of services and the pervasiveness of software in all domains. These drivers give rise to new threats and also exacerbate traditional ones like human errors and misconfigurations.
The threat landscape in this deliverable has been internally validated, by distributing a survey within the project consortium, where each project partner rated the relevance of each threat in their specific area(s) of business. From this first evaluation, it emerges that system threats are considered the ones entailing a higher risk, followed by application threats and device/IoT, network, and finally data and user threats. The reason why user threats are assessed as less risky is probably and partly due to the composition of the CONCORDIA consortium, which includes many computer-savvy organizations. In turn, data threats are often perceived as cross-domain threats and are therefore rated slightly lower than threats applied to a specific domain. The complexity of today's ICT systems is increasing concerns about system-centric security, making system threats the most relevant. Applications with IoT/device threats are also considered very relevant, showing how technology evolution is shaping the security perception. External validation has been started and will permit to validate our findings with a wider, complete and heterogeneous statistical sample.

Chapter 4 (legal perspective) captures how the European regulatory environment responds to threat escalation by discussing existing regulations and proposals for new regulations that aim to cater to such issues. The chapter first dives into the current regulatory landscape highlighting on the Cybersecurity Act, General Data Protection Regulation, Network Information Security Directive, the revised Payment Services Directive and the like. It then shifts its focus onto the proposals for new regulations such as the Regulation for a European Cybersecurity Competence Centre and the ePrivacy Regulation. The legal discussion, also, addresses some EU initiatives pertinent to Quantum Technologies and the protection of Critical Infrastructure that are in the offing and that cater to the diverse and ever-changing facets of technology. Lastly, the legal discussion provides for a mapping of the applicable regulations in relation to certain domains of interest, while pointing at existing challenges as well as forthcoming actions such as the announcement by European Commission European Commission of new legislation focusing on artificial intelligence.

Chapter 5 (economic perspective) discusses the economic impacts of cybersecurity on the different actors and stakeholders mapped by Task 4.3. Based on that, SEConomy is presented as a framework for the assessment of cybersecurity efficiency in terms of economic investments in cyber ecosystems. The framework allows to analyse security from a strictly economic point of view, considering that often critically important systems or

components have their investments in related security activities neglected. Also, a case study based on a Ransomware scenario is presented to demonstrate the operation of the framework. Additionally, challenges and complexities related to the risk assessment have been highlighted and discussed.

Activities in T4.1, T4.2, T4.3 are proceeding according to the plan and defined milestones have been reached.

Contents

1. Introduction

This section presents the policy context, an overview of the methodology used in this deliverable and, more in general, in WP4, and the structure of the document.

1.1. The Policy Context

Digitalization has been increasing exponentially the sharing of information, entailing a change from a "*need to know"* to "*need to share"* mentality. Increased sharing means that we should *protect ourselves better*.[1] "Digital technologies, especially, Artificial Intelligence (AI), have changed how we take decisions, communicate, live and work".[1] Thus, making AI essential to keep the online economy running and to ensure prosperity.

Acting upon these developments and acknowledging the growing risks resulting from the cyber activities of malicious state and non-state actors, the European Commission adopted on 13 September 2017 the Cybersecurity package on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'[2] that built on the review of 2013 Cybersecurity Strategy.[3] The Cybersecurity Package aims at three objectives: a) building EU resilience to cyber attacks, b) creating EU cyber deterrence, and c) strengthening international cooperation on cybersecurity. All actions taken so far, which are integral part of the Cybersecurity Package (including proposals of EU regulations as well as longer-term initiatives), are directed towards achieving these objectives that are of relevance for all EU Member States (MS) and beyond.

More specifically, the Cybersecurity Package is composed of proposals for new regulations, a set of recommendations, as well as the so called ''cyber diplomacy tool box''.[4] As far as these proposals are concerned, the associated developments evolved quiet rapidly within the last couple of years; the Cybersecurity Act has already become applicable in 2019, the Directive on Security of Network and information systems (NIS Directive) should have been transposed to the national legal order of all MS by May 2018, while the proposal to establish a European Cybersecurity Network and a Competence Centre to which the scope of CONCORDIA relates to is still found in the course of the trilateral process. The recommendations included under the Cybersecurity Package suggest a concrete line of actions both at national and EU level on how to increase cybersecurity of 5G networks,[5] on how to provide for a coordinated

[1] A Union that strives for more – My Agenda for Europe - POLITICAL GUIDELINES FOR THE NEXT EUROPEAN COMMISSION 2019-2024, available at: https://www.europarl.europa.eu/resources/library/media/20190716RES57231/20190716RES57231.pdf

[2] For more information, see, also: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-commission-scales-its-response-cyber-attacks

[3] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2013:0001:FIN

[4] See, also https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[5] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534

response to large-scale cybersecurity incidents and crises,[6] as well as on how to secure the process of the European elections of 2019[7] that at the time of the publication of the Cybersecurity Package were still lying ahead. Furthermore, the EU Council agreed to develop the ''cyber diplomacy toolbox'', a framework for joint EU diplomatic response to malicious cyber activities.[8]

The initiatives pertain to the proposal and adoption of regulations and soft law instruments surfaces, among other, the intent of the European Regulator to tackle the rising threats and to strengthen the trust of the individuals acting in their multiple capacities (e.g. consumers) and the trust of organizations in the online sharing of information. In a wider context, the European Regulators currently appear quite determined to put emphasis on the effectiveness of existing laws across the EU. To this end, the European Commission has published in July 2019 a Communication on Strengthening the rule of law in the Union.[9] It is relevant also for the regulatory framework applicable to cybersecurity, and provides for cooperation mechanisms and investment funds to support competent authorities at national level.

1.2. Methodology

Deliverable D4.1 is the first of three consecutive deliverables (D4.2 and D4.3 to follow) focusing on cybersecurity threat analysis. These three deliverables, and more in general WP4, will outline the landscape of (a) current and emerging threats and evolving attacks, by providing an end-to-end overview of cybersecurity threats, including current security gaps and challenges, existing countermeasures and future research actions (technological perspective in Task T4.1), (b) regulatory and most relevant applicable regulations from the EU (legal perspective in Task T4.2), and (c) economic aspects of cybersecurity, especially from an economic analysis approach (economics perspective in Task T4.3). D4.1 presents the first overview of (a) cybersecurity threats mainly focusing on the **current state-of-the-art** in the domains of interest of CONCORDIA, namely, network-centric, system-centric, application-centric, data-centric, user-centric, IoT/device-centric security. This section produces an outlook of emerging threats and attacks, as well as key technical takeaways for decision makers, (b) current regulations, especially NIS, ENISA, GDPR, PSD2, and eIDAS, and upcoming changes to those, and (c) EU cybersecurity economics projects, selected threads of relevance in the context of economics, and the economic analysis in a new approach to tackle a comprehensive methodology, as detailed in the following of this section.

[6] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, available at https://eur-lex.europa.eu/eli/reco/2017/1584/oj

[7] COMMISSION RECOMMENDATION of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf

[8] Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities("Cyber Diplomacy Toolbox"), available at: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

[9] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Further strengthening the Rule of Law within the Union State of play and possible next steps COM/2019/163 final

Technological perspective

Task T4.1 aims to produce threat reports focusing on the domains of interest of CONCORDIA (Section 2.1), as well as establishing liaisons and collaborate closely with the relevant European experts and stakeholders and contributing to the cybersecurity roadmap for Europe in Task T4.4.[10]

Activities in T4.1 will be conducted in the first three years of the project (starting M4) and are carried out along the following main phases.

- *Emerging threats and evolving attacks.* It provides an overview of the current state of the art on threats and cybersecurity in the domains of interest of CONCORDIA (Section 2.1). This phase collects relevant documents from literature, includes white papers and reports (e.g., ENISA threat landscape, Europol documents) and produces a snapshot of the status of cybersecurity, harmonizing knowledge from different activities and organizations. It evaluates the new trends in cybersecurity focusing on emerging threats and evolving attacks. This phase first provides an overview of assets, threats, and attacks, with particular reference to the use cases in WP2, shaping the current trends in cybersecurity (e.g., crypto-locker as a new type of attack for reputation downgrade, phishing attacks that target smart devices).
- *Gaps and challenges*. It manages crosscutting aspects of the threat landscape identifying threats and attacks that affect more domains of interest. It then analyses and discusses gaps and challenges with respect to identified threats and vulnerabilities
- *Countermeasures*. It provides a set of guidelines and an overview of existing countermeasures. A list of research actions will be also provided to shape the future research to the aim of mitigating identified threats and risks.

To better support the above three phases, a graph-based knowledge base on emerging threats and evolving attacks will be designed, in the context of T4.1, to enable users to follow threat landscape evolution. The knowledge base will evolve over time and link threats and attacks to actors, scenarios, and use cases. It will represent the main driver toward dissemination and validation, as well as support non-expert users in browsing the knowledge produced by the consortium on cyber threats and on the status of cyber security.

Activities in T4.1 will be fed in three different deliverables that provide an overview of technological findings as follows.

- D4.1 (this deliverable) presents a first threat analysis and state-of-the-art overview. D4.1 is the initial effort in this way and aims to build a comprehensive view of the state of the art that is currently scattered in dozens of documents. To this aim, D4.1 reviewed documents from many major players, including for instance ENISA, Europol, CSA, IETF, OWASP, and produced a coherent and consistent view of cyber security threats.
- D4.2 will refine the threat landscape and focuses on crosscutting aspects of threat analysis, as well as gaps and challenges.
- D4.3 will provide the final threat landscape and discuss future research actions and countermeasures.

[10] A first version of this cybersecurity threat analysis has been presented at CONCORDIA Open Door held in Luxembourg, October 2019

Activities in T4.1 build on the competences of partners in CONCORDIA, benefiting from their direct contributions. To this aim, we started different working groups in the domains of (i) Device/IoT-centric, (ii) network-centric, (iii) system-centric, (iv) data-centric, (v) application-centric, and (vi) user-centric security. Each of the working groups produced a section of this deliverable (Section 3.3-Section 3.8), elaborating on the current State-of-the-Art in the area that is addressed by the working group, producing an outlook of emerging threats and evolving attacks that can be expected in the future. The partners involved in the working groups provide relevant documents and material that can help in the threat analysis and reporting. More details on the working groups are reported in Section 3.1.3.
To assess the validity of our findings, we implemented an incremental validation process composed of three main steps. The first step consists of a validation survey distributed to CONCORDIA partners, each involving a respondent that was not directly involved in the deliverable activities. The second step consists of disseminating the survey to organizations part of the CONCORDIA stakeholders group, in order to retrieve a validation from outside the project. The third step considers the production of new material to make the content of this deliverable popularly available (e.g., blog posts, white papers). The validation strategy of D4.1 involved first respondents from within the consortium, which validated the analysis carried out in T4.1 providing hints and suggestions to increase the quality of findings. In this first deliverable, the interest of project partners in identified threats has been collected to validate their relevance (see Section 3.9).

Legal perspective
The legal perspective aims to examine the legal considerations pertaining to cybersecurity by looking i) at the regulatory environment and ii) into how CONCORDIA partners implement the resulting obligations, especially, those concerning compliance with Network Information Security Directive (NIS Directive) and the General Data Protection Regulation (GDPR). Taking into account what is dictated, primarily, under the applicable regulations mentioned above as well as the related practices adopted in reality, a set of recommendations are ultimately produced aiming to strengthen the effectiveness of existing rules and creating an organizational culture around cybersecurity.

Considering, also, the interdependencies of the tasks under WP4, as well as, more specifically the resulting outcomes mentioned under the technological perspective depicted above the legal perspective will capture the following:

- D4.1 (this deliverable) illustrates the regulatory environment by providing an overview of the most relevant current and proposed European regulations.
- D4.2 will address the actual practices and organizational measures in place aiming to safeguard cybersecurity at an organizational level.
- D4.3 will put forward recommendations on how to create an organizational culture on cybersecurity.

Economics perspective
The economics perspective maps actors, responsibilities, inter-dependencies, and risks involved and relevant for cybersecurity, to provide a basis for economic analysis models, ready to analyse and determine measurable factors in the area of cybersecurity mechanisms. These models can provide an accurate picture of cybersecurity economic impacts, thus helping stakeholders during the analysis of

economic impacts of threats and decision-making process toward an adequate level of cybersecurity. In addition, different stakeholders are identified by considering real-world scenarios, which include stakeholders that are more impacted by cyber attacks (e.g., governments, companies, and the financial sector). Thus, in the light of such information, a novel framework is proposed for estimating costs in complex distributed systems, which provide models for cost estimations and mapping of relations between interdependent systems and their components.
Activities conducted within the T4.3 will provide outcomes for different deliverables and activities within the CONCORDIA, which include:

- D4.1 (this deliverable) provides a discussion about the economic impacts of and introduces a phase-based framework called SEConomy for the risk assessment and analysis of cybersecurity investments. Also, based on highly specific threats and risks analysed, a case study was performed on a ransomware scenario.
- D4.2 will focus on the refinement of the SEConomy framework by providing new use cases under investigation. Also, a SEConomy-based tool will be proposed to support cybersecurity economics quantification and related risk analysis.
- D4.3 will provide the final recommendations on the economic perspectives and discuss state-of-the-art approaches proposed to support the decision-process of investments in cybersecurity as well as to minimize the loss of business affected by cyber attacks (e.g., cyber insurance).

1.3. Structure of the Document

D4.1 is structured as follows. Chapter 2 presents the CONCORDIA Environment focusing on domains of interests and stakeholders. Chapter 3 presents the technological perspective of cybersecurity threats focusing on assets, emerging threats, and key findings in the domain of interest of CONCORDIA. Chapter 4 captures the legal perspective by pointing at the most relevant current and, possibly, forthcoming regulations applicable at EU level and by drawing links with the identified research domains. Chapter 5 presents the economic perspective of cyber attacks and introduces a framework to assess costs of cybersecurity in complex distributed systems. Chapter 6 presents our concluding remarks and an outlook on future work.

2. CONCORDIA Environment

This section presents the CONCORDIA environment and summarizes the domains of interest that are the target of the study in this deliverable and stakeholders benefiting from it. Domains and stakeholders represent the common basis linking the work in this deliverable to the effort done in WP1 and WP2, on one side, and WP4 on the other side.

2.1. Domains of Interest

Cybersecurity threats are analysed in this deliverable from different perspectives, called domains, to the aim of identifying emerging threats and attacks, as well as setting the scene for the associated implications from a regulatory and economic standpoint in relation to the domains of interest of CONCORDIA. These domains, taken from the research domains of WP1 (Figure 1), are: (i) network-centric, (ii) system/software-centric, (iii) application-centric, (iv) data-centric, (v) user-centric, (vi) IoT/device centric security. However, given their importance, application- and data-centric security are treated separately in this deliverable. We also note that device-centric security is extended to cover IoT security in order to provide a wider and more coherent view that not only includes threats to devices but also to the corresponding platforms/infrastructures. We finally note that, being the security of software horizontal to all domains, domain system/software mainly concentrates on system-centric security.

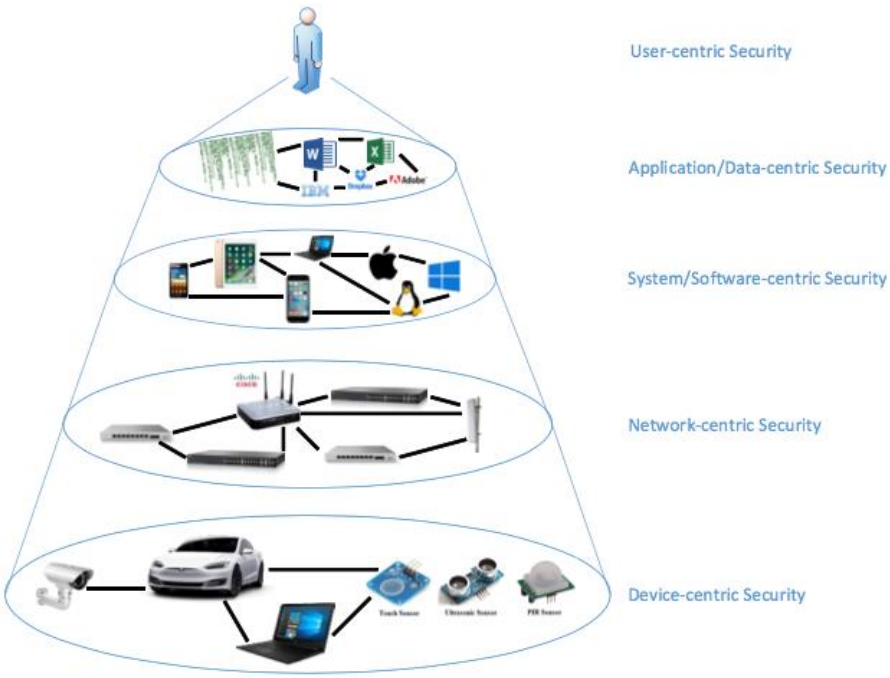


Figure 1 – Domains of interest

More in detail, network-centric security refers to the transportation of data as well as to the networking and the security issues associated with it. Topics range from DDoS protection, Software-Defined Networking (SDN), ad hoc networks to encrypted traffic analysis and cellular network. System-centric security centres around cloud and virtualized environments, while IoT/Device-centric security centres around modern

systems such as Internet of Things (IoT)/edge and corresponding devices, both targeting topics such as middleware, secure OS, and security by design. Malware analysis, systems security validation, detection of 0-day attacks, and service dependencies are specifically addressed. Data-centric security addresses issues concerned with management, analysis, protection, and visualization of data at all layers of a given system/environment, focusing on modern Big Data environments. Application-centric security addresses issues related to the security of applications, like modern services and their management. User-centric security addresses issues like privacy, social networks, fake news and identity management. The above domains apply to any environments ranging from traditional distributed IT systems, to devices that produce raw data, such as embedded systems, sensors, IoT devices, drones, and the associated security issues (e.g., IoT security), via service-based systems, such as, service-oriented architecture, cloud, and microservices.

2.2. Mapping of Stakeholders

The vision of CONCORDIA is to build strong cooperation between all its stakeholders and foster the development of IT products and solutions along the whole supply chain. As CONCORDIA aims to develop the solutions that are important for Europe, hence it needs good cooperation involving multiple and diverse stakeholders. It also aims to strengthen relations among its stakeholders and build a strong network among them. Figure 2 shows the first step in the identification of CONCORDIA stakeholders and the interaction between them. Several key stakeholders have been identified with which CONCORDIA will establish and foster liaisons. Stakeholders that could be the member of the network are European entities, Research entities, Companies, National and International entities [1]. The list of identified stakeholders are not exhaustive and additional stakeholders can be identified.

The possible European entities can be the European Union Agency for Network and Information Security (ENISA), the Computer Emergency Response Team for the EU (European Union) Institutions, bodies and agencies (CERT-EU), European Strategic Intelligence and Security Center (ESISC), and European Cyber Security Organization (ECSO). These entities are the centre of expertise for cybersecurity in Europe. They actively contribute to information and network security within the union. They deliver advice, solutions, develop and implement policy and respond to information security incidents and threats. They also help to discover breaches or anomalous activity and target to catch adversaries early in the attack lifecycle. They provide awareness of the threat landscape and helps companies and national entities to understand their adversaries. This could save the companies and national entities from financial damages. They also usher strict data security laws on them by providing standards. These standards provide clear direction to the companies and national entities in the configuration management process and ensure compliance with frameworks and improve the security of the organization.

The stakeholders in Figure 2 also include national entities and national agencies. Few examples of the national agency are Global Cyber Security Center (GCSEC), National Cyber security Agency of France, and National Cyber Security Centre of Lithuania. National entities include Military, Navy, Healthcare sector, and Airlines. National agencies are responsible to develop and distribute awareness and knowledge on cybersecurity. They provide support to the national entities and companies on policies, regulations, and standards. In some cases, they manage Internet operations

of national entities and propose cybersecurity plans and investigate cybersecurity attacks.

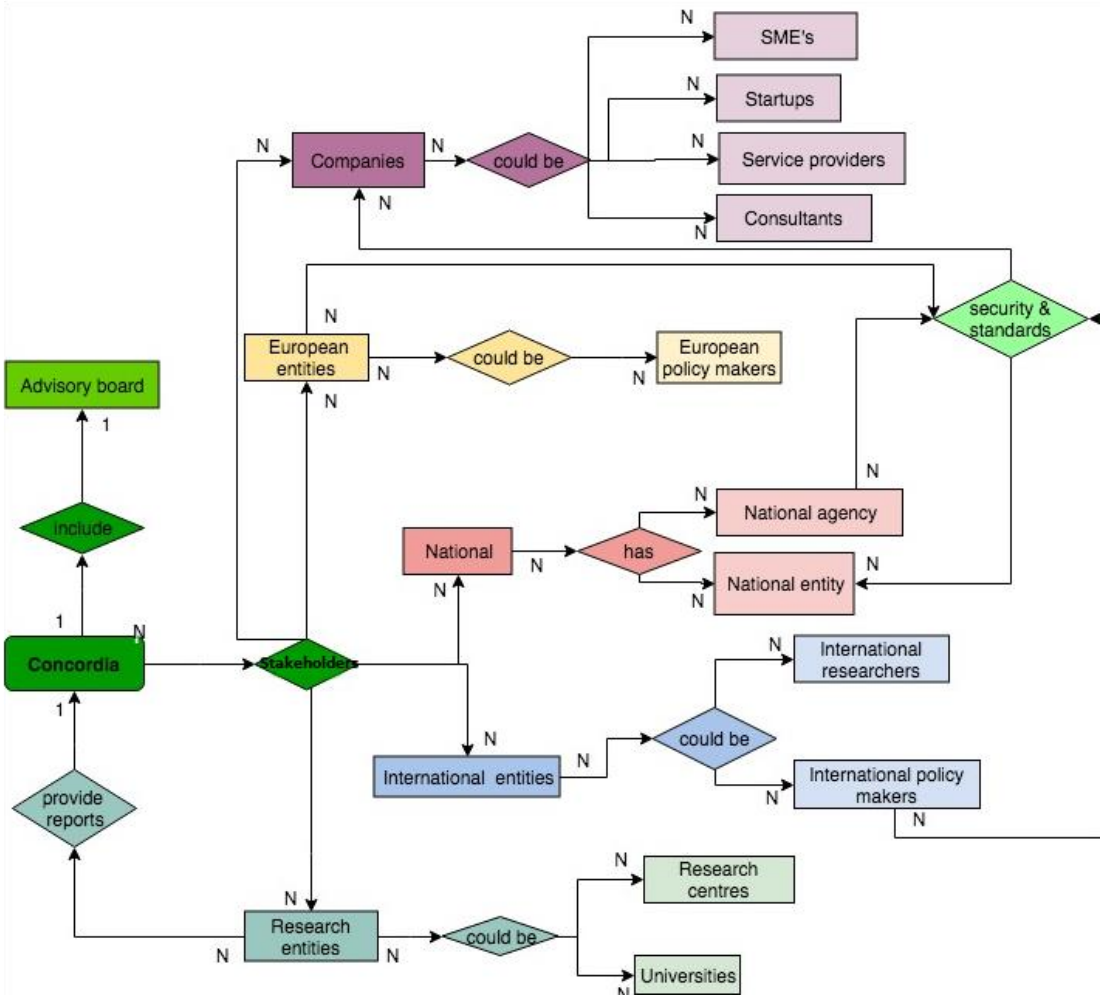


Figure 2 – Mapping CONCORDIA stakeholders

The possible sector of companies that can be the partner of CONCORDIA are startup companies, service providers, consultants, SME's, and large multinational company. Companies depend on the research entities for their research potential and talent to overcome cybersecurity challenges. Collaboration between companies and research entities help companies to increase security awareness but also help the research entities to understand concrete industry needs and requirements. Companies contribute their expertise and allow research entities to access their knowledge resources [2, 3].

Research entities can be the Universities and Research centers. Center for strategic and international studies (CSIS), National Counterintelligence and Security Center (NCSC) can be the possible stakeholders. Research entities contribute and participate in the research and development process and provide reports to the CONCORDIA partners about existing solutions and increase the security awareness among them. They can also propose several pilots in the companies and national entities. They develop innovative solutions to overcome cybersecurity challenges faced by the companies and national entities. Research entities also provide inputs to CONCORDIA

and emphasize the cybersecurity pain points and help CONCORDIA to fight against cybersecurity problems.

International entities such as researchers and policy makers can also be the partners of CONCORDIA. Examples of International policy makers are Women in International Security, the Payment Card Industry Security Standards Council, and the International Organization of Securities Commissions. European CERTs (Computer Emergency Response Team) in collaboration with international CERTs can build threat intelligence for Europe. The collaboration with international researchers will enable greater opportunities to witness the most recent trends and innovations worldwide in an area of cybersecurity.

CONCORDIA also includes an Advisory Board which comprises of leaders from the companies, national entities, standardization, policy, and politics. They provide strategic advice and helps in connecting with possible clients and users. They provide advice on the current and emerging technologies and ensure that the project stays true to its goals and objectives.

3. Cybersecurity Threat Report

We first clarify the standards, terminology, and process used in the discussion of the technical aspects of cybersecurity threats (Section 3.1). We then present a threat map summarizing all identified threats (Section 3.2). We further present the cybersecurity threat report providing a section for each domain of interest (Sections 3.3, 3.4, 3.5, 3.6, 3.7, 3.8). We present our findings (Section 3.9) and finally a first deliverable validation (Section 3.10).

3.1. Standards, Terminology, Process

We clarify the terminology that is used along this section, then discuss the standards at the basis of the methodology described in Section 1.2, and finally briefly analyse our process.

3.1.1. Standards

The cybersecurity threat reporting in this deliverable (technological perspective in Section 1.2) follows well-known standards in the field from the main standardization bodies such as ISO and NIST. Our methodology to identify threats follows the definition given in the last version of ISO 27001 presented in 2013.[11] We consider a classification based on the identification of assets and threats. The newer revision of ISO 27001 presented in 2013 allows identifying risks using any methodology. In addition, in the process of identifying emerging threats and attacks, our work will base on two additional ISO standards that have strong connection with ISO/IEC 27001:2013: ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls and ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management.

To improve the scope of our approach, we also consider relevant NIST standards such as: *i)* NIST SP 800-53 Rev. 4 NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, *ii)* NIST SPECIAL PUBLICATION 1800-5 IT Asset Management, enhancing visibility for security analysts, which leads to better asset utilization and security.

3.1.2. Terminology

Threat reporting is based on three pillars as follows.[11] [12]

- **Asset:** something that has value to the organization. An asset extends beyond physical goods or hardware, and includes software, information, people, and reputation.
- **Threat**: the potential cause of an incident that may result in a breach of information security or compromise business operations.
- **Vulnerability**: a weakness of a control or asset. Another similar but more complete definition by NIST is: vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.[13]

For instance, a digital repository can be considered as an asset. Examples of relevant threats and vulnerabilities are then listed as follows.

[11] ISO/IEC 27001 Edition 2013 https://www.iso.org/standard/54534.html
[12] ISO/IEC 27001 Edition 2005 https://www.iso.org/standard/42103.html
[13] Guide for Conducting Risk Assessments, NIST SP 800-30, September 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

- EXAMPLE 1. The threat can be a disk failure. A related vulnerability is that there is no backup of the repository (availability is not guaranteed).
- EXAMPLE 2. The threat can be a virus propagation and the related vulnerability is that the anti-virus program is not blocking it, that is, virus patterns are out-of-date or incomplete (issues of confidentiality, integrity, and availability).
- EXAMPLE 3. The threat can be an unauthorised access. The vulnerability is the access control scheme that is not working (loss in confidentiality, integrity, and availability).

As another example, an asset can be a human resource, for example a system administrator.

- EXAMPLE 4. The threat can be the unavailability of this person and the related vulnerability is that there is no replacement for this position (potential loss of availability).
- EXAMPLE 5. The threat can consist of configuration errors made by the system administrator. The vulnerability is the malfunctioning of a system or the diminished security protection (issues in confidentiality, integrity. and availability)

In the remainder of this section, for each of the 6 domains of interest, we analyse assets and threats, reporting on some recent attacks. For sake of readability, we will not discuss specific vulnerabilities at the basis of identified attacks. Also, to make our discussion consistent, where possible, we will refer to the threat group/threat nomenclature proposed by the ENISA threat taxonomy.[14]

3.1.3. Process

Recalling the discussion in Section 1.2, activities in T4.1 built on the competences of partners in CONCORDIA, benefiting from their direct contributions. To better manage threat reporting activities, we formed different working groups in the domains of (i) Device/IoT-centric, (ii) network-centric, (iii) system-centric, (iv) data-centric, (v) application-centric, and (vi) user-centric security. Each working group was coordinated by a project partner responsible for collecting relevant material and contributions from the consortium. The collected material was then analysed and prepared for the threat reporting in D4.1. Each working group produced a section part of this deliverable (Section 3.3-Section 3.8), elaborating on the current State-of-the-Art in the area addressed by the working group, producing an outlook of emerging threats and evolving attacks that can be expected in the future, as well as contributing to the key findings in Section 3.9, as follows.

- **Working Group 1:** "Device/IoT-centric security"
  Workgroup Chair: UMIL
  Reporting Section: Section 3.3
- **Working Group 2:** "Network-centric security"
  Workgroup Chair: TI
  Reporting Section: Section 3.4
- **Working Group 3:** "System-centric security"
  Workgroup Chair: UMIL
  Reporting Section: Section 3.5

[14] See https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/at_download/file

- **Working Group 4:** "Data-centric security"
  Workgroup Chair: UMIL
  Reporting Section: Section 3.6
- **Working Group 5:** "Application-centric security"
  Workgroup Chair: ATOS
  Reporting Section: Section 3.7
- **Working Group 6:** "User-centric security"
  Workgroup Chair: UMIL
  Reporting Section: Section 3.8

The overall methodology, implemented by all working groups, goes through a three-step process as follows. The first step is about the identification and collection of relevant assets in all domains of interest. According to identified asset, the second step identifies the related threat groups and detail specific threats. For each threat, the third step provides some examples of recent attacks. It is important to note that the same attack can be mapped on multiple threats in multiple domains. Where possible, we will map the attack with the most representative threat(s) only. The analysis will focus on identifying cybersecurity trends and on identifying emerging threats and evolving attacks guiding cybersecurity research of the next decade. The analysis has been based on an extensive review of actual threat incidents and attacks presented in articles, technical blogs, conference papers, as well as online surveys for gathering supplemental information. We note that our review and, in particular, threat group and threat identification start from the ENISA threat taxonomy and refine it, as deemed necessary, with the last cybersecurity evolutions.[14] Also, we reviewed documents from main organizations, including for instance CSA, IETF, OWASP, Europol and its Internet Organised Crime Threat Assessment (iOCTA).

A central question of past research on threat reporting and threat landscape is how to rank vulnerabilities; in other words, how to assess how severe the security problems affecting software/system configurations in the domains of interest are. In this deliverable, the problem of ranking vulnerabilities is out of scope, since the main goal of T4.1 (and corresponding deliverables D4.1, D4.2, and D4.3) is on identifying future and emerging threats and emerging attacks in the six domains of interest: (i) device/IoT-centric, (ii) network-centric, (iii) system-centric, (iv) data-centric, (v) application-centric, (v) user-centric security. In particular, T4.1 will evaluate the *new trends in cybersecurity* including emerging threats and evolving attacks and build a *shared knowledge on emerging threats and evolving attacks*, which possibly evolves over time.

3.2. Cybersecurity Threat Map

Drawing upon the domains of interest identified under Task 4.1, this section attempts to provide a cybersecurity threat map that summarizes the mapping between identified threat groups, threats, and the domains network, system, device/IoT, data, application, user, which will be then detailed in the following sections. Table 1 provides such a mapping and specifies the threat numbering format, driving the discussion in the remaining of Chapter 3. As an example, threat T2 "Denial of Service" in threat group TG4 "Nefarious Activity/Abuse" of domain D1 "Device/IoT" is referenced in the text as T1.4.2.

Table 1 – Cybersecurity threat map. Numbers in parenthesis are used for threat numbering in the form T(D).(TG).(T).

Domain (D)	Threat Group (TG)	Threats (T)
Device/IoT (1)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (2)
	Intentional Physical Damage (3)	Device modification (1) Extraction of private information (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software/activity (3) Misuse of assurance tools (4) Failures of business process (5) Code execution and injection (unsecure APIs) (6)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1)
Network (2)	Unintentional damage / loss of information or IT assets (1)	Erroneous use or administration of devices and systems (1)
	Interception and unauthorised acquisition (2)	Signaling traffic interception (1) Data session hijacking (2) Traffic eavesdropping (3) Traffic redirection (4)
	Nefarious activity/abuse (3)	Exploitation of software bugs (1) Manipulation of hardware and firmware (2) Malicious code/software/activity (3) Remote activities (execution) (4) Malicious code - Signaling amplification attacks (5)
	Organisational (failure malfunction) (4)	Failures of devices or systems (1) Supply chain (2) Software bug (3)
System (3)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2)
	Poisoning (3)	Configuration poisoning (1) Business process poisoning (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software/activity (3) Generation and use of rogue certificates (4) Misuse of assurance tools (5) Failures of business process (6) Code execution and injection (unsecure APIs) (7)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1) Malicious Insider (2)
Data (4)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)

	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2)
	Poisoning (3)	Data poisoning (1) Model poisoning (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software /activity (3) Generation and use of rogue certificates (4) Misuse of assurance tools (5) Failures of business process (6) Code execution and injection (unsecure APIs) (7)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1) Malicious insider (2)
Application (5)	Unintentional damage (1)	Security Misconfiguration (1)
	Interception and unauthorised acquisition (2)	Interception of information (1) Sensitive data exposure (2)
	Nefarious activity/abuse (3)	Broken authentication and access control (1) Denial of service (2) Code execution and injection (unsecure APIs) (3) Insufficient logging and monitoring (4) Untrusted composition (5)
	Legal (4)	Violation of laws or regulations (1)
	Organisational threats (5)	Malicious Insider (2)
User (6)	Human Errors (1)	Mishandling of physical assets (1) Misconfiguration of systems (2) Loss of CIA[15] on data assets (3) Legal, reputational, and financial cost (4)
	Privacy breaches (2)	Profiling and discriminatory practices (1) Illegal acquisition of information (2)
	Cybercrime (3)	Organized criminal groups' activity (1) State-sponsored organizations' activity (2) Malicious employees or partners' activity (3)
	Media amplification effects (4)	Misinformation/disinformation campaigns (1) Smearing campaigns/market manipulation (2) Social responsibility/ethics-related incidents (3)
	Organisational threats (5)	Skill shortage/undefined cybersecurity curricula (1) Business misalignment/shift of priorities (2)

From the above table, it emerges that threats groups are horizontal to the different domains. Some differences do nevertheless exist due to the peculiarities of each area. Also, threats in the area of data and users are cross domain due to the fact that often data represent the target of an attack, while users are often seen both as a target and as a threat agent.

3.3. Device/IoT-Centric Security

This section describes an overview of assets and threats in Domain 1 on Device/IoT-centric security. It concentrates on the recent evolution of the domain including an overview of assets and threats that focus on smart devices and IoT/edge systems. Major sources of information for this study are "ENISA Baseline for Security

[15] Confidentiality, Integrity, Availability (CIA)

Recommendations for IoT",[16] "IETF RFC 8576 on Internet of Things (IoT) Security: State of the Art and Challenges",[17] and "ITU-T Y.4806".[18] Details on attacks linked to the identified threats are reported for interested readers in Appendix A.1.

3.3.1. Context and Architecture

Internet of Things (IoT) can be defined as "*the networked interconnection of everyday objects, equipped with ubiquitous intelligence*" [3]. The exponential growth of connected devices (from minuscule sensors to bigger machines), which according to Intel[19] are expected to reach 200 billion by 2020, are revolutionizing current IT systems. Smart transportation, sustainable mobility, smart cities, e-health, smart vehicles, UAVs, and many more are just some examples of domains where IoT, edge computing and smart devices are changing the environment. The existence of billions of resource-constrained devices connected to the Internet introduces fundamental risks that can threaten users' life and personal sphere. Current environments are so pervasive and ubiquitous that users just become another component of the system.
IoT has specific peculiarities. It is a large-scale distributed architecture having more objects than the current internet. These objects are heterogeneous in functionalities and platforms/communication protocols. They cope with different legislations/regulations, but can be deployed in operation in places where the legislation is different. The devices themselves may need to show high automation, since they can be unsupervised, with limited user interface and deployed in a potential hostile environment. Another important aspect is that they could be fully integrated in the physical world. Each IoT device is resource constrained due to a number of reasons including costs and classified by IETF in terms of capabilities in three different classes as follows.[20]

- Class 0: pre-configured devices having the minimum management functionalities and capable to communicate just using gateways.
- Class 1: resource-constrained devices. They can communicate via internet but not with the full capabilities of HTTP and TLS.
- Class 2: devices capable to fully support most of the protocols but still designed for lightweight protocols.

Classes 0 and 1 are the most critical in terms of security leakages. Class 2 is critical as well and can be considered as the preferred target of an attack for their more advanced computation capabilities.

In this context, edge can be considered as an evolution of IoT to cope with the need of aggregating and processing big data. According to Gartner[21] 91% of today's data are

[16] Baseline Security Recommendations for IoT, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[17] RFC 8576 - Internet of Things (IoT) Security: State of the Art and Challenges, https://tools.ietf.org/html/rfc8576
[18] Y.4806 - Security capabilities supporting safety of the Internet of things, https://www.itu.int/rec/T-REC-Y.4806/en
[19] A guide to Internet of Things Infographic https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
[20] Terminology for Constrained-Node Networks https://tools.ietf.org/html/rfc7228
[21] What Edge Computing Means for Infrastructure and Operations Leaders https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/

created and processed in centralized data centers. By 2022, about 75% of all data will need analysis and actions at the edge.

More than other domains described in this deliverable, Device/IoT systems will benefit from a security-by-design approach due to their manufactured nature.[22] Currently less than 4%[23] of devices are adopting this approach mainly for budget constraints, facing the following hurdles.

- **Vulnerable by definition hurdle.** Differently from the portion of the IoT ecosystem that resides on the Cloud, devices are vulnerable by definition due to the fact that they operate on the open Internet, with constrained resources in an unsupervised environment prone to physical access. The reason of having constrained resources is that they are in most of the cases low-cost devices, and are not designed to support security features, similar to more traditional functional-oriented devices to be used in a business process where costs have to be confined as much as possible.
- **Long lifecycle and obsolescence hurdle.** IoT devices are designed to be on market as fast as possible with small budget and small profit margin. Their lifecycle is however much longer than what is planned by the procedures. In general, the pressure of the time to market on IoT devices is much higher than in other sectors and this causes a development (programming mainly) process more focused on functionality and usability and less on security. In addition, the attacks on these devices rarely affect the manufacturers (e.g., the botnet); therefore, from the manufacturer point of view it seems complex to evaluate the risk and the investment in security.[24] This led to a plethora of obsolete devices that are still connected to the network and in many cases unmanaged or even abandoned. Such devices, when collectively exploited as botnets can cause huge damage.
- **Regulatory fragmentation, liability hurdle and lack of awareness**. As it will be further discussed below, the European Regulator has taken actions with respect to the regulation of cybersecurity in a homogeneous manner across Member States. The Cybersecurity Act, for example, constitutes a clear example of this regulatory aim. There are, of course, other recently enforced regulations (e.g. NIS Directive) that do not guarantee the same degree of homogeneity, when it comes to the applicable regulatory frameworks and their enforcement.[25] The latter combined with the absence of regulation addressing all aspects of IoT in an up-to-date manner, hinders both the identification of commonly accepted requirements for manufacturers, as well as the setting of clear expectations from customers regarding cybersecurity. In this scenario, the distribution of liabilities become problematic in case of a security incident,

[22] Secure by Design: Improving the cyber security of consumer Internet of Things. Policy report UK Government, March 2018.
[23] IoT Security from Design to Lifecycle Management, An Embedded Perspective; ABI Research, 2018.
[24] The economics of the security of consumer-grade IoT products and services, Internet Society / Plum Consulting, April 2019.
[25] Note that this is clearly reflected in the recent Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, available at: https://ec.europa.eu/digital-single-market/en/news/report-assessing-consistency-approaches-identification-operators-essential-services

especially, when IoT is part of a large and complex business process as those occurring within the context of Industry 4.0 or when a single component is shared by several parties holding different roles in the supply chain.[26] In addition, the fragmented and slow adoption of standards and regulations, as well as the continuous emergence of novel technologies, make even more challenging for the law to effectively address technological developments in a timely manner. Finally, there is lack of awareness at societal level. End users are not well aware of the risks incurred both for themselves and the others and, therefore, cybersecurity is not widely embraced as an essential requirement in the market.

- **Safety hurdle.** IoT and specific domains of application like UAVs and autonomous cars are affected by safety concerns, for instance, because of the presence of actuators acting on the physical world. Therefore, security threats can become safety threats (e.g., cybersecurity attacks on connected vehicles can cause accidents[27]).
- **Complex and heterogeneous ecosystem hurdle.** IoT is a rich, diverse and wide ecosystem involving entities such as devices, communications, interface, and people. It has a very large attack surface where threats and risks are manifold and evolve rapidly. In addition, the surface depends on the application domain where the things are deployed (i.e., domestic unprotected or enterprise environment). Considering their impact on citizens' health, safety and privacy concerns in IoT are extremely wide, including very critical infrastructures, but also legacy ones enhanced with devices (e.g., industry 4.0). In this complex ecosystem, the integration of security is a very challenging task, due to the presence of possibly contradicting requirements like systems based on different authentication solutions that must cooperate. This problem is exacerbated by the current lack of specific expertise in IoT cybersecurity, which makes simple processes, such as the application of security updates, extremely difficult in practice.

In the remainder of this section, we concentrate on the "sensor and device" nature of Edge and IoT computing, which is considered by ENISA as the most critical part of the IoT environment,[16] and leave the discussion on the "cloud" backend to System-centric and Data-centric security in Section 3.5 and Section 3.6, respectively. We note that we consider UAVs and smart cars[27] as devices due to their increasing development and their impact on safety, even if they are more IoT applications than components.
On the other hand, mobile devices such as smart phones require a separate discussion. This type of devices is often excluded from the IoT ecosystem since they are primarily intended for human interaction and therefore not included into any of the mostly common IoT definitions.[28] [29] On the other hand, they can play a significant role in IoT, since they are sensors equipped and often act as gateways for body sensors (being part of the edge computation). Therefore, we follow the ENISA definition of the IoT architecture and considered them as a third-party device in the IoT ecosystem.[16]

[26] See, also, CREATE-IoT Deliverable 05.03
IoT Data Value Chain Model, available at: https://european-iot-pilots.eu/wp-content/uploads/2017/10/D05_03_WP05_H2020_CREATE-IoT_Final.pdf
[27] Cyber Security and Resilience of smart cars https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
[28] Define IoT https://iot.ieee.org/definition.html
[29] The Internet of Things https://www.ietf.org/topics/iot/

3.3.2. Assets

According to ITU-T U.4806 document of 2017 on Security capabilities supporting safety of the Internet of things,[18] IoT security and IT security share the same fundamental principles. However, given the unique nature of the IoT ecosystem it is not possible to apply the same methodologies and principles of the traditional IT security. In fact, many of security measures (e.g., TLS/SSL) cannot be adopted due to the resource restrictions. IoT devices can run for a very long period of time without supervision and in a hostile environment susceptible to hacking. Patching is almost impossible due to restrictions in terms of interfaces and they can be difficult to be detected to force upgrade. At the same time, powerful IoT devices, like cars, could afford over-the-air (OTA) updates but still many car manufacturers do not use it. IoT devices have a greater impact in case of attacks since they are embedded into physical systems and can cause physical damage. In addition, traditional security is primarily focused on fortify the perimeter. With the advent of Cloud, mobile devices, and IoT, this perimeter is becoming more articulated and almost impossible to be defined and protected in a traditional way.[30] This requires to re-think current security practices and guidelines.

In addition to the ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,[16] a major source of information for this study is the work jointly commissioned by the Cyber Security Agency of Singapore and the Ministry of Economic Affairs and Climate Policy of the Netherlands and their 2019 IoT security landscape white paper.[31] Other sources of information are the OWASP Principles of IoT Security[32] and the IETF Internet of Things (IoT) Security: State of the Art and Challenges[33] and CSA IoT Security Controls Framework[34] and the CSA Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products.[35]

Assets can be categorized in different classes as follows:

- Data – IoT and devices are the main source of data but, they do not have data as main assets since they stream data almost in real time. However, in case of edge or while in transit (e.g., passing to gateways), data become an important asset for this domain also considering the OWASP principle of IoT security related to "Data aggregation",[32] which can reveal sensitive patterns.
- Infrastructure – It comprises communication protocols (e.g. MQTT, ZigBee), communication devices like routers, gateway, but also power supply units and batteries.
- Devices – It is the essence of this category and refers to sensors, actuators, as well as firmware driving them. It includes also devices that serve the purposes of aggregating data (e.g., in edge systems) and managing sensors/actuators, as well as embedded systems in general.

[30] https://www.networkworld.com/article/3223952/internet-of-things/5-reasons-why-device-makers-cannot-secure-the-iot-platform.html
[31] TNO report http://publications.tno.nl/publication/34634724/5RwNLq/TNO-2019-iot.pdf
[32] Principles of IoT Security https://www.owasp.org/index.php/Principles_of_IoT_Security
[33] Internet of Things (IoT) Security: State of the Art and Challenges https://datatracker.ietf.org/doc/rfc8576/
[34] CSA IoT Security Controls Framework https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/
[35] Future-proofing the Connected World:13 Steps to Developing Secure IoT Products https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

- Platform and backend – It refers to IoT backend in cloud. It is part of IoT since it is fundamental for the operation and has a great impact on security. For clarity, it is discussed in detail in Domain 3 "System-centric security" (Section 3.5).
- Decision making – It regards the transformation of the acquired data into actions on the actuators or models. It can be computed on the edge. Similarly, to the platform and backend, we refer to Domain 4 "Data-centric security" for more details (Section 3.6).
- Management – It includes, when available, device management services like device usage, battery status, and the like, as well as update management, network setup and statistics, and applications and diagnostics.
- Security and privacy techniques – It refers to all security techniques that are the target for an attacker. These represent the interesting components that would result in unauthorised data disclosure and leakage, if compromised. In IoT environment they can be spread from device interface to gateways and Cloud backend.
- Roles - Introduced by the NIST Big Data Public Working Group, this category includes human resources and related assets.

Each asset class can be further refined in different sub-categories as presented in the following tables.[16]

Table 2 – Assets: Data

Class	Category	Description
Data	In transit	Assets focusing on encapsulating data while they need to be sent to another component/layer.
	At rest	It is mostly associated with the data that temporarily or permanently reside on the edge, gateways or sensors that streams on a batch basis.
	Aggregated	Mostly impacting at the cloud backend level when the aggregation takes place, but also impacting in case a number of devices of the same network/application are compromised. It is mostly associated with the data that temporarily or permanently reside on the edge, gateways or sensors that streams on a batch basis.
	Credentials	Files including important credentials like certificates tokens.

Table 3 – Assets: Infrastructure

Class	Category	Description
Infrastructure	Network/ protocols	Networking peculiarities and the corresponding protocols, for instance, the ones specialized for IoT like MQTT, and Zigbee.

	Routers/gateways	Networking components used to provide connectivity via packet forwarding and bridging between different protocols.
	Power supply	External (and wired) or internal via batteries

Table 4 – Assets: Devices

Class	Category	Description
Devices	Hardware	It includes the physical part of IoT devices like the physical memory, sensors, and physical interfaces.
	Edge nodes/ embedded systems	Computing services on the devices or at the edge, offering interfaces, aggregations, management services. It includes mobile devices.
	Firmware/software	Software installed on the device including low-level software for operating system-level functionalities.
	Sensors/actuators	The subsystems to detect and measure events, and to take a decision based on previously processed information.

Table 5 – Assets: Platform and backend

Class	Category	Description
Platform and backend	Device Web interface/services	It includes APIs and services. It is a major target for a number of impacting attacks.
	Cloud-level interface/services	See Section 3.5.2.

Table 6 – Assets: Decision making

Class	Category	Description
Decision making	Device/edge processing	It refers to data aggregation, an important trend in IoT and Edge open to a number of issues related to the possibility of revealing sensitive patterns.
	Cloud/Big Data processing	See Section 3.6.2.

Table 7 – Assets: Management

Class	Category	Description
Management	Device and network	Management subsystems of IoT devices (e.g., updates). It also considers configurations at any level including networking.
	Device status	Status level monitoring including batteries, usage patterns, and the like.

Table 8 – Assets: Security mechanisms

Class	Category	Description
Security mechanisms	Device	It includes access controls and other security mechanisms adopted by the device itself. It also includes physical SIM cards that can contains important security related data (see Data Asset above).
	Infrastructure	It includes security mechanisms that are in place at the level of infrastructures, like firewalling, channel encryption at gateway level.
	Platform	It includes the security mechanisms in place at the Cloud level of the IoT. See Section 3.5.

We note that the class Security Mechanisms includes sub-categories that covers most of the other assets. This is due to the fact that security controls in IoT can be distributed in different assets and inherit assets peculiarities and vulnerabilities.

3.3.3. Threats

We now discuss the threats that can be mapped to the Device/IoT asset taxonomy presented in the previous chapter. Details on attacks exploiting vulnerabilities linked to the identified threats are reported in Appendix A.1. In general, the IoT scenario revolutionizes the concept of security, which becomes even more critical than before. Security protection must consider millions of devices that are under control of external entities, freshness and integrity of data that are produced by these devices, and heterogeneous environments and contexts that co-exist in the same IoT environment [4]. Trend Micro, a cybersecurity solutions provider, stated that the IoT has become a primary target for cybercriminals. The SonicWall 2019 report shows that IoT malware increased 55% and threats related to encryption spiked 76% compared to 2018.[36] This trend leads to an increment in budget for security in IoT. According to Gartner,[37] the IoT security budget will reach $3.1 billion in 2021.

Concerning attack vectors in IoT, according to F-Secure Attack Landscape H1 2019, the Telnet protocol is the one mostly used among the TCP-based ones while the UPnP is the top exploit among the UDP ones.[38]

Given the peculiarity of IoT devices, which are in many cases outdated embedded systems, F-Secure estimated half a billion IoT devices vulnerable to 10-year-old vulnerabilities.[39]

[36] SonicWall Mid-Year update report https://www.sonicwall.com/resources/white-papers/mid-year-update-2018-sonicwall-cyber-threat-report/

[37] Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018 https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018

[38] ATTACK LANDSCAPE H1 2019 https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf

[39] F-Secure IoT threat landscape - Old hacks, new devices, https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/04/01094545/IoT-Threat-Landscape.pdf

Even considering the heterogeneous nature of the assets belonging to the Device/IoT domain, the IETF definition of threat, namely, "*a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm*", is general enough to cover with all the IoT threats. IoT has a specific peculiarity: the strong link between security leakages and safety. ITU-T in its report Y.4806 underlines this link identifying a list of threats that are capable to affect safety. OWASP identifies in the 2018 the top 10 IoT security threats where weakness of passwords, network services and interfaces are identified as the top three threats.
Our threat taxonomy is a consolidation of threats previously considered in other documents/reports[40] [41] [42] and is composed of the following category.

- TG1.1 – Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional damage including safety and information leakage or sharing due to human errors.
- TG1.2 – Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, can also be linked to TG5.
- TG1.3 – Intentional physical damage: in IoT the physical access to the devices that are spread in a potential uncontrolled environment is more serious than in another domain.
- TG1.4 – Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software.
- TG1.5 – Legal: This group provides for threats resulting from violation of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law. Section 4 of the present document will discuss aspects of this TG.
- TG1.6 – Organisational threats: This group includes threats to the organizational sphere.

We remark that Botnet is a security concern typically involving IoT but not very often targeting IoT itself. Botnets normally exploit IoT vulnerabilities to infect the devices. Initially, IoT botnets were grounded on manual physical malicious activities on the devices (TG1.3) or on exploiting the access control weaknesses and default passwords (T1.1.1). Later attackers focused on protocol weaknesses (TG1.2) vulnerabilities in general (TG1.4) and diffusion via malware. Recent botnets adopt hybrid approaches to infect the devices therefore they can be associated with different threats. In the following, we associate specific botnet of threat groups considering the principal threat type used to implement the botnet. In addition, proxy threats are common, where a compromised device is used as a proxy to launch attacks hiding the identity of the attacker. In this case, no infection is needed, just the reuse existing functionality.

[40] ENISA Smart Grid Threat Landscape, and Good practice
https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide
[41] ENISA Threat Landscape and Good Practice Guide for Internet Infrastructure
https://www.enisa.europa.eu/publications/iitl/at_download/fullReport
[42] ENISA Threat Landscape and Good Practice Guide for Smart Home and Converged Media
https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence

Threat Group TG1.1: Unintentional damage/loss of information or IT assets

Threat T1.1.1: Information leakage/sharing due to human errors

Human errors are among the most critical threats in today complex environments. These threats are accidental, meaning that they are not intentionally posed by humans, and are due to misconfiguration, clerical errors, misapplication of valid rules and knowledge-based mistakes. In IoT, most errors are related to poor/absent patch management, the adoption of weak passwords or failure to update default ones, as well as to wrong authorisation configurations. Device authentication or device authorisation may need a non-trivial human intervention since Internet objects ("things") usually do not have a priori knowledge about their ecosystem. The well-known lack of specialized IoT cybersecurity competences (even when only simple, "basic hygiene" security is needed) plays an important role in increasing the errors at this level (see Threat T1.6.1).

Assets: "Data", "Device", "Infrastructure", "Platform and backend", "Decision making".

Threat T1.1.2: Inadequate design and planning or incorrect adaptation

IoT devices rely on software that might contain severe bugs due to wrong design choices and absence of a reliable adaptation/update strategy to fix such errors. This makes the devices vulnerable to many different types of attacks from buffer overflow to lack of authentication (well-known, easy-to-guess, hardcoded password for device configuration). This can be considered one of the most important security threats, and in many cases, it is exploited to generate botnet attacks. IoT still misses an effective adaptation planning strategy to cope with this type of threats. This threat is therefore strongly connected with TG1.3.

Assets: "Device", "Infrastructure", "Platform and backend", "Management".

Threat Group TG1.2: Interception and unauthorised acquisition

Threat T1.2.1: Interception of information

This threat considers an attacker intercepting a communication between two communicating parties. In IoT network, not all the communication channels are sufficiently protected, for instance if keying material, security parameters, or configuration settings are exchanged in clear or if weak or unsuitable/vulnerable cryptographic algorithms are used. Related attacks include man-in-the-middle, communication protocol and session hijacking, or message replay. The man-in-the-middle attack relies on the fact that both the commissioning and operational phases may be vulnerable. In IoT, it is normally assumed that no third parties can eavesdrop during the execution of key materials exchange protocol (i.e., communication in clear form). IoT communication protocol hijacking takes advantage from the possibility to "sniff" the traffic and then uses aggressive techniques like forcing disconnection or reset. In case of session hijacking, attack activities are oriented to act as a legitimate host/device to steal, modify or delete transmitted data. In addition, device authentication or device authorisation may be non-trivial or need human intervention (see Unintentional damage / loss of information or IT assets threat group), since devices usually do not have a priori knowledge about the rest of the ecosystem or completely automatic mechanisms to differentiate legitimate and illegitimate devices (see physical threat group). An attacker with low privileges can misuse additional flaws in the implemented

authentication and authorisation mechanisms of a device to gain more privileged access to the device itself obtaining elevation of privilege.
Another attack that fits the IoT domain is the "harvest and decrypt" attack in which an attacker can start to harvest (store) encrypted data today and decrypt it years later, once a quantum computer is available (e.g., VENONA project[43]). This is linked to the fact that many IoT devices remain operational for a decade or even longer, and during this time, digital signatures used to sign software updates might become obsolete, making the secure update of IoT devices challenging. Reply attack uses a valid data transmission maliciously by repeatedly sending it or delaying it, in order to manipulate or crash the targeted device.
Assets: "Device", "Infrastructure", "Security mechanisms".

Threat T1.2.2: Unauthorised acquisition of information

IoT networks can be spoofed, altered, or replayed, to create routing loops, attract/repel network traffic, extend/ shorten source routes, to name but a few. As an example, an attacker can implement a sybil attack to present multiple networking level identities to other devices in the network.
In addition, IoT can be subject to disclosure of sensitive data, intentionally or unintentionally, to unauthorised parties. Confidential data may be captured by attackers from individual devices, during transit, or from the backend, local storage, edge nodes (information acquisition via physical access is described in TG1.3). Privacy must be also considered, for instance, when the sensor is transmitting sensible data like health-related data and when device location tracking provided by the device poses a privacy risk to users. This threat shares most of the attack strategies with Networking Domain (see Section 3.4). In the following, we describe some of them showing a clear connection with IoT environment where nodes can be manipulated/added more easily.
Assets: "Device", "Infrastructure", "Platform and backend".

Threat Group TG1.3: Intentional physical damage

Threat T1.3.1: Device modification

Having physical access to the IoT device allows a non-trusted factory to clone the physical characteristics, firmware/software and security configuration of a device. Deployed devices might also be compromised and their software reverse-engineered, allowing device cloning. Cloned devices may be sold cheaply in the market and can contain functional modifications including backdoors. Alternatively, a genuine device may be substituted with a variant or clone during transportation, commissioning or in operation. Another substitution is a firmware level substitution that is less expensive and less easy to discover that physical cloning or replacement. In some cases, this substitution occurs in the framework of a patching or upgrading, and it may or may not require physical access (we include this type of attack in this threat for completeness even if it can be obtained without full physical access). Other attacks that refer to this threat are device replication, camouflage, malicious device/node injection, to name but a few.
Assets: "Device", "Infrastructure".

[43] VENONA https://www.nsa.gov/news-features/declassified-documents/venona/

Threat T1.3.2: Extraction of private information

IoT devices are often physically unprotected. This permits physical attacks to extract private information such as keys, data from sensors (for example, healthcare status of a user), configuration parameters (for example, the Wi-Fi key), or proprietary algorithms (for example, the algorithm performing some data analytics task).

Assets: "Device".

Threat Group TG1.4: Nefarious activity/abuse

Threat T1.4.1: Identity fraud

Identity fraud in IoT primarily refers to both weak admin/user credentials and authentication, which is a common threat for IoT (at the top of the OWASP top Ten), and identity spoofing, which involves authentication protocol leakages in IoT, for instance, at device bootstrapping time. Poor credential management such as weak password choices or lack of multi-factor authentication for user and administrative interfaces of devices, gateways or back-ends, is a common vulnerability in many information systems and even exacerbated in IoT due to the limitations at device side. Passwords/credentials are in most of the cases guessable, weak and hardcoded at firmware level. Identity fraud in IoT can be achieved due to weakness of the identity provisioning protocols that can be spoofed.

Assets: "Device", "Infrastructure", "Platform and backend".

Threat T1.4.2: Denial of service

Traditional (Distributed) Denial of Service is a major threat for IoT where devices, being resource-constrained, are more susceptible to denial of services. It aims to threaten components availability by exhausting their resources, causing performance decrease, loss of data, service outages, on one side, but also potential safety issue, on the other side. In addition, compromised devices themselves are often used to disrupt the operation of other networks or systems via a Distributed DoS (DDoS) attack. Here, we consider DoS attacks that target IoT and are not generated by IoT devices.

Assets: "Device", "Infrastructure", "Security mechanisms", "Platform and backend".

Threat T1.4.3: Malicious code/software/activity

This class of threats usually targets all ICT stack and the 6 domains in this deliverable. Threats aim to distribute and execute malicious code/software or execute malicious activities. These threats usually involve malware, exploit kits, worms, trojans, and exploit backdoors and trapdoors, as well as developer errors/weaknesses. Devices can be infected with such malicious programs due to vulnerabilities in software or firmware, that are much more diffuse than in other domains due to the difficulties in keeping an IoT device updated.

Counterfeit device is an IoT specific threat that is difficult to discover, since the compromised device cannot be easily distinguished from the original. These devices usually have backdoors and can be used to conduct attacks on other ICT systems in the environment, in most of the cases botnet-based attacks.

Assets: "Device", "Infrastructure", "Security mechanisms", "Platform and backend".

Threat T1.4.4: Misuse of assurance tools

Assurance is the way to gain justifiable confidence that a system will consistently demonstrate one or more security properties, and operationally behave as expected, despite failures and attacks [5]. Assurance is based on audit, certification, and compliance tools and techniques [6] [7]. The manipulation of such tools and techniques can result in scenarios where the malicious behavior of attackers is masqueraded and is not discovered. Assurance information is necessary to ensure the security of the system during its entire lifecycle from its design to its operation. It is also necessary to guarantee compliance to regulations. In an IoT environment, the adoption of assurance is even more crucial due to the need to cope with the lack of security mechanisms at the peripheries.

Assets: "Data", "Devices", "Platform and backend", "Infrastructure", "Security Mechanisms", "Management".

Threat T1.4.5: Failures of business process

Poorly designed business processes can damage or cause loss of assets. IoT can be part of a complex system handling sensitive data, like in case of health or industrial applications. Threats to confidentiality of sensor data (e.g., wrong delivery through untrusted gateways) and integrity of sensor data (e.g., the use of temporal local tamperable data store) can have high impact.

Assets: "Devices", "Platform and backend", "Infrastructure", "Security Mechanisms", "Management".

Threat T1.4.6: Code execution and injection (unsecure APIs)

IoT applications are built on web service model and in many cases each device offers APIs that can become a target of attack, and be vulnerable to well-known attacks, such as the Open Web Application Security Project (OWASP) Top Ten list.[44] This threat is listed as the third mostly risky in the OWASP Top 10 IoT due to the fact that i) IoT offers poor administrative interfaces and ii) due to budget restrictions, IoT vendors do not dedicate much budget on its security and testing. In particular, code execution (e.g., XSS) and injection (e.g., SQL injection) are critical attacks that can increase risks. Due to the application nature of this threat, it will be discussed more in detail in Section 3.7.

Assets: "Platform and backend", "Security Mechanisms", "Management".

Threat Group TG1.5: Legal

Threat T1.5.1: Violation of laws or regulations

The management of legal aspects impacts IoT system and can represent a threat to the system itself. As mentioned earlier, the legislation landscape on IoT is quite complex, and IoT systems potentially involve devices produced under different legislations and regulations. Violations of laws or regulations, the breach of legislation, the failure to meet contractual requirements, the unauthorised use of Intellectual Property resources, the abuse of personal data, the need to obey judiciary decisions and court orders are examples of threats. Also, the lack of cyber-regulations in countries with high concentration of hacker groups is having an impact with these regards. In January 2018, Cyber Security Research Institute

[44] Many common vulnerability exposures for Big Data components, such as Hadoop, are reported in specialized Websites, see for example https://cve.mitre.org and https://www.cvedetails.com

report on Internet of Things sponsored by F-Secure stated that IoT represents a considerable threat to consumers, due to inadequate regulations regarding its security and use.[45] In some scenarios the situation is even more complex due to the ubiquitous nature of IoT sensors. For instance, Google was forced to announce in early 2018 that its Nest Security system included a microphone that was not disclosed to consumers.[46] More details on legal aspects are discussed in Chapter 4.
Assets: All assets.

Threat Group TG1.6: Organisational threats

Threat T1.6.1: Skill shortage
A possible shortage of skilled IoT cybersecurity experts is one of the main threats to IoT. Another aspect is the lack of security awareness at management level.[47] This threat has a strong link to threat group TG1 "Unintentional damage / loss of information or IT assets". The F-Secure chief, Mikko Hypponen declared in 2017 that "m*any IoT device vendors have little to no experience in building internet-connected devices*," and "*they build IoT devices to be cheap and to work, but not to be secure*."[48]
Assets: "Roles".

3.4. Network-Centric Security

This section contains an overview of assets and threats in Domain 2 on Network-centric security. It concentrates on the latter evolution of network security including also attacks on (software-defined) networks. Details on attacks linked to the identified threats are reported for interested readers in Appendix A.2.

3.4.1. Context and Architecture

Traditional network environments are characterized by well-defined perimeters and trusted domains. Networks have been initially designed to create internal segments separated from the external world by using a fixed perimeter. The internal network was deemed trustworthy, whereas the external was considered potentially hostile. Perimeter devices, such as firewalls and intrusion detection systems, have been the traditional technologies used to secure the network. However, this environment has changed over time together with the network architecture, introducing some effects/hurdles summarized below.

- **A large diffusion of IP-based networks.** In the third generation (3G) networks, the IP-based communication caused the migration of Internet security vulnerabilities and challenges in the wireless domains. With the increased need of IP based communication, the fourth Generation (4G) mobile networks enabled the proliferation of smart devices, multimedia traffic, and new services into the mobile domain. With the advent of the fifth generation (5G) wireless networks, the security threat vectors will be more important in size and variety, with additional greater concerns for user privacy.

[45] PINNING DOWN THE IOT https://fsecurepressglobal.files.wordpress.com/2018/01/f-secure_pinning-down-the-iot.pdf
[46] Users alarmed by undisclosed microphone in Nest Security System https://arstechnica.com/gadgets/2019/02/googles-nest-security-system-shipped-with-a-secret-microphone/
[47] See https://www.justice.gov/usao-ndca/pr/sunnyvale-based-network-security-company-agrees-pay-545000-resolve-false-claims-act
[48] Should You Fear the IoT_Reaper? https://blog.f-secure.com/should-you-fear-the-iot_reaper/

- **A more programmable network.** The advent of SDN (Software Defined Network) improves the network elasticity, simplify network control and management. Nevertheless, together with SDN it is plausible that new threat vectors are arising.
- **A cloud-based network.** The virtualization of the network components changed the traditional network concept, where networking functions were mainly implemented in dedicated devices and dedicated hardware. A network using NFV (Network Functions Virtualization) is mainly based on:
    - Virtualized network functions (VNF): they comprise the software used to create the various network functions in their virtualized format. These are then deployed onto the hardware, that is, the Network Functions Virtualization Infrastructure (NFVI).
    - Network Functions Virtualization Infrastructure (NFVI): it consists of all the hardware and software components, which are contained within the environment where VNFs are deployed.

  Network Functions Virtualization provides the basis for placing various network functions in different network perimeters on a need basis and eliminates the need for function or service-specific hardware.
- **Unclear network boundaries.** Virtualized and distributed network functions can span across remote locations, consequently the concept of well-defined trusted domains is no longer valid.
- **A network relying on the automation of the operations and self-organizing (SON).** SON was originally developed as an operational approach to streamline cellular Radio Access Network (RAN) deployment and optimization. However, mobile operators and vendors are increasingly focusing on integrating new capabilities such as self-protection against digital security threats, and self-learning through artificial intelligence techniques, as well as extending the scope of SON beyond RAN to include both mobile core and transport network segments. The automation of the network minimizes its lifecycle cost by eliminating manual configuration of network elements at the time of deployment, right through to dynamic optimization and troubleshooting during operation.

The context of this domain is the Telco scenario, with its main components: access, edge and core elements, with a particular attention to mobile network infrastructures given the current transition toward 5G. The transition to 5G will in fact bring several specific security improvements[49] that are grounded on the above aspects. The new characteristics and functionalities of the 5G network have an impact on the network architecture by enabling deployments where some sensitive assets or functions, currently performed in the physically and logically separated cores, can be moved closer to the edge of the network. This requires security controls to be moved too, in order to encompass critical parts of the whole network, such as the radio access part. In addition, the support of a wide range of use cases adds more complexity in the configuration and management of key parts of the network with the involvement of new players, such as integrators, service providers or software vendors.

[49] See https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview

3.4.2. Assets

A network asset is simply an asset that is part of a network. To provide a service, network assets are interconnected to each other. If a network asset is removed, the system or service may not function to full capacity or at all. Also, the network infrastructure itself can be considered as an asset, since it provides all hardware and software resources part of the network, enabling network connectivity, communication, operations and management of an enterprise network. An infrastructure asset provides the communication path and services between users, processes, applications, services, and external networks like the Internet. Network infrastructure devices include routers, firewalls, switches, servers, load-balancers, intrusion detection systems, domain name systems, and storage area networks.

The introduction of virtualization technology (see Section 3.3) drives the digital transformation of the network, slightly changing the asset definition. The network functions virtualisation concept virtualises the majority of elements/assets of a network. In this way entire classes of network node functions can be set up as building blocks that can be connected to create overall telecommunication networks referred as "network slice". Network slicing is an approach proposed with the advent of 5G to allow a single network to support services with completely different operational parameters and policies. The network is viewed as an asset pool of physical resources and virtual network functions (VNFs), connectivity, bandwidth and computational capabilities. A network slice combines these assets to form a virtual network. Different network slices will have different operational parameters and hence a different combination of assets. The slices may share network assets or may have assets specifically allocated to them, depending on the service policies.

In this context, it is not easy to provide a network asset taxonomy. However, a possible way to categorize network assets can be to group them based on their role, derived from the functions provided by the assets or network elements. For this purpose, in this deliverable the network has been divided into subdomains and network assets have been categorized accordingly to their provided functions (and inspired from ENISA, see Figure 3).[50]

- **Access network.** It connects individual devices to other parts of a core network through radio or fixed connections.
- **Core network.** It is the part of the network that offers services to the devices/customers who are interconnected by the access network. The core network also provides the gateway to other networks.
- **Infrastructure network/area network.** It includes hardware and software resources of an entire network that enable network connectivity, mobility management, network operation and management.
- **Peering points.** They support the communications between the subscribers of one provider and the subscribers of another provider. We consider in this group also the Internet Provider Exchange (IPX) roaming network.

[50] Guideline on Threats and Assets Technical guidance on threats and assets https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets

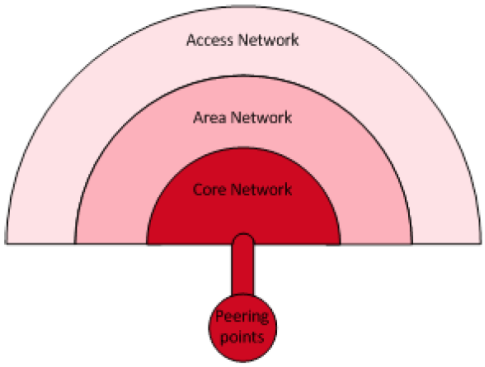


Figure 3 – Network asset categorization

Since some types of endpoint devices can also be considered as network assets a further group has been added to take them into account.

- **Endpoint network.** It includes systems/devices that communicates back and forth with the network to which they are connected. IoT devices are an example of assets in this category. This asset type is included here because in some settings the network provider retains some control (and responsibility) over these assets.

Each class can be further refined in different asset categories as presented in the following table.

Table 9 – Assets: Endpoint network

Class	Category	Description
Endpoint network	Fixed subscriber asset	Customer Premises Equipment (CPE), authentication systems related to fixed line CLI.
	Mobile subscriber asset	USIM, eSIM, iSIM, devices.

Table 10 – Assets: Access network

Class	Category	Description
Access network	Fixed Network Access (FA)	Network elements placed in the access layer, which connects individual devices to other parts of the core network through fixed connections. This category includes assets such as cabinets, Optical Line Terminal (OLT), Digital Subscriber Line Access Multiplexer (DSLAM).
	Radio Access Network (RAN)	Network elements placed in the access layer, which connects individual devices to other parts of the core network through radio connections. The main components that form a Base Station (BTS) site are – Base Band Unit

		(BBU), Remote Radio Head (RRH) and Antennae. Different deployments are possible today like Distributed Radio Access Network (D-RAN), where the 4G/5G radio at the macro site tower (or eNodeB/gNode) consists of a collocated Baseband Unit (BBU) at the base of the tower and a Remote Radio Head (RRH) at the top, interconnected by a fiber optic cable using the Common Protocol Radio Interface (CPRI). Thanks to the network cloudification Centralized Radio Access Network (CRAN) deployments are possible where the base station baseband processing (BBU) is centralized at the edge of the core network.
	Fixed Wireless Access (FWA)	Network elements which connects stationary or ‘fixed’ user equipment (UE) − terminals, modems, routers − located at the edge of the communications network to the network core.

Table 11 – Assets: Core network

Class	Category	Description
Core network	Access & session management	Network elements handling access and session management. Example of assets are MME (Mobility Access Management), AMF, SEAF (Security Anchor Function), SMF (Session Management Function).
	User plane management	Network elements handling user plane traffic. Example of assets are SGW-U, PDG (Packet Data Network).
	Authentication subscriber management	Database holding subscriber authentication credentials and profile. The category includes assets like Authentication Server, Authentication credential Repository.
	Policy control management	Network elements handling policy control management.

Table 12 – Assets: Infrastructure network/area network

Class	Category	Description
Infrastructure network/area network	Security asset	Security GW, Signaling Firewall.
	Cloud	Cloud infrastructure includes an abstraction layer that virtualizes resources and logically presents them to users through application program interfaces and API-enabled command-line or graphical interfaces.

Table 13 – Assets: Peering points

Class	Category	Description
Peering points	Interconnection to roamer partners	Network elements at the perimeter of the core network handling signaling security and control. This category includes assets like DRA (Diameter Router Agent), Security Gateway.

3.4.3. Threats

We now discuss the threats that can be mapped to elements of the network asset taxonomy presented in the previous section. Details on attacks exploiting vulnerabilities linked to the identified threats are reported in Appendix A.2. Threats reported here are not exhaustive but representative of the covered domain. Most of them are related to mobile network considering the network evolution toward 5G and the fixed-mobile network convergence. This section provides an overview of the main relevant security issues. Most of them are already known and under the attention of different standardization bodies, security working groups and alliances which are working on them by providing guidelines and countermeasures as well as configurations hardening. However, despite such actions, some of these attacks are still ongoing. This is in part motivated by the availability of open source attack tools described in Appendix A.2.

For several years now, vulnerable network assets have been exploited as preferred targets. Malicious cyber actors often target network devices, and, once on the device, they can remain there undetected for long periods. After an incident, where administrators and security professionals perform forensic analysis and recover control, a malicious cyber actor with persistent access on network devices can reattack the recently cleaned hosts. The adoption of a security assurance process that covers the entire life cycle management starting from secure design, secure development, secure deployment, security monitoring and security management is necessary to counteract these attacks. There are also cases where attackers do not need to compromise their intended target directly but can achieve their aim by compromising its supply chain where it is least secure. In the last years there was in fact an increase in breaches caused by vulnerable software. Any given software stack can contain many sources of components and libraries in differing versions, increasing the need to

assess, test, and patch carefully. This threat highlights the importance of managing the supply chain.
Another source of well-known network breaches is the use of legacy protocols. Signalling exchange is required to establish and maintain a communication channel or session on telecommunication networks as well as allocate resources and manage networks. For example, 2/3G networks used Signalling System 7 (SS7) and SIGnalling Transport (SIGTRAN) while 4G relies on Diameter; all generations use Session IP (SIP) and GPRS Tunnel Protocol (GTP). Many fundamental services, such as short messaging service (SMS), are managed by these protocols. Many of these signalling protocols are outdated and have been implemented under a trust model that assumed well-behaved mobile operators without the need to deploy strong security controls.
In addition, another type of attack vector comes from flaw in the specifications. The paper in [8] is an example of vulnerabilities discovered during a careful analysis of LTE access network protocol specifications and a demonstration of how those vulnerabilities can be exploited using open source LTE software stack and low cost hardware. The paper in [9] demonstrates instead the usefulness of adopting formal verification tools to automatically check whether the desired security properties are satisfied or if instead the defined protocols/procedures suffer from ambiguity or under-specification.
To complete our overview of the attack scenario, another vector comes from poor configuration of network nodes as highlighted in [10].
In the following section, the most relevant network threats are reported according to the following categories.[51] [52]

- TG2.1: Unintentional damage/loss of information on IT assets: this group includes all threats causing unintentional information leakage or sharing due to human errors.
- TG2.2: Interception and unauthorised acquisition: this group includes any attack, passive or active, where the attacker attempts to listen, intercept or re-route traffic/data. An example is the man-in-the-middle attack. This group also includes manipulation attacks where the attacker attempts to alter or interfere with data in transit, in particular with signalling messages and routing information.
- TG2.3: Nefarious activity/abuse: this group includes threats coming from nefarious activities. It requires active attacks targeting the network infrastructure of the victim.
- TG2.4: Organisational threats: this group includes threats to the organizational sphere.

Threat Group TG2.1: Unintentional damage/loss of information on IT assets

Threat T2.1.1: Erroneous use or administration of devices and systems

Attacks or human-errors are exploited to gain unauthorised privileged access to a system, which can lead to the installation of other malicious content or backdoors or even physical access to the devices. It is used as part of an attack, regardless of whether the target is a single system/asset or a whole network or facility.

[51] Mobile Telecommunications Security Threat Landscape, GSMA, January 2019 https://www.gsma.com/aboutus/resources/mobile-telecommunications-security-threat-landscape
[52] Threat Landscape 2018, ENISA https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

Assets: "Core Network", "Access Network", "Infrastructure Network/Area Network", "Peering Points".

Threat Group TG2.2: Interception and unauthorised acquisition

Threat T2.2.1: Signaling traffic interception

Most signaling protocols are dated and implemented in an insecure way. Some of them have not been designed with any security features. Signaling System 7 (SS7) and Diameter are signaling protocols used in mobile networks. It is widely known that these signaling protocols have no security defenses built in and have several severe security weaknesses, which can be exploited by attackers in many ways. SS7 is used to exchange information among different elements of the same network or between roaming partner networks (e.g., call routing, roaming information, features available to subscriber). Diameter is the replacement of SS7 for the 4G mobile network. An adversary could exploit signaling system vulnerabilities to redirect calls or text messages (SMS) to a phone number under the attacker's control.

Assets: "Core Network", "Peering Points".

Threat T2.2.2: Data session hijacking

Session Hijacking is an attack which is basically used to gain an unauthorised access between an authorized session connection. For example, the GPRS Tunnelling Protocol (GTP) allows mobile subscribers to maintain a data connection for Internet access while on the move. GTP manages tunnels for transporting IP packets throughout the core network to the internet. GTP comprises three parts—control plane (GTP-C), user plane (GTP-U) and charging (GTP-C). Since there is no authentication and encryption supported in GTP-U messages themselves, several attacks to GTP-U might be possible. An attack via the GRX global roaming exchange network can be conducted by employees of almost any mobile operator as well as by external attackers who have access to the operator's infrastructure. Such an attacker might be able to craft GTP-U messages and send them to the network to trigger answer messages and thus get information (e.g. about network topology), or just send malicious messages to the network. This may involve guessing a valid TEID (Tunnel Endpoint Identifiers), hijacking a TEID, unless the endpoints use non-predictable TEIDs.

Other common hijacking attacks exploited the vulnerabilities of Border Gateway Protocol (BGP). They are documented for instance in IETF's RFC 4272 "BGP Security Vulnerabilities Analysis", which was published in 2006. BGP fundamental vulnerabilities related to the lack of a mechanism to protect integrity and authenticity of messages in peer-to-peer communications. Also, the lack of a mechanism to validate the authority of an Autonomous system (AS) to announce prefixes or relay route information. Finally, BGP has no mechanisms to validate the authenticity of the path attributes in prefix announcements. These security vulnerabilities can be exploited by an adversary to perform BGP hijacking, when the adversary claims to be the origin of prefixes of another network. The result of this attack is that the traffic is forwarded to the wrong destination. This attack can be used to intercept, alter, or disrupt Internet traffic.

Assets: "Core Network", "Peering Points".

Threat T2.2.3: Traffic eavesdropping

An eavesdropping attack is possible if the traffic is not protected, for instance, user-plane traffic is not encrypted at the radio access level or if vulnerable/weak crypto algorithms are used. Eavesdropping is also possible by exploiting lack of protection on the backhaul link that connect radio access network to core network. In 4G networks the backhaul is composed of IP-based control elements and interfaces, making it vulnerable to IP-based attacks. In addition, eavesdropping can be possible also by exploiting the lack of mutual authentication between the radio access node and the core network, or the lack of prevention against IP-based attacks, or the lack of encryption of data and signaling traffic. If the backhauling link is not encrypted, then user security context information such as part of the currently used keying material will be revealed to an eavesdropper. Also, the user plane traffic would be available to eavesdroppers in clear. The impact of eavesdropping depends on what traffic is affected. Eavesdropping control plane traffic can be more critical as it may reveal information to the attacker that allows him to mount further attacks.
Assets: "Radio Access Network", "Infrastructure Network/Area Network".

Threat T2.2.4: Traffic redirection

Redirection of data can be accomplished at different levels. On local networks, IPv4 ARP spoofing, IPv6 router advertisement or automatic proxy discovery can be exploited. At the internet level, DNS spoofing is widely used to point legitimate hostnames to fake servers. Ultimately, redirection of data can be possible by data manipulation that can be especially performed if data integrity is not protected.
Assets: "Access Network", "Core Network".

Threat Group TG2.3: Nefarious activity/abuse

Threat T2.3.1: Exploitation of software bugs

The more the network environment will be software-defined, virtualized and transferred on general commodity hardware equipment, the more such environment could be exposed to vulnerabilities due to software bugs and poor configuration. Today, every year, thousands [53] of software bugs impact network devices such as routers, servers, databases or other functional elements of the networks. This type of threat also includes network failures when several systems fail to connect or to work together.

Through software bugs it is possible to attack the vulnerable device or the entire infrastructure causing, for instance, DoS, frauds, and other issues. To help customer to manage such situations, many network manufacturers such as Cisco, Juniper, Ericsson, Huawei set up specific Product Security Incident Response Team (PSIRT) Services, aimed to collect, analyse, and provide patches related to their products and finally to help their customers to address the possible issues suggesting related solutions.

Assets: "Access Network", "Core Network", "Infrastructure Network/Area Network", "Endpoint Network".

Threat T2.3.2: Manipulation of hardware and firmware

Attacks against hardware and firmware are appealing to attackers. Once they have compromised the firmware, they can safely persist on the device and evade the

[53] See https://www.cvedetails.com/vulnerabilities-by-types.php

security measures applied at OS, application or software levels. Since the malicious code lives within the firmware of physical components, the threat can easily survive a complete reimaging of the system or even replacement of the hard drive(s). This sort of persistent attack would typically occur as a second stage of malware infection. Once a system is initially compromised, malware could then look for vulnerabilities in the firmware and missing device protections that could allow malicious code to be implanted in the firmware itself. This threat points to Device/ IoT-centric security (see Section 3.3.3).
Assets: "Core Network", "Infrastructure Network/Area Network", "Endpoint Network".

Threat T2.3.3: Malicious code/software/activity

Malware is any piece of software written with the intent of damaging devices, stealing data, or causing a damage. Viruses, Trojans, and recently crypto-miners and ransomware are among the different types of malware. Although the primary target for the malware is traditionally to "infect" a device (fixed or mobile), malware is one of the main threats against network infrastructures (e.g. the control plane), and it will be even more dangerous with the emerging networks virtualization. When devices are considered, this threat is strongly connected to threat T1.4.3 in Device/IoT-centric security (Section 3.3.3).
Assets: "Core Network", "Endpoint Network".

Threat T2.3.4: Remote activities (execution)

Remote activities can take a variety of forms. In general, they refer to the process by which an agent can exploit a network vulnerability to run, for example, arbitrary code on a targeted machine or system.
Assets: "Core Network".

Threat T2.3.5: Malicious code - Signaling amplification attacks

Mobile networks do not have enough radio resources to provide service to every single customer at the same time. The scarcity of bandwidth requires advanced techniques to reuse idle resources in an efficient manner. The RRC protocol stack reassigns radio resources from a given user when the connection goes idle for a few seconds. When an inactivity timer expires, the radio bearer between the mobile device and the core network is closed and those resources become available to be reassigned to another UE. At this stage, the UE moves from connected to idle state. Each instance of bearer disconnection and setup involves a significant number of control messages exchanged among nodes within the Evolved Packet Core (EPC). DNS amplification is another example of attack that massively exploits open recursive DNS servers mainly for performing bandwidth consumption (DDoS attacks). The amplification effect lies in the fact that DNS response messages may be substantially larger than DNS query messages.
Assets: "Access Network", "Radio Access Network", "Core Network".

Threat Group TG2.4: Organization (failure malfunction)

Threat T2.4.1: Failures of devices or systems

System failures include the incidents caused by failures of a system, for example hardware failures, software failures or errors in procedures or policies (see Section 3.5 for more details). An example is a software bug in a system like an HLR that

suddenly stops its operation and consequently prevents all subscribers from connecting. This threat clearly points to Device/IoT (see Section 3.3.3).
Assets: "Access Network", "Core Network", "Infrastructure Network/Area Network".

Threat T2.4.2: Supply chain

A supply chain threat refers to the compromise of an asset, for instance, a software provider's infrastructure and commercial software, with the aim to indirectly damage a certain target (e.g., the software provider's clients). This type of attack is typically used as a first step out of a series of attacks. More concisely, it is used as a stepping-stone for further exploitation, once foothold is gained to the target system(s). Attackers do not need to compromise their intended target directly but, in many cases, can achieve their aim by compromising the supply chain where it is least secure. This potential threat highlights the importance of managing the supply chain holistically, and driving out or mitigating insecure elements.
Assets: "Infrastructure Network".

Threat T2.4.3: Software bug

A security bug is a software bug that can be exploited to gain unauthorised access or privileges on a computer system. Software bugs could have an impact on ICT systems, such as routers, servers, databases, and in turn impact networks or services. This type of threat also includes complex failures like network failures when several systems fail to connect or otherwise work together.
Assets: "Access Network", "Core Network", "Infrastructure Network/Area Network".

3.5. System-Centric Security

This section contains an overview of assets and threats in Domain 3 on system-centric security. Details on attacks linked to the identified threats are reported for interested readers in Appendix A.3. This section concentrates on the latter evolution in the system domain including an overview of assets, threats, and attacks that focused on virtualized infrastructures and the cloud. Major sources of information for this study are "ENISA Security Aspects of virtualization",[54] "ENISA Cloud Security Guide for SMEs: Cloud computing security risks and opportunities for SMEs"[55] and "ENISA Cloud Computing risk assessment", [56] the CSA "Top Threats to Cloud Computing The Egregious 11"[57] and "The Treacherous 12 Top threats to Cloud Computing".[58]

3.5.1. Context and Architecture

The notion of system in ICT is generic enough to denote almost everything that is based on software components. System is widely used as synonym of Operating

[54] ENISA study on the security aspects of virtualization https://www.enisa.europa.eu/news/enisa-news/enisa-study-on-the-security-aspects-of-virtualization
[55] Cloud Security Guide for SMEs https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes
[56] Cloud Computing Risk Assessment https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
[57] Top Threats to Cloud Computing: Egregious Eleven, https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven
[58] The Treacherous 12 Top threats to Cloud Computing, https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

System (OS), or in general software that enables applications to take advantages of the computation connectivity and storage capabilities of the hardware. Due to their centrality, their role in some crucial security features (e.g., authentication), and their complexity, OSs were a preferred target of many disruptive attacks in the past (e.g., Code Red exploiting IIS buffer overflow, Sasser attacking the Local Security Authority Subsystem Service, Snakso Linux server rootkit). Nonetheless, they will have a fundamental role even in the future due to the fact that OSs are increasingly immersed in a more complex environment (e.g., mobile devices, virtualized systems), where their vulnerabilities can be either exacerbated or mitigated and they can become a commodity for applications (e.g., containerization of applications). For instance, Linux OSs are deeply involved in complex environments such as IoT.

In this section, we concentrate our analysis on recent service-based systems and the relative enabling technologies, namely, virtualization and cloud computing, mentioning the above traditional OS-related threats and attacks when relevant. Virtualization and cloud computing fundamentals are briefly summarized in the following.

Virtualization. Virtualization solutions allow different users to manage and share physical hardware by supporting multiple shared environments that are isolated, while running on the same infrastructure. Virtualization introduces many benefits that strengthen cloud flexibility and efficiency, such as server consolidation and reduced costs for system operation and management, optimized resource utilization, multiple execution environments, and simplified management. Virtualization techniques and virtualized architectures introduce an additional layer of execution, including their own administrator role (virtualization admin), which requires proper management and security protection. This layer is made up of several different components, each with a role in the virtualization process, each representing a potential new target for malicious attacks [11] [12].

- The **hypervisor** is the component that acts as a mediator between virtual machines and the underlying physical devices. It mediates all hardware requests by the virtual machines down to the physical hardware, sharing physical devices as resources.
- The **virtual machine monitor** is an application component of the hypervisor that keeps track of activities carried out by virtual machines (i.e., it manages VM applications), forwards hardware request to physical resources, provides replicated platforms, and supports resource sharing between different virtual machines. It has the responsibility to guarantee end users virtualization transparency.
- **Guest machines**, also known as virtual machines, instantiate the virtualized (encapsulated) system made of the operating system and applications, using the hardware abstraction provided by the virtual machine monitor. Guest machines are isolated by the hypervisor controlling their activities and behave as if they were in a single execution environment with their own dedicated resources.
- The **host machine** is the real physical machine and its operating system (host operating system) that hosts the virtualized environment. The host operating system directly manages the physical hardware underlying the virtualized environment and is where the hypervisor runs.

- The **management server** is the virtualization platform made up of a set of components for directly managing the virtual machines, consolidating services, allocating resources, migrating virtual machines, and assuring high availability, to name but a few.
- The **management console** is the component that provides access to a management interface to the virtualization product for configuring and managing virtual machines. Virtual machines can thus be added, modified, deleted or configured.
- The **network components** that facilitate the development of virtual networks, where virtual network devices (e.g., switches, routers) are completely controlled though software, and the network protocols and stack are simulated to replicate physical ones insofar as possible.
- **Virtualized storage** that provides all the components for abstracting physical storage in a single storage device that can be accessed either over the network or through a direct connection. Storage virtualization introduces additional management overhead, since stored data can be only logically partitioned in different storage locations, while belonging to the same shared storage.

Virtualization introduces a complex mix of software components at different levels of the computing architecture (e.g., operating system, communication, management, interface), each with its own administrator privileges, thus enlarging the attack surface. Virtualization techniques, while providing undebatable advantages to security, also come with increased security risks that must be considered when deploying strong and secure virtualized infrastructure. This scenario is exacerbated by the trend towards containerization, where virtualization technology requires services to be deployed and served in a microservice fashion.

Cloud environment. Based on virtualized ICT infrastructure accessible through the internet, the cloud-computing paradigm supports a new vision of IT whereby software applications and computational resources are released as services and used on a pay-as-you-go [13] basis. Cloud computing is becoming the preferred way to provide IT services. The cloud paradigm comes with several advantages for customers (i.e., end-users and service providers), which can outsource part of their business (that require great IT skill) to the cloud, thus reducing costs for owning, operating, and maintaining computing infrastructure, increasing flexibility, and benefiting from scalable infrastructure. Furthermore, cloud computing provides: i) rapid elasticity that allows resources to scale out and down depending on demand and gives end users stable quality of service and ii) metering capacity for controlling and optimizing resource usage. Cloud computing provides three service models, Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS) [14].
The convenience introduced by cloud computing, in terms of flexibility and reduced costs for owning, operating, and maintaining computing infrastructure, comes at the price of increased security risks and concerns. Users deploying a service in the cloud lose full control over their data and applications, which are fully or partially in the hands of cloud providers. In addition, it makes the end user unaware of the infrastructure's performance and capacity constraints. On top of that, security represents one of the main problems hindering the shift of customers to the cloud. Security issues and requirements affect all layers of the cloud stack (service, platform and infrastructure layers).

In summary, the main peculiarity of modern system architectures is that they are based on multiple layers of software components providing support for the upper layers and interacting with the bottom ones. Application-oriented services can be considered at the top of this layered pyramid, integrating with cloud technologies, and building on virtualization technologies. Even IoT/Edge (see Section 3.3) relies on the top of this pyramid for their operations. This modern system architecture inherits security concerns and hurdles that are relevant for this deliverable.

- **The middleware hurdle.** A virtualized/cloud ecosystem is made of software layers including management and control tools that constitute a complex middleware ecosystem, where there exist a number of critical connections among the services offered by each layer. Misconfigurations and APIs related threats can exploit such complexity making the remediation more complex to be implemented, paving the way to dangerous persistent threats. If virtualization is adopted as the bottom layer, it interacts with the surrounding environment made up of hardware and software, and builds on or interacts with them to provide a secure, robust, and effective virtualized system, for the upper layers. It offers some advanced security features such as isolation, but it also inherits some of the traditional OS security leakages (e.g., for Host or Guest OS). Cloud often relies on these virtualized resources to build a constellation of services, including security-oriented services (e.g., secure channels and authentications) providing functionalities at infrastructure and application layers, and in general to support business processes.
- **The sharing of physical resource hurdle.** It impacts both cloud and virtualization layers, but it is more challenging for virtualization layer that is more related to the sharing of physical resources. In virtual environments, where physical resources are shared between tenants, there may be a set of behaviors that result in the disclosure of sensitive information. For instance, exposure via scavenging in virtualized environments is even more serious than in physical or cloud systems [15]. Virtualized environments seek to cope with this severe class of threats by providing isolation solutions and by promoting fair distribution of resources among all virtualized entities (networking entities included). However, these approaches are difficult to implement due to the intrinsic characteristics of virtualized systems that share computing resources and distribute them (possibly on demand) at runtime.
- **The multitenancy hurdle.** It impacts the cloud layer more than the virtualization layer, because the number of tenants at cloud layer is in general greater than the number of tenants at virtualization level. It is the counterpart of resource sharing from cloud perspective where multiple tenants share the same cloud platform having some administrative rights to act on it. It has a lot in common with the sharing of resources since it can lead to the disclosure of information and incapacitation due to overloading of specific requests. It is exacerbated in case the cloud is implemented on a virtualized environment. It is also linked to the fact that Cloud systems usually deal with a very complex hierarchical structure of administrator privileges at different cloud levels.
- **The monitoring and management hurdle.** Introspection is of paramount importance for both virtualization and cloud. Since they are layered architectures, it is fundamental to monitor and keep everything under control; on the other side, this opens to serious security threats. Sensitive data can be inferred by exploiting the introspection of a privileged process. For example, in case of virtualization, the Virtual Machine Monitor (VMM) allows external

observers to inspect VMs without interfering with them. The VMM is a crucial target for usurpation-based misappropriation, due to its role in virtualization, as well as to the presence of vulnerabilities that allow guest-OS users the potential to execute arbitrary code on the host OS. This is an example of exacerbation of traditional OS vulnerabilities.

- **Sharing of traditional OS threats hurdle.** It is linked to the middleware hurdle. Both virtualization and cloud rely on traditional software systems (e.g., operating systems). The security of a virtualized system depends on the security of the guest operating systems, including the protection against all those attacks that are not peculiar to virtualized OSs, but can target a generic OS installed on certain physical hardware. Similarly, the security of the cloud may rely on the security of the virtualized or the Guest/Host OS layers depending on the level of offering used. Also, containers depend on the security of the kernel of the host OS that shares a number of security features with containers.

The above set of hurdles becomes even more dangerous when combined, exploiting the multilayer nature of current systems. For instance, in a cloud environment based on virtualization, privilege escalation can be even more dangerous than in a traditional environment because of multitenancy, the hierarchical structure of administrator privileges, and the sharing of physical resources that make difficult to counteract intrusion threats. Intruders may in fact obtain privileges through resources that are not the direct target of the intrusion or even resources beyond the visibility of the virtualized environments that nevertheless share the same physical layer.
We note that even if virtualization and cloud are tightly coupled, there is a non-negligible trend of having cloud directly on physical machine (aka bare-metal cloud). According to MarketWatch, the bare-metal cloud market is expected to grow to USD 7.73 billion by 2023, at a CAGR of 31.12% compared to 2017.[59] This trend is grounded on two requirements: i) computational capabilities, ii) simplification of software layers. The second has a link to security due to the assumption that simplicity helps security, but on contrary, it brings back the centrality of traditional OSs, which are far of being considered less affected by security threats and simpler to handle.

3.5.2. Assets

Assets can be categorized in 6 different classes as follows:

- Data – In modern systems architectures, data represent an important asset (discussed more in detail in Section 3.6). For instance, in case of virtualization, they refer to data exchange strategy (i.e., at hypervisor, VMM and management level) or virtual machine/device/container image file data format (Guest machines, virtual devices). In case of cloud, they refer to data exchange channel between cloud components, or how their configurations are stored and protected at rest.
- Infrastructure - It includes all the services aimed to guarantee access to the physical world, including virtualized storage infrastructure and virtualized networking infrastructure, but also access to memory and computation

[59] Bare Metal Cloud Market – Overview and scope,Size, industry Trends, Outlook, Opportunity Till 2023 https://www.marketwatch.com/press-release/bare-metal-cloud-market-overview-and-scopesize-industry-trends-outlook-opportunity-till-2023-2019-10-07

resources. At the level of cloud, it mainly refers to services for datastore provisioning and networking provisioning.

- Middleware – It comprises all the intermediate software layers that characterized modern software systems, from cloud SaaS to hypervisors, and host machines.
- Management – It refers to all management components keeping the entire system monitored for a number of purposes, from performance to traceability and security. It includes VMM, management server and console at virtualization layer and cloud management components.
- Security mechanisms – It refers to all security techniques that are the target for an attacker. These represent the interesting components that would result for instance in unauthorised access to the system, if compromised. For instance, the cloud/virtualization access control mechanisms preserving the multitenancy of the platform, as well as service level security components for channel integrity and confidentiality.
- Roles - it includes human resources and related assets. Cloud tenants and privileged users are the most important roles.

Each class can be further refined into different asset categories as shown in the following table, where a category may refer to specific peculiarities of a specific layer or represent a cross-layer entity.

Table 14 – Assets: Data

Class	Category	Description
Data	In transit	It is associated with services that provide functionalities for data encapsulation and exchange between components/layers.
	At rest	It is associated with services that provide abstractions of storage services.
	Virtual file format	File format used to incapsulate the virtualized environment at file system level.
	Credentials/ configurations	Files that are fundamental to set up working infrastructure at virtualization and cloud levels, and to set up authorisation and authentication across the set of services.

Table 15 – Assets: Infrastructure

Class	Category	Description
Infrastructure	Network	Based on the concept of SDN for virtualization environment. It shows specific peculiarities and shares the basic functions as in the physical network.
	Virtualized storage	Abstraction of the real storage offered as a service in cloud and virtualized as needed.
	Compute nodes	Specific cloud nodes that offer computation capabilities as a service.

Table 16 – Assets: Middleware

Class	Category	Description
Middleware	Hypervisors	Middleware enabling virtualization. It offers basics functionalities and has a central role in offering security features such as isolation.
	Host machines	OSs mounted on the host (physical) machine.
	Platforms	The service platforms used as containers for the cloud services offered to the users or internally to support cloud functionalities.

Table 17 – Assets: Management

Class	Category	Description
Management	VMM	Crucial component in virtualization that permits VM monitoring and inspections.
	Management server/console	Similar to VMM at cloud service level. Crucial to keep the cloud platform under control and to monitor user activities to maintain efficiency.
	Audit/logs engine	Cloud/virtualization components for auditing and log inspection. In cloud, these assets are based most of the time on third parties' tools.
	Assurance tools	Tools to verify the correctness of the adopted security/privacy mechanisms.

Table 18 – Assets: Security mechanisms

Class	Category	Description
Security mechanisms	Infrastructure	It refers to the security of the distributed systems at all layers from the virtualized environment to the cloud architecture.
	Access control/ authorisation	It refers to services offering authentication among cloud components. It is also offered at virtualization level to handle resources.
	Channel integrity and confidentiality	Services that allow internal channel confidentiality and integrity.

Table 19 – Assets: Roles

Class	Category	Description
Roles	Administrator	In cloud and virtualization, the hierarchy of administrative privileges is very fine grained and spans all services at all layers.
	Tenant	In the framework of a shared environment, a tenant is a Cloud service client that has a specific set of administrative privileges.

We note that most of the categories and sub-categories in the above tables are still relevant for generic systems. For example, OS, a very typical and common resource in every enterprise infrastructure, shares security concerns with the virtualized ones except for some peculiarities of the virtual environment (e.g., OS escape attacks). On the other hand, leakages at OS level in most of the cases apply also to virtualized OSs.

3.5.3. Threats

We now discuss the threats that can be mapped to the modern system asset taxonomy presented in the previous section. Details on attacks exploiting vulnerabilities linked to the identified threats are reported in Appendix A.3. CSA in its "Top Threats to Cloud Computing: The Egregious 11" of the 2019, surveyed industry experts on security issues in the cloud industry in order to rate 11 salient threats, risks and vulnerabilities. The most prominent outcome is that compared to the previous CSA report, traditional cloud security issues under the responsibility of cloud service providers (CSPs), such as denial of service, shared technology vulnerabilities and CSP data loss, and system vulnerabilities are no more ranked as important for the Cloud user perspective. This suggests an increased maturity of the cloud user understanding of the cloud, on one side, but should not lower the attention on such threats from the CSP perspective. It is interesting to note that the top threats reported are more in the area of potential control plane weaknesses and limited cloud visibility. Misconfiguration and inadequate change control, for instance, are ranked at position number two. Misconfiguration is the leading cause of data breaches in cloud. Also, absence of an automatic proactive change control is perceived as another risky weakness.

Our threat taxonomy is a consolidation of threats previously considered in other documents/reports and is composed of the following categories.

- TG3.1 – Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional security leakage due to human errors.
- TG3.2 – Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties (including cloud internal communication channels). This TG, depending on the circumstances of the incident, could, also, be linked to TG3.5.
- TG3.3 – Poisoning: This group includes all the threats due to configuration/business process poisoning and aiming to alter system behaviors (i.e., at any layers).
- TG3.4 – Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure at any layers like management hijacking and identity fraud.
- TG3.5 – Legal: This group provides for threats resulting from violation of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law. Section 4 of the present document will discuss aspects of this TG.
- TG3.6 – Organisational threats: This group includes threats to the organizational sphere.

Threat Group TG3.1: Unintentional damage/loss of information or IT assets

Threat T3.1.1: Information leakage/sharing due to human errors

Human errors are among the most critical threats in today ICT environment. These threats are accidental, meaning that they are not intentionally posed by humans, and are due to misconfiguration, clerical errors (for example pressing the wrong button), misapplication of valid rules (poor patch management, weak passwords), and knowledge-based mistakes (software upgrades and crashes).

According to IBM X-Force Threat Intelligence Index of 2018,[60] misconfigured cloud servers, networked backup incidents and other improperly configured systems were responsible for the exposure of more than 2 billion records, or nearly 70% of the total number of compromised records tracked by X-Force in 2017. In the 2019 report, IBM reported that publicly disclosed misconfiguration incidents increased 20% year-over-year. Human errors at virtualization level can be even more dangerous and complex to be identified (e.g., wrong VM images management/cloning).

Examples of attacks at virtualization level are available in Threat T3.1.2. They are related to wrong internal processes, but similarly they can be due to human errors in configuring them or to human mistakes.

Assets: "Data", "Infrastructure".

Threat T3.1.2: Inadequate design and planning or incorrect adaptation

Inadequate design and deployment, including adaptation, of a modern cloud-based system can result in threats to managed data. As an example, migration to the cloud requires a careful design and planning to preserve security during and immediately after the migration. This means the implementation of appropriate security architecture to withstand cyber attacks. Unfortunately, this process is still not well perceived by the company leading to a series of security incidents. The main reason is that organizations implement a "lift-and-shift" cloud migration, simply porting their existing IT stack and security controls to a cloud environment. Similarly, weak control plane while designing a full cloud solution may cause severe issues. In virtualized environments, several processes can be affected by intrinsic vulnerabilities due to their peculiarities. For instance, migrations are needed for balancing the workload, but open security issues while migration is in progress. Other virtualization-specific processes that can be affected are VM rollback and VM cloning.

This threat refers to business process design. It also shows some similarity with business process failure (T3.4.6) and business process poisoning (T3.3.2), but it is due to unintentionally wrong design. If the process refers to moving, cloning, or copying VM files, then it can be linked to unauthorised acquisition of information (T3.2.2 as well). Due to this connection, some of the following attacks can be considered as examples also for other threats.

Assets: "Middleware", "Management", "Infrastructure".

[60] IBM X-Force Threat Intelligence Index https://www.ibm.com/security/data-breach/threat-intelligence

Threat Group TG3.2: Interception and unauthorised acquisition

Threat T3.2.1: Interception of information

It considers an attacker intercepting a communication between two communicating links. Inter-node communication with cloud components is often unsecured by the default configuration, it is possible to hijack a user session or gain unauthorised access to services in social networks, and communication protocol flaws can result in data breach.

Cloud Stacks software distributions (for example Open Stack) do not always use protocols for data confidentiality and integrity between communicating applications (e.g., TLS and SSL) and are not always configured properly (e.g., changing default passwords). In addition, this effect is further exacerbated in complex layered environments based on virtualization, because they permit cross-inspection of various tenant's data flow, as well as topology inference that could serve to set up several attacks. Meltdown and Spectre, for instance, are two CPU-level vulnerabilities that can be exploited to create a side channel focused on deducing the content of computer memory. These vulnerabilities can be exploited even in virtualized environments, leading to an even more serious security risk, given the sharing of physical resources among multiple tenants.

VM network traffic sniffing/spoofing are among the most critical threats in virtualization. Privilege domain processes like management interface can intercept all network traffic before it gets to the unprivileged user domain. The network traffic of a particular VM can be sniffed to read the communication or to perform traditional MITM attacks. Even if extremely difficult (i.e., the target and the attacker must be executed on the same core), virtualization permits a more low-level interception of information at cache level (both L2 and L1) due to the sharing of the same hardware resources. For instance, a side-channel attack on L2 cache. This threat is strongly connected also with network-centric domain in Section 3.4.

Assets: "Network", "Compute Nodes", "Management Server/Console", "Access Control/Authorisation".

Threat T3.2.2: Unauthorised acquisition of information (data breach)

Unauthorised acquisition of data following data breaches is an important threat,[61] which is the main focus of Section 3.6, where data is the main asset. However, in cloud/virtualized environments, data breaches have some peculiarities that are worth to be discussed in this threat. In virtual/cloud environments, where physical resources are shared between tenants, there may be a set of behaviors that result in the unauthorised acquisition of information. For instance, exposure via scavenging in virtualized environments is even more serious [16] than in physical systems. In general, the physical sharing of virtualization or the logical sharing of the cloud enhance the severity of accessing to unauthorised data.

Assets: "Data".

[61] Europol, Internet Organised Crime Threat Assessment (IOCTA), Strategic, policy and tactical updates on the fight against cybercrime
https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

Threat Group TG3.3: Poisoning

Threat T3.3.1: Configuration poisoning

Configuration poisoning is a serious threat in complex environments such as cloud and virtualized data centers. [62] It is sometimes called deliberate/intentional misconfiguration. It is very difficult to detect and shares similar impact as unintentional misconfiguration. In most of the cases, it implies a malicious insider. F5 Labs researchers study the breaches due to intentional insecurity and the growth rate from 2017 to 2018 was an alarming 200%.[62] For instance, one poisoning activity can be related to modification of firewalling service (i.e., web Application Firewall) configuration, to avoid deep packet inspection on certain port. Several configuration poisoning activities targeted the audit mechanisms or cloud console monitoring system to hide the attacker activities (e.g., the log system poisoning). [63]

Configuration poisoning shares technical similarities with misconfigurations due to human errors, but it differs from it for the fact that poisoning is intentional, and it brings in most of the cases to an invalid configuration that provides an advantage for the attacker. On the other hand, misconfiguration (mistake) is not intentional, but still difficult to be discovered yet less difficult than the intentional ones. Configuration poisoning can be either the effect of an external attack or of a malicious insider attack. For this reason, it has a strong link with other threats of TG3.4. Poisoning can be focused to produce a configuration that exposes the server to attacks. However, since intentional, the type of configuration modification is much more complex to be detected that misconfiguration, mainly due to the fact that the attacker wants to hide herself as well as to hide the fact that something is not well configured.

Assets: "Middleware", "Management", "Infrastructure", "Security Mechanisms".

Threat T3.3.2: Business process poisoning

It refers to what is also called Business Process Compromise (BPC), an attack that silently alters parts of specific business processes, or machines facilitating these processes, to generate significant monetary profit for the attackers. According to Trend Micro, 43% of surveyed organizations have been impacted by a BPC.[64] In most of the cases, the business process is implemented at application level, but it can also be associated with internal cloud or virtualization business process related to automatic or programmable activities. In case of VM relocation, for instance, to handle load balancing, the target location server can be altered to a weaker configuration where memory copy protection can be disabled.

This threat relates to inadequate design and planning or incorrect adaptation threat T3.1.2, but with the difference that this is an intentional alteration of working business process. It is therefore also connected with malicious insider threat T3.6.2 that can more easily alter business process from inside. In addition, in many cases,

[62] Intentionally Insecure: Poor Security Practices in the Cloud https://www.f5.com/labs/articles/cisotociso/intentionally-insecure--poor-security-practices-in-the-cloud

[63] Hybrid Cloud Security Best Practices Focus On The Five C's: Console, Configuration, Connectivity, Cloud Data, And Containers https://cyberdefense.orange.com/wp-content/uploads/sites/9/2019/09/forrester_report_hybrid_cloud_security.pdf

[64] Half of management teams lack awareness about BPC despite increased attacks https://www.helpnetsecurity.com/2018/12/07/business-process-compromise/

it is obtained via poisoning of configurations of the business process T3.3.1. In cloud and virtualization, most of these alterations are malicious alterations of business process configurations.
Assets: "Middleware", "Management", "Infrastructure", "Security Mechanisms".

Threat Group TG3.4: Nefarious activity/abuse

Threat 3.4.1: Identity fraud

Identity handling may be more difficult due to the more complex and stratified hierarchical administration of privileges of the different layers down to the virtual one. As an example, at the virtual network level, when aggregating virtual networks into a federation, issues of role segregation and policy conflicts may arise, providing room for identity fraud. Moreover, the dynamics of adding and removing entities may be used by malicious entities to gain a new identity, for example, through inconsistencies in the migration process. Replay attacks are also facilitated by shared communication channels, which can be exploited at the virtual router level by replying to old control messages [17]. Concerning repudiation, the disposable nature of VMs, providing log features and the rollback procedures typical of virtualized environments, may have a strong impact on the non-repudiation of actions registered via logging [18]. Cloud adoption introduces multiple changes to traditional internal system management practices related to identity and access management (IAM). IAM must be able to scale and support immediate de-provisioning of access to resources. It must be automated and integrated in the cloud environment. In addition, IAM becoming increasingly interconnected for instance due to federation. In such environment, password theft is even more severe (e.g., network lateral movement attack such as "pass the hash"). In case of legacy system password strength, rotation must be verified since they are still among the mostly common cases of leakages. Similarly, in case of management of cryptographic keys, the handling of keys lifecycle (creation, distribution and deletion) have a fundamental role to reduce breaches. In the cloud, hijacking of cloud service and subscriptions accounts is riskier due to the peculiarity of the Cloud model itself, where data and applications reside in the cloud services.
Assets: "Middleware", "Management", "Security Mechanisms".

Threat T3.4.2: Denial of service

Traditional DDoS is among the main threats to complex systems. They aim to threaten components availability at any of the layers by exhausting their resources, causing performance decrease, loss of data, service outages, on one side, and data availability, on the other side.
In layered environments based on virtualization, this disruption is exacerbated due to the sharing of resources. For instance, physical resource overloading may cause degradation of a virtual network's performance, leading to disruption in communications, especially when the resources are in the same area as the underlying network. We note that this may happen: i) unintentionally during the system's lifecycle (difficult to predict) or ii) maliciously in case of coordinated attacks.
Virtualized environments seek to cope with this severe class of threats by adopting isolation solutions and by promoting fair distribution of resources among all virtualized entities (network entities included). However, these approaches are

difficult to implement due to the intrinsic characteristics of virtualized systems that share computing resources and distribute them (possibly on demand) at runtime.
Assets: "Middleware", "Infrastructure", "Security Mechanisms".

Threat T3.4.3: Malicious code/software/activity

This class of threats usually targets all ICT stack and the six domains addressed in this deliverable. They aim to distribute and execute malicious code/software or execute malicious activities. These threats usually involve malware, exploit kits, worms and Trojans. They exploit backdoors and trapdoors, as well as developers' errors/weaknesses. Malicious attackers can host malware on cloud services. Cloud services that host malware can be perceived as more legitimate because the malware uses the CSP's domain and can use cloud-sharing tools to further propagate itself. Hyper-jacking is a special type of malicious activity that affects hypervisors in virtualized environment. The target is to violate the integrity of the hypervisor to get control over it. Other malicious activities are the VM hopping that allows to jump from a VM to another on the same physical server and VM escape that takes advantages from isolation failures between hypervisor and the VM to gain control of the hypervisor and VMs. Malware-infected VM/container images can be deployed in the relative repositories of images to be used by an attacker when launched on a trusted infrastructure leading to serious security issues.
Assets: "Middleware", "Security Mechanisms", "Virtual File Format".

Threat T3.4.4: Generation and use of rogue certificates

This class of threats usually target all ICT stack and the 6 domains in this deliverable. Certificates are largely used in cloud to make the service working in a trustworthy ecosystem.
Assets: "Middleware", "Management", "Infrastructure", "Security Mechanisms".

Threat T3.4.5: Misuse of assurance tools

Assurance is the way to gain justifiable confidence that IT systems will consistently demonstrate one or more security properties, and operationally behave as expected, despite failures and attacks [5]. Assurance is based on audit, certification, and compliance tools and techniques. The manipulation of such tools and techniques can result in scenarios where the malicious behavior of attackers is masqueraded and is not discovered. Assurance information is necessary to ensure the security of the system during its entire lifecycle from its design to its operation. It is also necessary to guarantee compliance and regulation. This is valid through all the domains but especially for cloud and virtualization it is quite crucial due to the intrinsic lack of transparency [7] [6].
Assets: "Data", "Middleware", "Management", "Infrastructure", "Security Mechanisms".

Threat T3.4.6: Failures of business process

According to ENISA taxonomy, improper business processes can damage or cause loss of assets. In the cloud environment, one of the main causes of this type of threat is the limited cloud usage visibility. There can be two behaviors, un-sanctioned app usage and sanctioned app misuse, which refer to internal company regulations and processes that are not satisfied completely. In case of un-sanctioned app use, employees can use cloud application without any specific permission, any support

for the corporate leading to what is called shadow IT.[65] This behavior is risky when implies insecure cloud services that do not meet the corporate guidelines.
IBM recently found that one out of three employees at Fortune 1000 companies regularly use cloud-based SaaS apps that have not been explicitly approved by their internal IT departments.[66]
An example of shadow IT that causes much more issues than what it was supposed to solve, was the adoption of chat room service for managing a post-attack scenario on a big company. The chat room allows an attacker to learn sensible information about the company due to an unknown vulnerability that was used without alerting the security department.[67]
For the sanctioned app misuse, it is very complex to be detected but still very dangerous and can be connected to external threat actors that impersonalise legitimate internal user. An example of app misuse that is a violation of the company policy is to do a backup on a personal SaaS service.
This threat relates to the lack of security governance/awareness and to the need of having users' behavioral analysis for compliance with company policies.
Assets: "Virtual machine", "Platforms", "Infrastructure".

Threat T3.4.7: Code execution and injection (unsecure APIs)

At virtualization level, it is possible to execute code on hypervisor from a malicious VM via memory modification (heap memory) of hypervisor or to compromise the management interface via its web application exploiting CSS and SQL injection. Cloud applications are built on web service model; APIs can then become a target of attack, and be vulnerable to well-known attacks, such as the Open Web Application Security Project (OWASP) Top Ten list [44] (see Section 3.7). In particular, code execution (e.g., XSS) and injection (e.g., SQL injection) are critical classes of attacks that can increase risks. Cloud computing strongly relies on software user interfaces (UIs) and APIs to allow customers to manage and interact with cloud services. The security and availability of general cloud services are dependent on the security of these APIs. They are exposed at the perimeter and therefore very likely to be attacked. An increasing emphasis was dedicated to how to handle API keys as they are largely used in cloud services.[68]
More specifically for the cloud, CSA identified a meta-structure (i.e., the protocols and mechanisms that provide the interface between the infrastructure layer and the other layers) and an appli-structure (i.e., the applications deployed in the cloud and the underlying application services used to build them) failures as related to the APIs that ignore their existence, for instance, when APIs still use just username and password ignoring the other more advanced offered security features. Similarly, to mitigate appli-structure failures, in 2019, Apple restricted iOS app providers to do screen recording as a means of analytics. Glassbox is one of the most

[65] Gartner predicts that by 2020, one-third of all successful security attacks will come through shadow IT systems.
[66] Bring shadow IT into the light: Discover, assess, approve and educate https://www.ibm.com/information-technology/bring-shadow-it-light-discover-assess-approve-and-educate-0
[67] Shadow IT: Every Company's 3 Hidden Security Risks https://www.darkreading.com/endpoint/shadow-it-every-companys-3-hidden-security-risks/a/d-id/1332454
[68] Insecure API Implementations Threaten Cloud https://www.darkreading.com/cloud/insecure-api-implementations-threaten-cloud/d/d-id/1137550

famous application that was blocked due to this Apple policy. Generic API threats, given their application nature, are threated more in detail in Section 3.7.
Assets: "Middleware", "Virtual machine", and "Platforms".

Threat Group TG3.5: Legal

Threat T3.5.1: Violation of laws or regulations data

Occurrence of a breach of EU and national laws. Depending on the exact form of EU law, certain regulations (e.g. GDPR) are directly applicable across EU Member States, while those in the form of Directive (e.g. NIS Directive) become applicable as soon as they are transposed in the national legal orders of the Member States. Note that, in the occurrence of a breach of law, affected individuals and organizations may seek for remedies both in the national courts, as well as before the European Court of Justice.
Assets: All assets.

Threat Group TG3.6: Organisational threats

Threat T3.6.1: Skill shortage

A possible shortage of skilled system administrators and managers is one of the main threats to complex systems. Lack of skill for virtualized environments, as well as the lack of technical competences on a specific cloud ecosystem, may have a tremendous impact on the entire cloud system. These sectors even if are somehow related to sysadmin area requires specific competences to be acquired to maintain security under control. This threat has a strong link to threat group TG3.1 "Unintentional damage / loss of information or IT assets".
Assets: "Roles".

Threat T3.6.2: Malicious insider

Insider threats can be distinguished in unintentional or malicious insiders. Unlike external threat actors, insiders do not have to penetrate firewalls, VPNs and other security defences at the perimeter. Insiders operate within a company's security circle of trust, where they have direct access to resources. This makes this type of threat very complex to counteract. The Netwrix 2018 Cloud Security Report indicates that 58% of companies attribute security breaches to insiders, including negligence.[69] Being in this privileged position, the insider can be the vector of many other threats, like the ones relative to poisoning TG3.3, but also to nefarious activities TG3.4.
Assets: "Data", "Middleware", "Management", "Infrastructure", "Security Mechanisms".

[69] Cloud Security Risks and Concerns in 2018 https://blog.netwrix.com/2018/01/23/cloud-security-risks-and-concerns-in-2018/

3.6. Data-Centric Security

This section describes an overview of assets and threats in Domain 4 on data-centric security. Details on attacks linked to the identified threats are reported for interested readers in Appendix A.4. It includes an overview of assets and threats that span file system, DBMS, and data warehouse. It then concentrates on the latter evolution in the data domain, namely, Big Data ecosystem.

3.6.1. Context and Architecture

The ability of sharing, managing, distributing, and accessing data quickly and remotely are at the basis of the digital revolution that started several decades ago. The role of data in today's technology is even more important, having entered the, so called, data-driven economy. Data management and inference based on them are fundamental for many enterprises, from micro to large, to make value and compete in the global market, and replaced the central role that was usually owned by communication means. The data domain observed important changes at all layers of an IT chain: i) data layer: from data to big data, ii) database layer: from SQL to NoSQL, iii) platform layer: from data warehouse and DBMS to Big Data platforms, iv) analytics layer: from data mining to machine learning and artificial intelligence. For instance, data mining focuses on discovering unknown patterns and relationships in large data sets. Machine learning aims to discover patterns in data, by learning patterns parameters directly from data; it is composed of a training step and the algorithm is not programmed to manage such patterns. It builds and keeps the model of the system behavior. Artificial intelligence mimics human intelligence and tries to reason on data to produce new knowledge.

In this context, Big Data has recently become a major trend attracting both academia, research institutions, and industries. According to IDC,[70] "*revenues for Big Data and business analytics will reach $260 billion in 2020, at a CAGR of 11.9% over the 2017-19 forecast period*". Today pervasive and interconnected world, where billions of resource-constrained devices are connected and people are put at the center of a continuous sensing process, results in an enormous amount of generated and collected data (estimated in 2.5 quintillions bytes of data each day[71]). The Big Data revolution fosters the so-called data-driven ecosystem where better decisions are supported by enhanced analytics and data management. Big Data are not only characterized by huge amount of data, but points to scenarios where data are diverse, come at high rates and must be proven to be trustworthy, as clarified by the 5V storyline [19]. Big Data are defined according to 5V: i) Volume (huge amount of data), ii) Velocity (high speed of data in and out), iii) Variety (several ranges of data types and sources), iv) "Veracity" (data authenticity since the quality of captured data can vary greatly and an accurate analysis depends on the veracity of data source), and v)"Value" (the potential revenue of Big Data). Big Data has been defined in different ways starting from Gartner "Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization " to McKinsey Global Institute "Big Data as data sets whose size

[70] IDC, Worldwide Semiannual Big Data and Analytics Spending Guide, 2018, https://www.idc.com/getdoc.jsp?containerId=prUS44215218

71 Bernard Marr, How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read, May 2018, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#363f1fcf60ba

is beyond the ability of typical database software tools to capture, store, manage and analyse."

Big Data management and analytics are among the most critical pressing needs for all organisations that want to move their business a step forward. Critical issues still need to be solved to fully support Big Data Analytics diffusion, such as the management of Big Data complexity and the protection of data security and privacy. In particular, the EU H2020 project TOREADOR identified the different hurdles for Big Data widespread adoption [20]. Some of these hurdles are relevant for the threat landscape in this deliverable.

- **The security/privacy compliance hurdle.** Many domains where Big Data can make a real difference (including the ones in WP2, such as, healthcare, transportation) are highly regulated for security and privacy [21] [22]. The peculiarities of judicial space cannot be addressed on a project-by-project basis. Rather, certified compliance of each Big Data analysis process (e.g., in the form of a Privacy Impact Analysis and privacy controls) must be made available from the outset to all actors that use Big Data in their business model.
- **The legal hurdle.** From a legal standpoint, data management, however, raises a series of questions that need to be carefully examined. For instance, how to efficiently grant and protect intellectual property rights? Similarly, how to shape the economical exploitation of data in distributed environments, especially when third parties are involved [23] and furthermore, how to provide evidence that data processing is compliant to norms and directives [24]?
- **The technology opacity hurdle.** While Big Data analytics can in principle support existing or new value propositions in a number of business domains, choosing and deploying the "right" analytics on the "right" computational infrastructure is still more an art than a science or an engineering practice [25] [26],only reachable by big enterprises and affected by lacks of skills/competences.

This quick evolution of the data domain made the need of protecting such data at the centre of the research agenda worldwide. New threats and attacks are emerging, and introduce the need to concentrate on relevant regulatory and security issues, which are discouraging some (small) players by full adoption of Big Data techniques. Security issues include the need of protecting this massive amount of digital information, and in particular data protection and privacy issues, and the protection of the (critical) infrastructure supporting it. A report from Verizon[72] shows that personal data are the biggest category of compromised data (see Section 3.8 for more details), followed by payment data and then medical data.

[72] Verizon, 'Ransomware, botnets, and other malware insights', 2018 Data Breach Investigations Report, 2018, pp. 9.

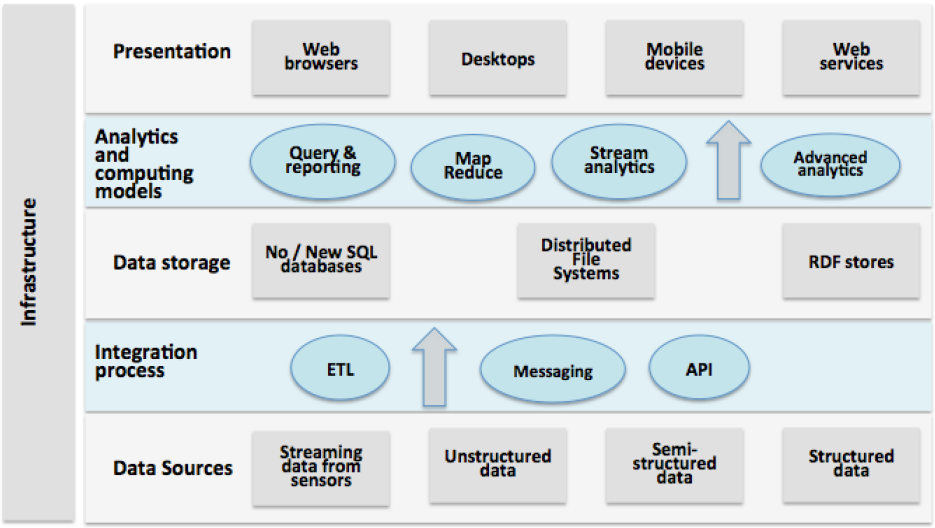


Figure 4 – Layered architecture of Big Data systems (taken from ENISA Big Data Threat landscape https://www.enisa.europa.eu/publications/bigdata-threat-landscape/at_download/fullReport)

In our analysis, we refer to the system-, technology-, and product-independent architecture introduced in the ENISA Big Data Threat landscape[73] as our reference architecture. Figure 4 presents a high-level conceptual model and introduces the terminology used in the following of this section. It specifies common components in 5 layers: "Data sources", "Integration process", "Data storage", "Analytics and computing models" and "Presentation".

- Layer "Data sources" includes all sources of data from smart devices (minuscule sensor as well as bigger devices such as smartphones), to structured information such as relational databases, and to any sort of unstructured and semi-structured data.
- Layer "Integration process" involves all components for collecting and integrating data, provides functionalities for preparing and pre-processing data.
- Layer "Data storage" provides all components and systems including distributed file systems, RDF stores, NoSQL and NewSQL databases, supporting persistent storage of huge data sets.
- Layer "Analytics and computing models" includes all components for analysing and processing data. It specifies the analytics to be computed (e.g., the expected outcome - descriptive, prescriptive, predictive - and the learning approach - supervised, unsupervised, semi-supervised), on one side, and how data are routed and parallelized (e.g., processing type - real-time, near real-time, batch- and expected latency - low, medium, high).
- Layer "Presentation" includes the visualisation technologies, how the results of analytics are organised for display and reporting. For instance, it defines data display type.

3.6.2. Assets

According to ENISA's Guideline on Threats and Assets published in the context of ENISA's Security framework for Article 4 and 13a proposal, an asset is defined as "[...]

[73] Big Data Threat Landscape, ENISA, January 2016, https://www.enisa.europa.eu/publications/bigdata-threat-landscape/at_download/fullReport

anything of value. Assets can be abstract assets (like processes or reputation), virtual assets (for instance, data), physical assets (cables, a piece of equipment), human resources, money". An item of our taxonomy is either a description of data itself, or describes assets that generate, process, store or transmit data chunks and, as such, is exposed to cyber-security threats. In addition to the ENISA Big Data Threat Landscape,[73] a major source of information for this study is the work undertaken by the NIST Big Data Public Working Group (NBD-PWG) resulting in two draft Volumes (Volume 1 about Definitions and Volume 2 about Taxonomy). Another source of information is the report "Big Data Taxonomy", issued by Cloud Security Alliance (CSA) Big Data Working Group in September 2014, where a six-dimensional taxonomy for Big Data, built around the nature of the data, is introduced.

Assets can be categorized in 5 different classes as follows:

- Data – It is the core class and includes all types of data from metadata, to structured, semi-structured and unstructured data, and stream of data.
- Infrastructure – It comprises software, hardware resources denoting both physical and virtualized devices, computing infrastructure with batch and streaming processes, and storage infrastructure with various database management systems.
- Big Data analytics – It includes protocols and algorithms for Big Data analysis, as well as all processing algorithms for data routing and parallelization. It points to the design and implementation of procedures, models, algorithms, as well as analytics results.
- Security and privacy techniques – It refers to all security techniques that are the target for an attacker. These represent the interesting components that would result in unauthorised data disclosure and leakage, if compromised. Examples are security best practice documents, cryptography algorithms and methods, information about the access control model used, and the like.
- Roles - Introduced by the NIST Big Data Public Working Group, it includes human resources and related assets.

Each class can be further refined into different asset categories as shown in the following tables [73].

Table 20 – Assets: Data

Class	Category	Description
Data	Metadata	Schemas, indexes, data dictionaries and stream grammars' data.
	Structured data	Traditional structured data in database records defined following a data model. For instance, a relational or hierarchical schema; structured identification data, as for example users' profiles and preferences; linked open data; inferences and re-linking data structured according to standard formats.
	Semi-structured and unstructured data	It includes logs, messages and web (un)formatted data (Web and Wiki pages, e-mail messages, SMSs, tweets, posts, blogs, etc.), files and documents (e.g. PDF files and Office suite data in Repositories and File Servers), multimedia data (photos, videos, maps, etc.), and other non-textual material besides multi-media (medical data,

		bio-science data and raw satellite data before radiometric/geometric processing, etc.).
	Streaming data	Single-medium streaming (for example in-motion sensor data) and multimedia streaming (remote sensing data streams, etc.).
	Volatile data	Data that is either in motion or temporarily stored. For instance, network routing data or data stored in the device RAM.
	Variable data	Permanent data instances, which may change over time.

Table 21 – Assets: Infrastructure

Class	Category	Description
Infrastru-cture	Software	It includes operating systems, device drivers, firmware, server-side software packages and applications. Applications includes software-as-a-services and functionalities that utilize other assets to fulfil a defined task, such as for example asset management tools, requirements gathering applications, billing services and tools to monitor performances and SLAs.
	Hardware (physical and virtual)	Servers including physical devices and hardware nodes virtualized systems and virtual data center, with management consoles, virtual machine monitors, virtual machines), clients, network devices, media and storage devices, smart devices, Human Interface Devices (HID) and mobile devices.
	Computing infrastructure models	It includes architectures, models and paradigms for data processing. It refers to batch processing, for example MapReduce; real-time/near real-time streaming data, as for example Sketch or Hash-based models; a unified approach supporting both, as for example Cloud Dataflow.
	Storage infrastructure models	It includes architectures, models, and paradigm for storage.

Table 22 – Assets: Data analytics

Class	Category	Description
Data analytics	Data analytics algorithms and procedures	It includes algorithm source code with all parameters, configurations and thresholds, metrics, models. It also includes advanced techniques that streamline the data preparation stage of the analytical process.
	Analytical results	It considers the results of an analytics process, textual or in graphical mode.

Table 23 – Assets: Security and privacy techniques

Class	Category	Description
Security and privacy techniques	Infrastructure security	It considers the security of the distributed computation systems and the data stores, including security best practices and policy set-ups. It also focuses on new IaaS paradigm in the cloud.
	Data management	It considers all documents and techniques presenting the approaches implemented for maintaining and protecting Data Storage and Logs, and documentation relating to granular audits and the tracing of data through its life cycle (Data provenance).
	Integrity and reactive security	It considers endpoint security focusing on implemented practices, techniques, and documents. It focuses on solutions for security validation and filtering, as well as real-time security monitoring, including incident handling and information forensics.
	Data privacy	It includes all techniques for data protection (e.g., encryption, signature, access control) as mandated by law.

Table 24 – Assets: Roles

Class	Category	Description
Roles	Data provider	Enterprises, organizations, public agencies, academia, network operators and end-users providing data to data consumers.
	Data consumer	Enterprises, organizations, public agencies, academia and end-users, consuming data produced by data providers.
	Operational roles	System orchestrators (business leader, data scientists, architects, etc.), Big Data application providers (application and platform specialists), Big Data framework providers (Cloud provider personnel), security and privacy specialists, technical management (in-house staff, etc.).

Most of the categories and sub-categories in the above tables are still relevant for generic data, where Big Data is just a specialization. For example, relational databases are a very typical and common resource in every enterprise infrastructure, not necessarily storing large data volumes. Even when relational databases hold large data volumes, they are often manageable through traditional hardware clusters, appliances and software tools.

3.6.3. Threats

We now discuss the threats that can be mapped to the (Big) Data asset taxonomy presented in the previous section. Details on attacks exploiting vulnerabilities linked to the identified threats are reported in Appendix A.4. In general, threats, such as network outage or malfunctions of the supporting infrastructure, may heavily affect Big Data. In fact, since Big Data has millions of data items and each item may be stored

in a separate physical location, this architecture leads to a heavier reliance on the interconnections between servers. Also, physical attacks (deliberate and intentional), natural and environmental disasters, and failures/malfunction (e.g. malfunction of the ICT supporting infrastructure), since their effects are strongly mitigated by the intrinsic redundancy of Big Data, though Big Data owners deploying their systems in private clouds or other on-premises infrastructure should take these attacks under serious consideration.
Data are compromised at huge rates, more than 25 million records compromised in the first semester of 2018,[74] with an increased cost of 6.4% in 2018. Social media counts the top amount of breached records, while healthcare leads the number of incidents. The average cost of a data breach raised to $3.9 million, while the average number of breached records by country was 25,575, with a cost per lost records of 150$ and time to identify and contain a breach 279 days.[75]

According to ENISA Big Data Threat Landscape,[73] a threat to a Big Data asset can be considered as *"any circumstance or event that affects, often simultaneously, big volumes of data and/or data in various sources and of various types and/or data of great value"*. It can be further divided in Big Data breach when "*a digital information asset is stolen by attackers by breaking into the ICT systems or networks where it is held/transported*" and Big Data Leak "*the (total or partial) accidental disclosure of a Big Data asset at a certain stage of its lifecycle [...] due to inadequate design, improper software adaptation or when a business process fails*". A Big Data Breach involves a malicious attacker behavior resulting in an unauthorised access, while a Big Data Leak involves an honest-but-curious attacker or an observer.
The threat taxonomy is a consolidation of threats previously considered in other documents/reports[40] and is composed of the following category.

- TG4.1 – Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional information leakage or sharing due to human errors.
- TG4.2 – Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, could, also, be linked to TG4.5.
- TG4.3 – Poisoning: This group includes all threats due to data/model poisoning and aiming to picture a scenario that not adhere to reality.
- TG4.4 – Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software.
- TG4.5 – Legal: This group includes threats due to violation of laws or regulations, the breach of legislation, the failure to meet contractual requirements, the unauthorised use of Intellectual Property resources, the abuse of personal data, the necessity to obey judiciary decisions and court orders. We will discuss all these issues in detail in Section 4.
- TG4.6 – Organisational threats: This group includes threats to the organizational sphere.

[74] WP2018 O.1.2.1 - ENISA Threat Landscape 2018
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/
[75] Ponemon Institute's Cost of a Data Breach Report 2019

Threat Group TG4.1: Unintentional damage / loss of information or IT assets

Threat T4.1.1: Information leakage/sharing due to human errors

Human errors are among the most critical threats in today complex environments.[74] [75] [76] These errors cause accidental threats, meaning that they are not intentionally posed by humans, and are due to misconfiguration, clerical errors (for example pressing the wrong button), misapplication of valid rules (poor patch management, weak passwords), and knowledge-based mistakes (software upgrades and crashes).

Assets: "Data", "Infrastructure".

Threat T4.1.2: Inadequate design and planning or incorrect adaptation

Inadequate design and deployment, including its adaptation, of a Big Data platform can result in threats to managed data. For example, data replications, though is often seen as countermeasure to threat T4.4.2, could also represent an attack driver, in case (one of) these replicas (storage nodes) are weak or simply increase the probability of data disclosure and data leaks. As another example, the use of an encrypted storage communicating in a network exchanging data in clear could result in a data leak scenario. The design and deployment of the Big Data platform can then represent a source of threats if not deeply tested and verified. One additional threat related to the design is the lack of scalability of some tools. This threat is also connected to Threat T4.4.2 (Denial of Service)

Assets: "Data", "Big Data analytics", "Software", "Computing Infrastructure models", "Storage Infrastructure models".

Threat Group TG4.2: Interception and unauthorised acquisition

Threat T4.2.1: Interception of information

It considers an attacker intercepting a communication between two communicating parties. It is possible to hijack a user session or gain unauthorised access to services in social networks, and communication protocol flaws can result in data breaches. Big Data software distributions (for example Hadoop, Cassandra, MongoDB, Couchbase) do not always use protocols for data confidentiality and integrity between communicating applications (e.g., TLS and SSL) and are not always configured properly (e.g., changing default passwords).

Assets: "Data", "Roles", "Infrastructure".

Threat T4.2.2: Unauthorised acquisition of information (data breach)

Unauthorised acquisition of data following data breaches is also an important threat,[61] and considers incidents resulting in a compromise or loss of data. In addition, GDPR in Europe is predicted to increase the number of extortion attacks. Attackers will try to extort money with the threat of GDPR penalties deriving from data disclosure.[77]

Assets: "Data", "Roles", "Infrastructure".

[76] Information Leakage, http://projects.webappsec.org/w/page/13246936/Information%20Leakage, 2018.

[77] Trend Micro Security Predictions for 2018: Paradigm Shifts https://www.trendmicro.com/vinfo/my/security/news/threat-landscape/2018-trend-micro-security-predictions-paradigm-shifts

Threat Group TG4.3: Poisoning

Threat T4.3.1: Data poisoning

The increasing development of systems that take decisions on the basis of collected data, as well as inferences based on them, make the trustworthiness of data critical. Data poisoning then becomes a fundamental threat to all system building their processes and activities on data. Data integrity is not the only property to protect and guarantee. Data provenance, non-repudiation, and accountability should also be provided.

Assets: "Data", "Security and privacy techniques", "Data management", "Data privacy".

Threat T4.3.2: Model poisoning

It aims to poison the machine learning models, by poisoning data (Threat T4.3.1) used for the training of the model. The idea is that if an attacker can poison the data used for training, the resulting model will represent a behavior different from the real and correct behavior of the target system.

Assets: "Data", "Data Analytics".

Threat Group TG4.4: Nefarious activity/abuse

Threat T4.4.1: Identity fraud

Identity fraud is the leading type of data breaches.[74] Access credentials are in fact among the most critical data managed by Big Data platforms. They are used to access personal accounts possibly containing highly sensitive information such as credit card numbers, payment and billing details. Personal data are often coupled with profiling data such as user preferences, habits. These data are often used for impersonation fraud, creating big opportunities for identity thieves.[78] In this context, where social networking is in everyday life, social engineering raises back its importance and becomes a basis for new attacks. This threat is mentioned in this section for completeness and further analysed in Section 3.8.

Assets: "Data", "Infrastructure".

Threat T4.4.2: Denial of service

Traditional (Distributed) Denial of Service is among the main threats for complex Big Data platforms. They aim to threaten components availability by exhausting their resources, causing performance decrease, loss of data, service outages, on one side, and data availability, on the other side.

Assets: "Infrastructure".

Threat T4.4.3: Malicious code/software/activity

This class of threats usually target all ICT stack and the 6 domains in this deliverable. They aim to distribute and execute malicious code/software or execute malicious activities that target the confidentiality, integrity, and availability of data. These threats usually involve malware, exploit kits, worms, trojans, and exploit backdoors and trapdoors, as well as developer errors/weaknesses. Malicious

[78] Big data creates big opportunities for identity thieves: see http://www.c4isrnet.com/story/military-tech/it/2015/01/19/big-data-identity-theft/22004695/

software also targets distributed programming frameworks, which use parallel computation, and may have untrusted components.
Assets: "Data", "Software", "Computing infrastructure models".

Threat T4.4.4: Generation and use of rogue certificates
This class of threats usually target all ICT stack and the 6 domains in this deliverable. They aim to use rouge certificates to access Big Data assets and communication links, causing data leakage, data breaches, misuse of brand, and upload/download malware or force updates (see Threat T4.4.3).
Assets: "Data", "Big Data analytics", "Software", "Hardware".

Threat T4.4.5: Misuse of assurance tools
Assurance is the way to gain justifiable confidence that IT systems will consistently demonstrate one or more security properties, and operationally behave as expected, despite failures and attacks [6] [27]. Assurance is based on audit, certification, and compliance tools and techniques [5]. The manipulation of such tools and techniques can result in scenarios where the malicious behavior of attackers is masqueraded and is not discovered. Assurance information is necessary to ensure the security of the system during its entire lifecycle from its design to its operation. It is also necessary to guarantee compliance to regulations.
Assets: "Security and Privacy Techniques", "Data", "Infrastructure".

Threat T4.4.6: Failures of business process
According to ENISA taxonomy,[14] improper business processes can damage or cause loss of assets. This class includes threats to confidentiality (e.g., wrong anonymization) and integrity of data (e.g., wrong management of replicas that can bring to scenarios of Big Data degradation, increasing the risk of inconsistent data). This threat points to threats to business processes in the other domains, especially system-centric security (Section 3.5) and application-centric security (Section 3.7).
Assets: "Data", "Big Data analytics".

Threat T4.4.7: Code execution and injection (unsecure APIs)
Big Data applications are built on web service model; APIs can then become a target of attack, and be vulnerable to well-known attacks, such as the Open Web Application Security Project (OWASP) Top Ten list[44] (see Section 3.7 for more details). In particular, code execution (e.g., XSS) and injection (e.g., SQL injection) are critical classes of attacks that can increase risks. Web Applications attacks and breaches often result in larger data breaches.[79]
Assets: "Data", "Storage Infrastructure models" .

Threat Group TG4.5: Legal

Threat T4.5.1: Violation of laws or regulations
The poor management of legal aspects pertinent to Big Data system can be considered as a threat to the system itself. In this respect, the GDPR and the Free Flow of Non-Personal Data Regulation, for instance, dictate -among others- how organizations are expected to handle personal data, who is ultimately responsible for the protection of personal data in the context of complex supply chains, what

[79] 2019 Global Threat Intelligence Report https://www.nttsecurity.com/gtir

are the associated obligations concerning mixed data sets of both personal and non-personal data and how to mitigate risks (e.g. for profiling). Chapter 4 of the present document will further address certain related aspects under the current and proposed regulatory framework.
Assets: All assets.

Threat Group TG4.6: Organisational threats

Threat T4.6.1: Skill shortage

A possible shortage of skilled data scientists and managers is one of the main threats to Big Data.[80] This threat has a strong link to threat group TG4.1 "Unintentional damage / loss of information or IT assets".
Assets: "Roles".

Threat T4.6.2: Malicious insider

Insider threats are among the most critical security threats, and can involve unintentional or malicious insiders [28]. The view that insider attacks may inflict larger damages than outside attackers is widely shared [28] [29].[81] [82] Their impact is also increasing due to the fact that, on one side, no effective security solutions exist for this threat and, on the other side, the value of data is increasing exponentially. Insiders are in fact authorized users with legitimate access to sensitive/confidential documents, possibly knowing existing vulnerabilities [28]. Malicious insiders have therefore multiple incentives to carry out an attack that ranges from revenge to revenue when sensitive data are at their disposal.
Assets: "Roles", "Data", "Infrastructure Security", "Integrity and Reactive Security"

3.7. Application-Centric Security

This section describes an overview of assets and threats in Domain 5 on application-centric security. Details on attacks linked to the identified threats are reported for interested readers in Appendix A.5. It includes an overview of assets and threats that span the full spectrum of applications. Major sources of information for this study are OWASP[83] and SANS[84] reports. It is important to note that this section does not consider applications providing functionalities for infrastructure/system/network management, which are already discussed in other domains in this chapter.

3.7.1. Context and Architecture

Internet-related technologies have changed the way in which users access services and functionalities. Since the beginning of the Internet era, many applications (e.g., e-mail, web browsing, file sharing) have been distributed through powerful servers available online 24/7 using a client-server approach. At the beginning of 2000s, the advent of service-oriented architectures changed this consolidated scenario, moving

[80] See for example reports from McKinsey https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation and from the Financial Times http://www.ft.com/cms/s/0/953ff95a-6045-11e4-88d1-00144feabdc0.html#axzz3ntU3lM00
[81] R. F. Trzeciak. 2017. SEI Cyber Minute: Insider Threats, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496626
[82] PWC. 2017. Global Economic Crime Survey 2016: US Results. https://www.pwc.com/us/en/forensic-services/economic-crime-survey-us-supplement.html.
[83] OWASP™ Foundation - the free and open software security community, https://www.owasp.org/index.php/Main_Page
[84] SANS Institute, https://www.sans.org/

to a scenario where even client software was delivered and accessed through services and applications available online. In this context, two main approaches have been followed. On one side, SOAP services often considered as "Big Services" implemented custom applications as monolithic components using ad hoc XML-based standards. SOAP services are the evolution of remote procedure call (RPC) and provide custom APIs. Lately, RESTful services have been defined, where all applications are modelled using the standard HTTP APIs and CRUD (CREATE, READ, UPDATE, DELETE) operations. RESTful applications quickly became the cornerstone of what is referred to as "application-driven economy",[85] where business processes are entirely built by composing and coordinating (micro-)services among them. In this context, cloud (and mobile) applications proliferate and are becoming a critical vector of attacks.

Cloud applications implement the Software as a service (SaaS) cloud service model, supporting the component-based development model and developing a generic software as a composition of atomic, independent components. The SaaS model allows consumers to use and compose applications deployed on the cloud. Applications can be accessed remotely, for instance through a web browser or a program interface. The success of this model is due to standard, self-descriptive interfaces that simplify the integration and reuse of single applications. The SaaS user does not control the physical infrastructure, operating system, network, storage, and application capabilities. Users merely manages certain specific application-configuration settings. Today, most of the applications we use are delivered through the cloud, accessed through the web, and rely on HTTP(S) protocol and operations, such as for instance Google Docs, Dropbox and Office365. Most of these applications are built as RESTful services maximising the benefits for the final users, as well as the developers.

A cloud application can be defined as an application operating on the Cloud and absorbing peculiarities of both desktop and web applications.[86] In general, they provide offline mode and rich user experience with no need to local installation. It can be either accessed using the web browser or a native application, with all or part of the computation done remotely.[87] For instance, Dropbox in a web browser leaves all computations to the remote service; GoogleDocs in a web browser permits to execute activities locally if no connection is available; Office365 allows you to continue working on documents locally, even without Internet connection.

We note that in the following we consider cloud applications as inclusive as possible, generalizing to service-based applications (including cloud and web applications).

3.7.2. Assets

According to OWASP TOP 10 2017,[88] risk and threats are continuously evolving as the fundamental technology and architecture of application change. For instance, the advent of microservice architectures, which replaces monolithic applications, come with specific security challenges. The increasing trend in moving functionalities from server side to client side are changing the pace of security assessment and protection.

[85] App economy to grow to $6.3 trillion in 2021, user base to nearly double to 6.3 billion https://techcrunch.com/2017/06/27/app-economy-to-grow-to-6-3-trillion-in-2021-user-base-to-nearly-double-to-6-3-billion/

[86] Cloud App https://www.techopedia.com/definition/26517/cloud-app

[87] What is a Cloud Application? https://www.cloudbakers.com/blog/what-is-a-cloud-application

[88] OWASP Top 10 -2017 The Ten Most Critical Web Application Security Risks https://www.owasp.org/images/7/72/OWASP_Top_10-2017_(en).pdf.pdf

In addition to the OWASP TOP 10 2017, a major source of information for this study is the work undertaken by the SANS institute resulting in CWE/SANS TOP 25 Most Dangerous Software Errors.[89]
Assets can be categorized in 5 different classes as follows:

- Data – It includes all types of application data and metadata.
- Interfaces – Platform and APIs
- Security techniques – It refers to all security techniques that are the target for an attacker. These represent the interesting components that would result in application breaches, if compromised. Examples are security best practice documents, cryptography algorithms and methods, information about the access control model used, and the like.
- Roles - Introduced by the NIST Big Data Public Working Group, it includes human resources and related assets.

Each class can be further refined in different asset categories as presented in the following tables.

Table 25 – Assets: Data

Class	Category	Description
Data	Application data	It includes all data that are managed and exchanged by an application with the internal network and the external world. It ranges from raw data, to final results, via all possible layers of data transformations/analysis.
	Application metadata	It includes all metadata associated with applications, from configurations to credentials.

Table 26 – Assets: Interfaces

Class	Category	Description
Interfaces	Platform interfaces	It refers to the interfaces offered by the platform (including traditional OS) hosting the applications, and used by the application itself to access platform functionalities/libraries.
	Application APIs	It includes all APIs offered by an application to users as well as other services/applications. For instance, it refers to REST APIs, SOAP APIs, and the like.
	Service compositions	It includes all artifacts related to service composition including service orchestration and choreography. For instance, it considers the specific composition workflow, the configuration of the component services, the orchestrator.

[89] CWE/SANS TOP 25 Most Dangerous Software Errors https://www.sans.org/top25-software-errors#_utma=32063036.1074415474.1568715260.1568715260.1568715260.1&_utmb=32063036.10.9.1568715627949&_utmc=32063036&_utmx=-&_utmz=32063036.1568715260.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&_utmv=-&_utmk=42405799

Table 27 – Assets: Security techniques

Class	Category	Description
Security techniques	Platform security	It considers the security of the hosting platform, as well as corresponding service container, the service distributed computation systems, libraries, and security tools, including security best practices and policy set-ups.
	Application security	It considers the security of the specific application, including local protection mechanisms (e.g., firewall, IDS/IPS, anti-virus).
	CIA triad	It refers to all security and privacy solutions and tools for protecting confidentiality, integrity availability of applications and corresponding data.

Table 28 – Assets: Roles

Class	Category	Description
Roles	Application provider	Enterprises, organizations, public agencies, academia, network operators and end-users providing applications to application consumers.
	Application consumer	Enterprises, organizations, public agencies, academia and end-users consuming applications.
	Operational roles	System orchestrators (e.g., business leader, data scientists, architects), application providers (e.g., application and platform specialists), application framework providers (e.g., Cloud provider personnel), security specialists, technical management (e.g., in-house staff).

3.7.3. Threats

We now discuss the threats that can be mapped to the application asset taxonomy presented in the previous chapter. Details on attacks exploiting vulnerabilities linked to the identified threats are reported in Appendix A.5. Our review was driven by the OWASP and SANS generic risk assessment cited in the previous sections. In general terms, threats, such as injection and application malfunctioning, may strongly affect IT in general. In fact, current IT systems are heavily based on applications/services composed at run time and therefore exposed to attacks and breaches. Also, attacks to hosting platforms (deliberate and intentional), failures/malfunctions (e.g. malfunction of the ICT supporting platform) can be important sources of risk.
We introduce the major characteristics of the threat taxonomy, with a special focus on cyber-security threats; that is, threats applying to information and communication technology assets. We also consider threats not related to ICT and caused by humans during their activities.

A threat to application assets can be considered as *"any circumstance or event that affects, often simultaneously, services and applications distributed over the Web"*. The threat taxonomy is a consolidation of threats previously considered in other documents/reports [88] [89] and is composed of the following categories.

- TG5.1 – Unintentional damage: This group includes all threats causing application malfunctioning or loss of confidentiality/integrity/availability due to human errors.
- TG5.2 – Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, could, also, be linked to TG5.4.
- TG5.3 – Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the platform of the victim, as well as public interfaces of the hosting platform and applications.
- TG5.4 – Legal: This group provides for threats resulting from violations of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law. Section 4 of the present document will discuss certain aspects of this TG identified.
- TG5.5 – Organisational threats: This group includes threats to the organizational sphere.

Threat Group TG5.1: Unintentional damage

Threat T5.1.1: Security Misconfiguration

Security misconfiguration is one of the most exploited threats. Cyber attackers often try to exploit unpatched software, use default accounts, or unused pages to gain unauthorised access to systems. The problem can target systems at any layers and give the attacker the possibility of compromising the system and bypassing access control checks. This threat is related to threats in other domains: Threat T4.1.1 and Threat T4.1.2 in Data-Centric Security (Section 3.6.3) Threat T3.1.1 in System-centric Security (Section 3.5.3), Threat T1.1.1 in Device/IoT-Centric Security (Section 3.3.3).

Assets: "Interfaces", "Security Techniques".

Threat Group TG5.2: Interception and unauthorised acquisition

Threat T5.2.1: Interception of information

Interception of information is another important threat that plague the application domain. This threat is horizontal and target all domains involving weaknesses in network communications, system components and devices, data exchange, and users' activities. In this domain, interception of information is mainly due to weaknesses and flaws in the protocols for communication encryption (e.g., SSL). This threat is related to threats in other domains: Threat T4.1.1, Threat T4.2.1, and Threat T4.2.2 in Data-Centric Security (Section 3.6.3), threat T3.2.1 in System-Centric Security (Section3.5.3), Threat T1.2.1 in Device/IoT-Centric Security (Section 3.3.3).

Assets: "Data", "Interfaces", "Security Techniques".

Threat T5.2.2: Sensitive data exposure

Sensitive data exposure is a major plague for applications and is often the results of misconfigurations or weak security protection. Many web applications and APIs do not properly protect sensitive data.[88] Rather than trying to decrypt an encrypted communication, cyber attackers try to intercept it, steal keys, access clear text.[88]

The most common weaknesses concern, not surprisingly, the store/exchange of sensitive data in plain text, as well as how crypto is employed (e.g., weak key generation and management, weak algorithm). This threat results in common sensitive data leakage and breach (see Section 3.6.3) both for data in transit and at rest. This threat is related to threats in other domains: Threats T4.1.1, T4.2.1, T4.2.2, T4.4.4 in Data-Centric Security (Section 3.6.3), as well as T5.1.1 and T5.1.2 in this section.
Assets: "Data", "Security Techniques", "Roles".

Threat Group TG5.3: Nefarious activity/abuse

Threat T5.3.1: Broken authentication and access control

Broken authentication and access control allow an attacker to compromise an application and often the entire system hosting it. As a consequence, a bug in the application functions implementing authentication and session management, as well as access control, result in catastrophic consequences, allowing attackers to compromise passwords, keys, or session tokens, assume other users' identities.[88] Restrictions on authorisations are also not properly enforced. Access control weaknesses are similar and permit unauthorised operations affecting confidentiality and integrity of data and applications.
Assets: "Data", "Security Techniques", "Roles".

Threat T5.3.2: Denial of service

Denial of service has been extensively discussed in both device/IoT-, network-, system-, and data-centric security (Sections 3.3.3, 3.5.3, 3.6.3). One of the main targets of denial of service is applications for a variety of reasons, economic, political, ideological, and the like. This threat is related to threats in other domains:
Assets: "Data", "Interfaces", "Security Techniques", "Roles".

Threat T5.3.3: Code execution and injection (unsecure APIs)

Code execution and injection are common threats for applications. Unsecure APIs are supporting criminals in their malicious activities since the advent of Internet and are increasing in importance since the advent of distributed services. The relevance of this threat has been already shown in the previous sections, due to the fact that today any systems or data management platform are accessible as a service through APIs. This threat is related to threats in other domains: Threat T4.4.2 in Data-Centric Security (Section 3.6.3), Threat T3.4.3 in System-Centric Security (Section 3.3.3), and Threat T1.4.3 in Device/IoT-Centric Security (Section 3.3.3).
Assets: "Data", "Interfaces", "Security Techniques". .

Threat T5.3.4: Insufficient logging and monitoring

This threat supports criminals in going undetected. It reduces the performance of intrusion detection and attack identification, decreasing the response and remediation effectiveness.[88]
Assets: "Data", "Interfaces", "Security Techniques".

Threat T5.3.5: Untrusted composition

This threat subsumes many other threats in this deliverable focusing specifically on composite services. Composite services in fact orchestrate atomic services to provide advanced functionalities. This composition, however, introduces new risks

that go beyond the risks of atomic service [27] [30]. First of all, composite services could result in a compromise due to combined information they have access to. Then, the composition of strong atomic services does not result in a strong composite service. Afterwards, the strength of a composite service is the strength of the weakest atomic service. Finally, multiple communications and storages need to be protected at time.
Assets: "Interfaces".

Threat Group TG5.4: Legal

Threat T5.4.1: Violation of laws or regulations
Taking, also, into account the discussion above on violation of applicable laws, it can be argued the most relevant laws in this case are the GDPR and the Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) to be further elaborated under Chapter 4 of the present document. National laws of Member States can certainly apply, but those are, essentially, left outside the scope of this deliverable.
Assets: All assets.

Threat Group TG5.5: Organisational threats

Threat T5.5.1: Malicious insider
As already discussed in Threat T4.6.2 in Section 3.6.3, insider threats are among the most critical security threats to be faced, and can be distinguished in unintentional or malicious insiders [28] It is quite shared the view that insider attacks may inflict larger damages than outside attackers [28] [29].[81] [82] Their impact is also increasing due to the fact that, on one side, no effective security solutions exist for this threat and, on the other side, the value of data is increasing exponentially. Insiders are in fact authorized users with legitimate access to sensitive/confidential documents, possibly knowing existing vulnerabilities [28]. Malicious insiders have therefore multiple incentives to carry out an attack that ranges from revenge to revenue when sensitive data are at their disposal.
Assets: "Roles", "Data", and assets "Platform Security", "Application Security".

3.8. User-Centric Security

This section describes an overview of assets and threats in Domain 6 on User-centric security. Details on attacks linked to the identified threats are reported for interested readers in Appendix A.6. Here the term *users* refers to human users of information technologies in a professional context. We do not include software systems mimicking human users (e.g., bots, autonomous agents) and also, in the classification of security threats and attack samples, we exclude home users engaging in recreational personal usage of information technologies. Rather, we specifically categorize assets according to a typical industrial scenario and, equally, threats as perceived from a company's perspective. In general, users may have the double role of perpetrator of a threat (e.g., a threat is carried out by human actions) or victims (e.g., individuals are the asset targeted by a threat). Therefore, what should be reasonably included in the user-centric security domain? Individuals as perpetrators or as victims? There is not a clear-cut answer, especially considering that users as perpetrators of security violations are necessarily considered in other domains too, and several semi-automated attack vectors, such as botnets, are operated by humans. Furthermore,

humans are responsible for all kind of cybercrimes, at the end even social bots used in frauds have been designed by humans and provide illicit benefits to some humans. The same for humans as victims. For most security incidents, the consequences are likely to impact humans. Systems experiencing downtime, malicious applications, compromised IoT networks likely have a negative impact on human activities. Therefore, some more stringent criteria should be adopted. In this section, the overall criterion is to discuss threat groups as related to user-centric security when:

- individuals responsible for a threat could be referred to users of a corporate network and systems (e.g., we include employees whose laptops are stolen);
- the threat has a relevant and direct impact on users (e.g., we exclude indirect consequences of a security incident, but we include the so-called "CEO frauds");
- the threat's social nature is the key factor for analysing the impact (e.g., goal and motivations of organized criminal groups or state-sponsored actors are key for several large threat categories);
- the threat has a relevant social impact (e.g. we consider threats to brand reputation, smearing campaign, misinformation, social responsibility)

In all, what we want to present is an analysis having a special focus on relevant aspects of the threat landscape directly involving the human factor.

3.8.1. Context and Architecture

The user-centric domain focuses on humans as valuable assets, and for this reason targets of threats and victims of cybersecurity incidents, and on humans as criminals exploiting ICT technology to perpetrate cybercrimes. Our point of view, as already mentioned, is the one of cybersecurity professionals working in an industrial context. Therefore, in particular with respect to cybercrimes, our focus is on categories that may directly affect company's assets and cybersecurity practices and procedures. It is important to explicitly specify the approach, because Users as a domain (or the *Human Factor* of cybersecurity, as sometimes it is called) could be analysed from the points of view of different disciplines and approaches. Studies from the Criminology and Sociology fields have often discussed criminal behavior in online contexts and making use of digital technologies. Those are valuable contributions to the understanding of these phenomena, but we will consider them only marginally, otherwise the discussion will take us too far from our mostly technological and professional-oriented perspective. The raise of organized crime groups and of state-sponsored adversaries, instead, are important for our analysis, because clearly correlated with specific industrial targets and threats. Users are often the target, direct or indirect, of attacks. In a professional setting, top and middle management, employers, and collaborators are targets of cybersecurity attacks for their role in the organization, their knowledge, and their privileges. The role of users as indirect targets has been also considered in other domains of this section. In many incidents aimed to access corporate's data or resources, users play an important role, for example, as first contact point and vulnerability between the adversary and the company. We do not discuss again those cases here.

Instead, we focus more specifically to *human errors*, as a specific class of threats strongly characterized by users' behavior. Human errors, as a specific category, has been studied in disciplines where errors very likely lead to dramatic consequences, such as in transportation, in the military context, and in general for industries working in hazardous situations and critical scenarios. With respect to cybersecurity, many times, human errors concerning IT technology just lead to small or negligible consequences or represent a systematic recurrence that needs to be managed but does

not represent a catastrophic unforeseen scenario. However, what is important to note is that the risk of catastrophic consequences from human errors is increasing with the increasing reliance on IT technologies in many industrial sectors, such as financial services, data management, manufacturing, information, and the public sector. Even industries traditionally not IT-intensive, such as entertainment and accommodation, have experienced severe cybersecurity incidents due to human errors. The other related observation is that it is rare that in IT systems the single human error leads to a catastrophic outcome. A chain of events, procedures, decisions, and errors is usually the real cause, with the single human error as just one of the failures bringing to the adverse consequence.

Another relatively new class of threats that heavily involves the Users domain and whose importance is increasing regards the role of social media, in particular, in the amplification of information about incidents, errors, losses, opinions, and reputation regarding a company. The amplification effect of social media is a threat to a company, because an apparently minor problem might become a major incident in the public opinion. Also, it is a threat because media/social media could be manipulated for distorting the market, or could be effective vectors of misinformation or smear campaigns against a company or some of its most representative individuals. These media-driven market manipulations and public-opinion disinformation campaigns have become even more relevant in recent years because, on one side, an increasing share of the population is getting news primarily from social media; on the other side, the ability to spread fabricated information on social media, possibly with the help of software agents, has improved, either for commercial or political goals.

The full recognition and ability to manage human-centric threats by the information security community is complicated by several hurdles.

- **Analysis and Modelling hurdle**. Considering human-centric threats, it is difficult to analyse them in pragmatic terms, including the ability to describe, decompose, and classify, and reproduce them in a form useful for quantitative analyses, graphical or numerical simulations, or coding into algorithms. Reasons for this difficulty ranges from the lack of familiarity with appropriate models and methods to describe behaviors, the multidisciplinary nature of the threat and the need of cross-disciplinary skills and teams, as well as the fundamentally different methodologic nature of the analysis and modelling approach that a user-centric threat requires with respect to purely technological threats.
- **Quantification hurdle**. Tightly connected but different in nature from the previous is the hurdle given by the difficult quantification of everything connected with user-centric threats. When the security threat has to do with or depend on decision criteria, errors, cognitive bias, gullibility, skill shortage, novelty or even paradoxical side effects of expert judgement, in short on people's behavior, measurements and data collection are complicated and often result in poor quality data. This inevitable problem has greatly impaired the development of quantitative models of risk in information security, of simulation frameworks, and dynamic non-linear models of systems under attack.
- **Cultural and Education hurdle**. The inclusion of user-centric threats indeed represented a cultural leap in the information security field, traditionally based on the two pillars of Engineering and Computer Science. User-centric threats require different skills and expertise, also a different mentality, not just familiar with behavioral issues, but, perhaps more important, with uncertainty and

stochastic phenomena. Again, this clash of different cultural approach is very evident in for risk analysis, which traditionally has been developed on quantitative, probabilistic models and methods, and instead in information technology and security is largely based on qualitative approaches and almost never adopts stochastic models. How to fill this cultural gap is still unclear, despite the many suggestions for designing comprehensive academic curricula and training initiatives.

- **Organizational hurdle**. As a cascade effect of previous hurdles, another difficulty related to user-centric threats is produced on organizations. Identify, measure, analyse, and manage user-centric threats often has a diffuse impact on organizations, because it can involve different branches, from human resources to operations, information systems, legal, marketing, up to the C-level. This may easily produce conflicts, for example when stricter rules have to be enforced, or control measures and so forth. It also may negatively affect the performance of personnel, to this end there are many historical examples of solutions to security problems involving the personnel and how day work is performed that backfired and secondary negative side effect were produced.

3.8.2. Assets

Assets can be categorized in 3 different classes as follows:

- Internal/affiliated – This class groups asset categories that typically reflect the roles of individuals in the company. The four categories have clear distinct features: whether or not they are mostly victim of targeted attacks, the odds to be involved in security incidents or to be responsible of insider threats and so on.
- External – External assets are both individuals and legal person, and represents the stakeholders not included in company's operations and processes. They are the customers and the suppliers, and those representing different interests, like the owners/shareholders, legal authorities and agencies, and the local community and country.
- Intangible – With this last class, we include two important intangible assets (i.e., neither referred to internal nor external assets), namely the financial market and the public opinion. Both are meta-entities that exert an important role for a company and could possibly be influenced by the consequence of a security incidents.

Each class can be further refined in different asset categories as shown in the following tables.

Table 29 – Assets: Internal/affiliated

Class	Category	Description
Internal/ affiliated	Directors/ C-level	It includes the higher ranked people in an organization/company, those typically with decisional authority, for example to green-light purchases or expenditures (e.g., wire transfers, etc.), and with knowledge of sensitive/key business or financial information (e.g., S&A, partnerships, contract signing, etc.). Targeted attacks to these apical positions are the norm.

	Employees/ non-ICT	It includes common employees and mid-level managers not specifically trained or experiences with ICT threats and incidents. This category usually turns out in the statistics as more likely to be victims of security incidents (e.g., phishing, pretexting, ransomware, social engineering, etc.). In special cases, common employees might be in critical roles, for the information or privileges they have (e.g., staff personnel), and for this reason victims of targeted attacks.
	Employees/ ICT	It includes common employees and mid-level managers specifically trained or experiences with ICT threats and incidents. This category should be less exposed to common cybersecurity threats and better informed. However, in this category there are key professional roles (e.g. system, database, or network administrator) possibly victims of targeted attacks or, on the opposite, representing the most common source of insider threats.
	Consultants/ contractors/ business partners	It includes all non-employed personnel with some form of access privilege to company's assets. It is a heterogeneous category, which, depending on the specific role, may share characteristics with non-ICT or ICT employees.

Table 30 – Assets: External

Class	Category	Description
External	Suppliers	Suppliers represent an asset for a company because the failure of the supply chain could produce severe consequences. Therefore, an attack to one or more suppliers may provoke the disruption of the supply chain or other commodity services (e.g., energy distribution). On the other side, an attack to the company may have as a cascading effect on suppliers' equipment or processed, with possible liability. Users to consider is, for these reasons, also suppliers' personnel, which may propagate to the company the effect of a human error or a cybercrime they have suffered, or, vice versa, if the error or the cybercrime have been committed in the company's premises.
	Customers/ user base	Customers are evidently one of the primary User-related assets for a company. Failing to deliver a service, interruption of the production, downtime of online availability and presence, loss of reputation, perceived quality drop, unethical behavior and so forth may threaten the loyalty of the user base/customers, with unpredictably catastrophic consequences.
	Authorities/ agencies/	In this category, users are mostly legal person, but nevertheless they are stakeholders with respect to a company. Liabilities, breaches of law and regulations,

	institutions/ unions	breaches of employers' rights or contractual obligations are some of the possible consequences of an IT incident.
	Owners/ shareholders	Owners and shareholders are obviously stakeholders whose interests a company's management largely depends on. The owners and shareholders are assets to be protected also from adversarial market manipulation strategies, including smear campaigns and disinformation on social media.
	Local/ regional/ national community	This category includes the environment where a company operates, being it the local community, the region, the country or a supra-national body (e.g., the European Union, the federal state). In all cases, the company very likely has a social responsibility with respect to public investments that have favored the company (e.g., infrastructural investments, subsidizes to sustain occupation, etc.) and with respect to the families and the communities of its employees.

Table 31 – Assets: Intangible

Class	Category	Description
Intangible	Market evaluation/ share	This category represents the financial system (i.e., "the market") from which a company depends. Adverse effects of a security incident could easily affect the company's market value.
	Public opinion/ reputation	The public opinion and in general the company's reputation are assets to protect from security incidents, which may lead to a loss of credibility for the company, bad press coverage, accusation of unethical behavior and so forth. As a consequence, this loss of reputation may determine a decrease in customers' fidelity, market evaluation, and possibly access to financial credit.

3.8.3. Threats

We now discuss the threats that can be mapped to the User asset taxonomy previously presented. Details on attacks exploiting vulnerabilities linked to the identified threats are reported in Appendix A.6. Before introducing the major characteristics of the threat taxonomy, a note of caution should be presented because the User domain, of all the cybersecurity domains, is the more recent to be considered as a primary domain of concern and, for this reason and also for the non-technical nature of many related aspects, its scope is still somehow debated or sometimes ambiguously defined. For example, still few years ago, the Health Information Trust Alliance stated that "cybersecurity does not address non-malicious human threat actors, such as a well-meaning but misguided employee." [31] This means that, still recently and, at least, for a relevant organization in one of the key industrial sector, human errors were largely out of the scope of cybersecurity. This would be unconceivable with respect to current cybersecurity analyses, after the User domain has been elevated at the same level of traditional cybersecurity domains such as Systems, Networks, or Data.

On the other side, it is not uncommon today to encounter articles on online cybersecurity-related magazines and in surveys making claims such as "malicious insiders [...] and human error [...] to be the two top cybersecurity threats".[90] These claims, together with the utterly misleading logical fallacy of considering users (or the human factor) as threats (as well as the too often repeated analogy, in technical circles, between users and the weakest link in a chain), grossly overstate and confound threats connected with the User domain, with the aim of shifting the attention of organizations and professionals to the newest hype. Click-baiting editorial styles or commercial interests are likely part of the motivations for such a poor information, but a general lack of understanding and experience with studies on human errors and user behavior connected to IT technologies is equally an important factor.

However, these anecdotes should remind of the fact that the boundaries and the threats of the User domain are still to be regarded as, to some extent, subjective and not yet well established.

More thoroughly conceived and articulated analyses have appeared in recent years raising the attention to the human factor in cybersecurity. For example, NIST, through the Federal Information System Security Educators' Association (FISSEA), has concluded that human errors and negligence often play an important role in chain of events leading to data breaches. Also, security risk management and business operations are often disconnected functions, resulting in a poorly coordinated process management.[91] The Verizon Data Breach Investigation Report (DBIR),[197] a respected annual survey, for the current 2019 edition confirms that the category *Miscellaneous Errors*, while not among the most relevant for security incidents (i.e., security events not resulting in data breaches, such as Denial of Services), it is instead one of the lost likely pattern for data breaches. Interestingly, other categories that could be partially referred to the User domain, such as *Privilege Misuse* (e.g., employees using their system and data access privileges outside their job duties) and *Cyber-Espionage* (e.g., this threat category often adopt deceitful techniques to target specific employees or make use of unfaithful insiders), are relevant. Such results hardly represent a surprise, in fact their relevance is a fact from years.

Many have debated about the importance of the organization for cybersecurity and, to this regard, the expression *Human-centered security* has been used. Holz et al. [32] have presented a detailed research agenda aimed at reorganizing industrial processes of cybersecurity around the role of individuals in all their form, as software developers, IT integrators, system administrators, and end users. Many others, for instance ENISA[92], Corradini and Nardelli [33], and Safa et. al. [34] have addressed the security threats related to users focusing on the perceived need of more and better training of the workforce. The lack of adequate training programs and curricula for cybersecurity professionals as one of the main reason for the gap in available workforce is widely debated worldwide and the subject of several proposals [35] [36] [37].

[90] Human Factor is a Persistent Cybersecurity Threat, Survey Says. *Security Magazine*, August 2019. https://www.securitymagazine.com/articles/90734-human-factor-is-a-persistent-cybersecurity-threat-survey-says

[91] Cybersecurity – the Human Factor: Prioritizing People Solutions to improve the cyber resiliency of the Federal workforce. *FISSEA*. 2017. https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf

[92] ENISA, *Cyber Security Culture in organisations.* February 2018. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Regarding cybercrimes, the User domain is more specifically concerned with identifying whom is responsible, which characteristics they exhibit, and their main motivations and pattern of activity. Two large profiles have emerged in recent years: criminal organizations and state-sponsored groups; the former mainly responsible of financially motivated crimes, the latter mainly driven by cyber-espionage and data breaches. Criminal groups exploit vulnerabilities in existing technologies, as well as the features offered by new technologies, engaging in the traditional arms race with law enforcement and companies' prevention and mitigation solutions. State-sponsored attacks are often framed with reference to cyberwarfare [38] [39]. Despite that reference could be reasonable in certain situations and for specific contexts, however, it often confounds the analysis by focusing more specifically on geopolitical and military issues than on more operational and business-related threats [40]. State-sponsored attacks are mostly related to cyber-espionage; thus, they represent a lucrative activity for the perpetrators and, often, a severe competitive loss for the victims [41] [42] [43]. Therefore, they should probably be more conveniently framed with respect to international market competition and the protection of strategic investments.
Finally, we mention two classes of threats that still are not commonly included in cybersecurity threat taxonomies: threats to a company's market share and threats from amplification effects on media. Analyses of the economic and financial consequences of a security breach have been studied from long [44] [45] [46] [47]. However, it is still an issue that has not entered the mainstream in cybersecurity and requires more and better detailed analyses. In some cases, the actual negative effects, especially long term effects, have been questioned, on the basis of the complex and non-linear cause-effect relationships governing stock prices [48] [49] [50].
The amplification effect of media, traditional or online, with respect to risks and threats is a well-known effect that is still largely ignored in cybersecurity threat taxonomies. On the opposite, it is important to consider, at least as one of the new threat sources to put on a watch list. Episodes where the social amplification of risks, driven by the media, have had relevant effects are discussed in the literature [51] [52] [53] [54].

In summary, a threat to User assets can be considered as *"any circumstance or event that produces adverse effects primarily on individuals as part of an organization or as stakeholders. The threat should be carried out through digital means, either voluntarily (attack/cybercrime) or involuntarily (human error)"*. The threat taxonomy is composed of the following categories:

- TG6.1 – Human errors: This group includes all threats causing unintentional information leakage or sharing due to human errors.
- TG6.2 – Privacy breaches: This group includes all threats causing privacy breaches.
- TG6.3 – Cybercrime: This group includes all threats due to data/model poisoning and aiming to picture a scenario that does not adhere to reality.
- TG6.4 – Media amplification effects: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software (see Appendix A.6 for more details).
- TG6.5 – Organisational threats: This group includes threats to the organizational sphere.

Threat Group TG6.1: Human errors

Threat T6.1.1: Mishandling of physical assets

Physical assets like laptops and disposable data storage are often lost or stolen. In most cases, this event has moderate effects, if any, but it happened that in few circumstances it resulted in severe consequences. This is a typical threat caused by human errors.

Assets: All assets.

Threat T6.1.2: Misconfiguration of systems

System misconfiguration is probably the most typical example of human error. All types of systems are systematically misconfigured, often resulting in small failures, sometimes representing one of the major causes of cyber risks, as witnessed by all security surveys.

Assets: All assets.

Threat T6.1.3: Loss of CIA on data assets

This threat generally refers to data breaches and data leaks, so it mostly refers to the Data domain. However, it often has an undoubtedly human component that makes it worth to be included in the User domain, too. Access privileges are often misused, credentials are managed improperly, and trust is given to someone impersonating someone else or exploiting employees' good faith.

Assets: All assets.

Threat T6.1.4: Legal, reputational, and financial cost

A security incident may have effects that go well beyond the technical domain and production processes. Intangible goods, such as the brand reputation, the financial solidity of the company, and the trustworthiness of the management could suffer some consequences that might be addressed outside the technical competences and mostly by the financial direction, marketing, and the highest company management levels.

Assets: All assets.

Threat Group TG6.2: Privacy breaches

Threat T6.2.1: Profiling and discriminatory practices

In recent years, the US Federal Trade Commission FTC) has actively monitored data brokers practices and its reports have shed a light on such a crucial while elusive industrial segment of the digital society with enormous implications on online privacy. The conclusion of the FTC is disheartened: "*In the nearly two decades since the Commission first began to examine data brokers, little progress has been made to improve transparency and choice*". In Europe, GDPR has introduced severe limitations and fines for commercial profiling, however, it does not seem to have stopped the practice of profiling web users for advertising purposes. Other

discriminatory practices have been conjectured for Internet giants like Google[93] and Facebook.[94]
Assets: "External".

Threat T6.2.2: Illegal acquisition of information
Illegal acquisition of data may happen as a consequence of hacking, of malware exfiltrating information, or of data breaches. is also an important threat, and considers incidents resulting in a compromise or loss of data. This threat represents the typical domain of privacy. Users could be both targets and actors for this threat, depending on their role. The issue has been debated and analysed extensively and has evident cross-domain aspects. Several comprehensive reports and survey are available [55] [56], as well as specific professional skills and profiles.
Assets: All assets.

Threat Group TG6.3: Cybercrime

Threat T6.3.1: Organized criminal groups' activity
As mentioned before, the threat from organized criminal groups has been clearly recognized in analyses produced in recent years as those mostly related to financial gain. The use of malware, botnet, ransomware, and hacking is often related to criminal organizations, which are moving online for their illegal activity. Dark web markets selling illegal goods, private encrypted online chat, and other online forums are new ways for organized criminal groups to extend their business.
Assets: "Internal", "Intangible".

Threat T6.3.2: State-sponsored organizations' activity
Similar to the previous threat, we have already presented the threat connected to state-sponsored organizations as the one mostly related to cyber-espionage. Market competition in key sectors of the economy, such as advanced technology, energy, and innovative manufacturing techniques, has always suffered of industrial espionage. The diffusion of online services and networked systems as enormously increased the possibilities for those willing to access to proprietary data.
Assets: All assets.

Threat T6.3.3: Malicious employees or partners' activity
Threats from insiders have been extensively debated in the last two decades, at least, with alternate emphasis. In some years, the threat from malicious employees reached the hype on specialized press, with someone even claiming that it had exceeded the dangers from outside an organization. More pragmatic studies and surveys, such as Verizon DIBIR, have instead confirmed that despite some fluctuation in the reported cases, the proportion between breaches originated from the inside and those from the outside remained close to the classical 20-80 proportion. Therefore, it never happened a sort of explosion of internal attacks.

[93] David Shepardson and Bryan Pietsch, U.S. states launch antitrust probe of Google, advertising in focus. Reuters, September 2019. https://www.reuters.com/article/us-tech-antitrust-probe/u-s-states-launch-antitrust-probe-of-google-advertising-in-focus-idUSKCN1VU107
[94] Katie Paul and Akanksha Rana, U.S. charges Facebook with racial discrimination in targeted housing ads. Reuters, March 2019. https://www.reuters.com/article/us-facebook-advertisers/hud-charges-facebook-with-housing-discrimination-in-targeted-ads-on-its-platform-idUSKCN1R91E8

What is instead true is that inside attackers are likely to exploit better information and higher privileges, increasing the odds of severe consequences.
Assets: "Internal".

Threat Group TG6.4: Media amplification effects

Threat T6.4.1: Misinformation/disinformation campaigns
This threat group is the less common in cybersecurity threat taxonomies and wants to consider the relevance that media (social and online media, in particular) have in spreading information and amplifying the effect of news in the public opinion, which does not just include laymen, but professionals, business partners, potential customers and investors, and the authorities, too.
Assets: All assets.

Threat T6.4.2: Smear campaigns/market manipulation
Similar to the previous threat, in this case we account for the possibility that a smear campaign is directed towards a company or some representative figures with the aim of manipulating the market, for instance the stock price or a market opportunity.
Assets: All assets.

Threat T6.4.3: Social responsibility/ethics-related incidents
Ethics has been under the spotlight in the last few years, mostly for questionable activities of companies of the so-called "shared economy" and the potential consequences of AI-driven decision technologies. This represents a new cybersecurity threat for organizations, which might be attacked by crafting an incident based on ethical problems. Combined with previous threats regarding online media, the ethics-related issues represent a new form of social responsibility for companies, that should be carefully considered because a negative press or public opinion campaign might have severe consequence on business.
Assets: All assets.

Threat Group TG6.5: Organizational threats

Threat T6.5.1: Skill shortage/undefined cybersecurity curricula
We have previously introduced and discussed about this threat. Skill shortage in cybersecurity is a problem regularly debated in cybersecurity conferences and professional events, because it regards the majority of organizations. New initiatives to standardize academic curricula exist, together with a trend towards professionalization of the role of cybersecurity experts [36][95]. However, it is still not clear and certainly far from a large agreement what should be the core skills of a cybersecurity expert and how to have a larger and better prepared workforce.
Assets: "Internal".

Threat T6.5.2: Business misalignment/shift of priorities
This represent the typical domain of *eGovernment*, where one of the main goals is to keep a constant alignment between IT and business goals and between IT

[95] CyBok, The Cyber Security Body Of Knowledge. Version 1.0, October 2019. https://www.cybok.org/

processes and the corporate strategy. Similarly, a governance of corporate cybersecurity is needed and should be more mature than the present situation.
Assets: "Internal" and "External".

3.9. Key Takeaways

This section summarizes the most important findings, as key takeaway, emerging from the threat landscape carried out in this deliverable. This section, together with asset and threat taxonomies will be made available as a web page and continuously updated to simplify browsing by readers and implement a community-based prioritization of the threats.

- **Endemic persistent threats.** Crosscutting traditional threats, like software bugs, malware, and DoS, which span all over the ICT domains, from OS to networking and applications, are becoming persistent and endemic. Even old vulnerabilities can revive in the context of a new domain not mature enough to consider security as first class requirement. Even advanced architectures must be designed to face security threats, like in the case of 5G services, virtualized operating systems, and layered systems, where a number of countermeasures are used to limit their impact (e.g., sandboxing, isolation). Persistent threats are increasingly exploiting new possibilities given by new assets, platforms, and application domains. For instance, DoS is evolving towards targeting mobile devices and sensors, by speeding up battery consumption, instead of inducing service failures. Mobile devices are becoming a suitable target vector due, for instance, to poor security skills of the users. For instance, stealthy multimedia files can be used to carry out the attack, unrecognized by unexperienced users, instead of more traditional DoS flooding techniques [57].
  Relevant domains: All

- **Balance security and domain-specific constraints.** Not all the domains can adopt the same security countermeasures to deal with cybersecurity risks. There is the need to find a good trade-off between the security level to be achieved, also, as set forth by the associated legal and economic requirements. On one hand, the economic impacts of cybersecurity on the different actors and stakeholders can have important consequences (see Chapter 5 for more details). The assessment of cybersecurity efficiency in terms of economic investments in cyber ecosystems become fundamental to analyse security from a strictly economic point of view, considering that often critically important systems or components have their investments in related security activities neglected. For instance, in IoT, there is an ongoing discussion on the adoption of lightweight cryptography for embedded devices in order to find a balance between security and cost constraints.[96] This reduced cryptography protection quality is not feasible in other domains, where security breaches and data leakages are likely to have severe impacts and a number of persistent threats still exists. The European Regulatory framework provides the basis to respond to cybersecurity threats, also, by allowing in the longer terms the related capacity building across sectors. However, the rapid development of current

[96] The Debate Over How to Encrypt the Internet of Things https://www.wired.com/story/lightweight-encryption-internet-of-things/amp

architectures and infrastructures render it challenging for existing regulations to remain effective for newly introduced regulations to be sufficiently future proof. Nevertheless, the European Regulators have been taking prompt action by amending existing regulations as, for instance, the ePrivacy Directive and by announcing initiatives such as the announcement by the European Commission of new legislation focusing on artificial intelligence.
Relevant domains: All

- **Physical access and insider threats.** Having physical access to assets is a serious insider-related threat and often permits to easily bypass security protections (e.g., in the IoT domain). In general, insider threats are difficult to mitigate, both when an access to critical information with high privileges is granted by software components and when an access is granted to humans/employees. In the latter case, there is the additional difficulty of predicting human behavior and intentions. For the future, it is a common belief that these threats might become even more insidious, especially when human-based (Netwrix 2018 Cloud Security Report indicates that 58% of companies attribute security breaches to insiders). This trend will be further exacerbated in the IoT context thanks to the distributed nature that makes easier to hide the insider activities. Huge effort will be put in the future to identify anomalous human behavior in conjunction to insider threats.
Relevant domains: All

- **Relation between security and safety.** ICT is nowadays permeating every sector and impacts people everyday life. It is clear that there is an increasing connection between cybersecurity and safety, and this will be more and more exacerbated in the future. The impact of IoT cybersecurity on safety for instance is crucial and current trends in adoption of IoT in critical environments such as automotive and UAVs will increase it tremendously. Another scenario where safety is connected with IoT security is health. There is an increasing adoption of IoT devices in hospitals and at the same time very low awareness about the security impact of having critical devices connected to the Internet. In this scenario, there is also a critical privacy concern to be addressed since in most cases hospital infrastructures, even if certified for HIPAA, are not ready to host IoT ecosystems that most of the times share the same networking segment as the rest of the hospital system.
Relevant domains: Device/IoT, System

- **User profiling.** The need of profiling users has a long history in ICT and was grounded on the need of control. It emerges more concretely when linked to business profits. Profiling is also one of the preliminary stages to carry out a cyber attack and to gain an advantage. The profiling capabilities (e.g., using social engineering) will be more and more exploited in the future for attacks preparation and for targeted spam campaigns. The success of smart home IoT devices is enlarging the perimeter exploitable for profiling purposes. Alexa and Google home, to name the ones with the largest user base, are fully connected and powerful devices having as one of their main goals to profile the users. They are also perceived as ubiquitous devices, and this lower the transparency of the interaction with them, increasing the risk due to low awareness. This type of devices is also connected to a powerful AI that will constitute in the

future a new target for an attacker having the objective to lead the IoT to take a wrong decision (e.g., to not recognize a specific face as the one of a criminal).
Relevant domains: Device/IoT, Data, User

- **Diffusion of Ultra-Wideband networks.** The network is the primary attack vector. The more the network is powerful, the more the attack vector is critical. With the adoption of 5G, network slicing will offer differentiated services over the whole network, opening the possibility to provide networking infrastructure as a service. New threats will be introduced from the adoption of network slicing in the context of verticals. Such threats are related to data leakage between multiple virtual environments or slices, bad slice isolation that can result in security resources exhaustion in other slices. Low latency of 5G could allow better coordination among zombies in a DDoS attack scenario and to exploit protocol leakages connected to performance. In the context of IoT, the capillary diffusion enabled by 5G will allow, for instance, an attacker to focus on a specific area covered by a slice, where a large number of compromised devices can interfere with the cellular connectivity leading to a new generation of better localized DDoS.
Relevant domains: Device/IoT, Network

- **Decentralization and computation capability at the edge**. Edge computing is migrating functionality to the edge and with them also security concerns. Some of these concerns shift from a powerful and protected environment to a less powerful and less protected one. This shift needs to be carried out very carefully to provide functionalities without impacting the security features. Edge computing is adopted in many contexts including new incoming ultra wide band networking services. For instance, the access network domain will be impacted by the support of Mobile Edge Computing (MEC) that provides enhanced functionality at the edge of the network. Some sensitive functions currently performed in the physically and logically separated core are likely to be moved closer to the edge of the network, requiring relevant security controls to be moved too.
Relevant domains: Network, Application

- **Increased software and services embedded in networking.** Software is increasingly permeating networking, bringing more functionalities and flexibility, but also enlarging attack surfaces. Software Defined Networks (SDN) and Network Functions Virtualisation (NFV) technologies are moving the traditional network architecture built on specialised hardware and software to virtualized network functions. The consequence is an increased exposure to third-party suppliers and importance of robust patch management procedures. 5G will be based on this ecosystem of networking services. Any software vulnerability will become more significant in this context. In the report about the EU coordinated risk assessment of the cybersecurity of 5G networks,[97] published on 9 October 2019, *core network functions* of the 5G network are underlined as *critical* because affecting the core network may compromise the confidentiality, availability, and integrity of all network

[97] EU-wide coordinated risk assessment of 5G networks security https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

services. Also, *management systems and supporting services* are considered critical assets since they control important network elements and can therefore be used to conduct malicious activity, such as sabotage and espionage. Moreover, the loss of availability or integrity of these systems and services can disrupt a significant portion of 5G network functionalities.
Relevant domains: Network

- **Artificial Intelligence as a booster of cybersecurity attacks.** The adoption of Artificial Intelligence and Machine Learning techniques can substantially expand the attack surface of every domain, permitting to discover vulnerabilities both in software components and in business process logic [58]. Artificial intelligence and machine learning techniques are at the basis of many business decisions and the success of the inferences based on them can result in a huge (economic) value. For these same reasons, they become targets of attacks by cyber criminals. On one side, data poisoning become a huge driver towards more complex attacks. On the other side, model poisoning aims to poison the source of training data in order to fake the learning algorithm in considering a malicious behavior as a normal one. In this context, adversarial machine learning had a huge boost and become a hot research topic, while computation architectures, such as Big data platforms, are enabling these threats on a large scale. An example of how powerful the AI is becoming thanks to the amount of data currently available and the computation capability of the distributed architecture is the current increasing trend of the deepfake.[98] Differently from the past, attackers are targeting people reputation to gain an advantage and to play a scam (e.g., artificial intelligence-generated voice deepfake).
Relevant domains: System, Data, User

- **Social Media and Social Networks Threats.** Social media and social networks represent another source of emerging cybersecurity threat for the user-centered domain. The raise of social bots, that is, automatic software agents disguised as humans, is widely debated, for example in connection with the adoption of Artificial Intelligence methods able to replace humans interacting over social media. However, social bots might become a problem for cybersecurity too, for example in the case of phishing [59], for the spread of disinformation [60] [61], or political propaganda [62]. In general, social bots for social media [63] and Artificial Intelligence for software tools involved in decision processes [64] [65] are widely considered as both a remarkable opportunity and possibly an insidious threat for people, in both cases a challenge for future systems, organizations, and institutions [66].
Relevant domains: System, Data, User

- **Layered and Virtualized Systems.** Current systems are based on several software layers, often including a virtualization layer. In layered systems, the security of the upper layers relies on the security of the lower ones, forming a chain where each layer can be the weakest one. The trend is to increase the

[98] A Voice Deepfake Was Used To Scam A CEO Out Of $243,000
https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#114964a22241

level of sharing and the density of the multitenancy, exacerbating the impact of most of the threats. In addition, weaknesses of traditional systems based on specific OSs will be inherited as well in the context of each layer. Specific threats for the layer protection mechanisms are evolving starting from virtualization and containment escape to cross layer hijacking. In general, containment, isolation, and sandboxing mechanisms will expose vulnerabilities in the future and their exploitation are normally associated to a very high-risk score.
Relevant domains: System, Network

- **Misconfigurations of security mechanisms and lack of transparency.** Given the complex multi-layer nature of current architectures, misconfigurations and in general issues due to the lack of transparency are largely considered as among those with the most severe impact. According to CSA, misconfigurations and inadequate controls will become increasingly problematic especially in cloud environments, as well as weaknesses in authentication, lack-of-control, and visibility, while more traditional threats to confidentiality based on malicious code are becoming less important for cloud and virtualization.
Relevant domains: System

- **Business process compromise.** BPC traditional threats are becoming more and more diffuse nowadays for business process implemented in the cloud. This is possible also due to the advanced AI capabilities of an attacker to improve BPC-based attacks. These attacks are able, for instance, to exploit behavioral information via shadow IT, which is increasing due to the plethora of services that are becoming part of daily activities of employees. The current lack of insurance tools capable to mitigate this behavioral-oriented threat should be addressed in the future.
Relevant domains: System, Network

- **Human errors.** One notable trend is that human interactions with machines, and in particular the proportion of workers whose place of work is strongly intertwined with IT technologies, have increased fast in the last decade, as clearly analysed by the European Agency for Safety and Health at Work [67]. A human mistake is more likely than in the past possibly causing failures in machine-controlled processes, a broad category that includes cybersecurity incidents. The reason is in the frequent presence of human-machine interfaces in business processes as well as in the increasing complexity of digital-physical interactions in workplaces. Often, it could turn out to be mostly (i) a problem of business procedures, (ii) employees under the pressure of a tight schedule or with conflicting requirements between security and productivity, or (iii) even a consolidated usage of a technology, not aligned with original specification, that the company has tolerated (or promoted) along many years [68]. The healthcare is a sector that presents sensible user-centered threats and is often mentioned as one mostly endangered by emerging cybersecurity threats [69]. Not only healthcare personal information of patients is leaked or mismanaged, a type of security incident that hardly could be called "emerging" [70], but also medical devices are considered at risk and increasingly exposed to cybersecurity threats [71].
Relevant domains: All

- **Skill shortage and configuration errors.** Today, single and not-expert users are directly involved in complex business processes and can influence them. Configuration errors are therefore increasing as never seen before, introducing a huge amount of new opportunities for cyber criminals to affect the CIA (Confidentiality, Integrity, Availability) properties of systems and users. For instance, security misconfigurations such as wrong access policies, weak passwords, unpatched systems, and the like, make the overall environment unsecure. Personal data of the users can be stolen and sold on the black market. Entire systems can be hijacked and remotely controlled, while specific sensors/devices put offline by exhausting their resources. Portion of the whole system can be compromised to launch more complex attacks (e.g., Mirai botnet).
  This complexity is even exacerbated when the architecture requires interdisciplinary competences in order to be used, like in the case of a Big Data platform. Privacy implications of Big data processing relate to the computation architecture, as well as with the algorithms, models, and learning peculiarities. The increase in system and platform complexity does not find a counterpart in the skills and competences, resulting in an important lack of data scientists able to properly manage such new technologies.
  Human errors in system configurations are still at the forefront of the issues driving new and old attacks.
  Relevant domains: All

- **Data breaches.** The fundamental role assumed by data in every aspect of our life makes attacks that aim to data breach and leak increasing.[74] In this context, traditional attacks like phishing and (D)DoS are reviving a new boost and mainly target the CIA triad of data. Given the potential huge revenue for attackers stealing data, targeted phishing attacks and malwares have been presented in the last few years. For example, phishing attacks are not aiming at big numbers of compromised users, but rather they target rich individuals, people with access to financial accounts or sensitive business data, or even public authorities that handle PII related data.[74] As another example, malwares mostly target data and in particular unauthorised data wiping, modification, access. They count 30% of all data breaches incidents.[99]
  Moreover, the EU General Data Protection Regulation (GDPR) that became applicable as of May 2018 introduced a series of novelties, including the mandatory reporting of data breaches to the competent authorities, provided that certain requirements are met. Today, a data breach or leakage can become a new weapon in the cybercriminal hands, which will increase the number of extortion attacks with the threat of GDPR penalties deriving from data disclosure. Note that the reporting of security incidents to competent authorities is, also, dictated under then Directive on the Security of the Networks and Information Systems (NIS Directive) that was to be transposed to the national legal orders of the Member States by May 2018.
  Relevant domains: All

[99] 2018 Verizon Data Breach Investigations Report, https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report

- **Applications and software everywhere.** As applications are spreading at all layers of an ICT systems, attacks targeting them are spreading as well. Malware attacks continue to rule the roost, particularly targeting cloud (and IoT) applications. Ransomware are still strong in this area and difficult to challenge by national law enforcement agencies alone. Mobile malware is growing exponentially since 2017, following the increase in the use of mobile systems, such as mobile banking that is overtaking online banking.[61] In this context, it is quite likely that a growth and development of mobile malware targeting users and applications will be observed.
  Relevant domains: Application

- **Complexity of the application deployment environment.** Traditionally, the application deployment environment is considered quite stable. It is handled as a landing platform for the application development. Nowadays, the complexity and dynamics of the surrounding environment are changing this scenario. The increase in platform complexity and the proliferation of many (third-party) libraries open the door to new attacks (e.g., privilege escalation, hijacking, code execution) that threaten not only the platform itself, but also the users relying on it.
  Relevant domains: Application

- **Service miniaturization.** The advent of microservice architecture has increased the revenue for enterprises and supported new businesses, at the same time neglecting non-functional properties such as security and privacy. This scenario represents one of the most important challenges to be faced in the next years. The miniaturization of services and devices (IoT sensors), as well as the pervasive and continuous involvement of humans in the functioning loop, have resulted in an environment with an unprecedented level of risk.
  Relevant domains: Application, Device/IoT, System

- **Cyber-physical systems as enablers of next-generation attacks to users.** Cyber-physical systems have brought changes to several aspects of daily life, like in electrical power grids, oil and natural gas distribution, transportation systems, health-care devices, household appliances, and many more. They could clearly show a relevant user-centered component, either for their development and maintenance, or the consequences of their operation. As often is the case with emerging technologies, they are riddled with security vulnerabilities that could easily become threats to users and individuals [72].
  Relevant domains: Device/IoT, System, User

Table 32 describes the binding between identified key takeaways and corresponding domains.

Table 32 – Key takeaways: Summary

Key Takeaways	Interested Domains
Endemic persistent threats	All
Balance security and domain-specific constraints	All
Relation between security and safety	All
Physical access and insider threats	Device/IoT, System
User Profiling	Device/IoT, Data, User
Diffusion of Ultra Wideband networks	Device/IoT, Network
Decentralization and computation capability at the edge	Network, Application
Increased software and services embedded in networking	Network
Artificial Intelligence as a booster of cybersecurity attacks	System, Data, User
Social Media and Social Networks Threats	System, Data, User
Layered and Virtualized Systems	System, Network
Misconfigurations of security mechanisms and lack of transparency	System
Business process compromise	System, Network
Human errors	All
Skill shortage and configuration errors	All
Data Breaches	All
Applications and software everywhere	Application
Complexity of the application deployment environment	Application
Service miniaturization	Application, Device/IoT, System
Cyber-physical systems as enablers of next-generation attacks to users	Device/IoT, System, User

3.10. Technical Validation

3.10.1. Process

To assess the validity of our findings along the project duration, we define an incremental validation process composed of three main steps. The first step consists of a validation survey distributed to CONCORDIA partners, each involving a respondent that was not directly involved in the deliverable activities. The second step consists of disseminating the survey to organizations outside the consortium (e.g., part of the CONCORDIA stakeholders group), accompanied by a summary (HTML and PDF versions) of our deliverable, in order to retrieve a validation from outside the project. The third step considers the production and dissemination of new material to make the content of this deliverable popularly available (e.g., blog posts, white papers). The validation strategy in D4.1 first involved respondent from within the consortium, who that validated the analysis carried out in T4.1 providing hints and suggestions to increase the quality of findings. In this first deliverable, the interest of project partners in identified threats has been collected to validate their relevance using a survey (see Section 4.2). We also prepared and initially disseminated in a blog post another survey

to collect validation from outside the consortium. We are finally preparing new material to simplify dissemination of our findings, including the blog post already mentioned and an HTML version of the deliverable to simplify access by external readers.

3.10.2. Internal Validation

As already mentioned in Section 1.2, the activities in T4.1 relied on the competences of partners in CONCORDIA, benefiting from their direct contributions in identifying existing threats and major attacks. After the activities around technical aspects of cybersecurity threats were completed, we implemented a first validation of the relevance of the threats identified in Chapter 3. We therefore prepared a questionnaire, where each project partner could rate the relevance of each threat in Sections 3.3-3.8 from 1 (very low relevance) to 5 (very high relevance) in their specific area(s) of business. 30 partners replied to the questionnaire. The survey can be accessed at https://ec.europa.eu/eusurvey/runner/a40a2555-b136-10ad-bf61-b09e4555b33b and is protected with password "concordia". The results are reported below according to the six CONCORDIA domains of interest.

3.10.2.1. Device/IoT-Centric Security

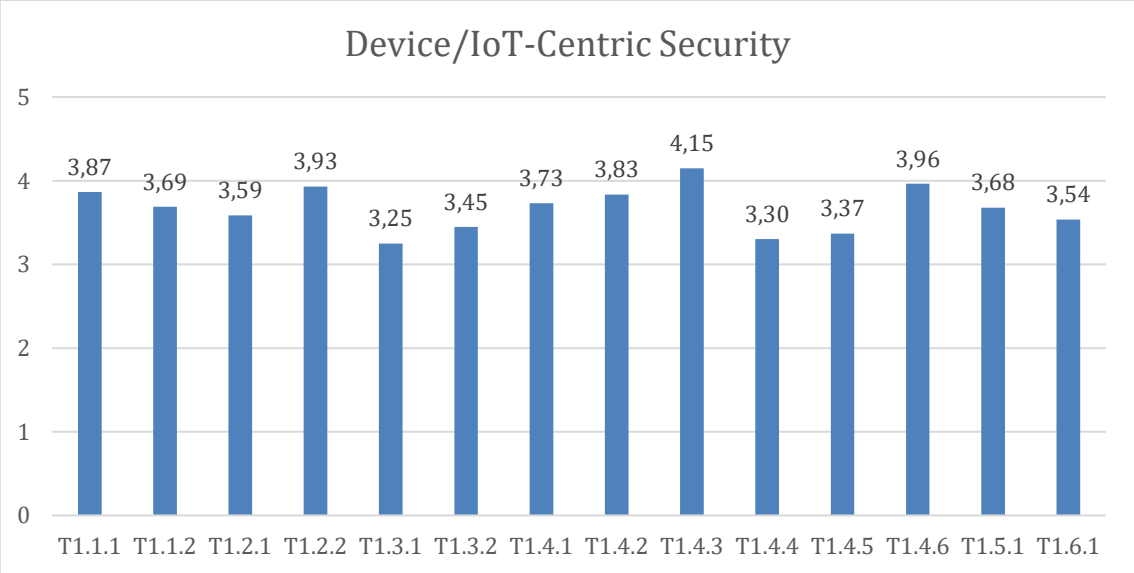


Figure 5 – Threat relevance in Device/IoT-Centric security

Almost all threats fall in the area of High relevance (average score between 3,5 and 4,5 in Figure 5). The three most critical risks are:

- T1.4.3 "Malicious code/software/activity" with average score of 4,15;
- T1.4.6 "Code Execution and Injection (unsecure APIs)" with average score of 3,96;
- T1.2.2 "Unauthorised acquisition of information" with average score of 3,93.

The less critical risks (average score under 3,5) are:

- T1.3.1 "Device modification" with average score of 3,25;
- T1.4.4 "Misuse of assurance tools" with average score of 3,30;
- T1.4.5 "Failures of business processes" with average score of 3,37;
- T1.3.2 "Extraction of private information" with average score of 3,45.

From the results, it emerges that intentional physical damage is the threat group with lower relevance, probably due to the fact that often users have the perception of having the physical assets under control, while they are more worried about the management of data and services. Also, information leakage/breaches, as well as traditional attacks involving DoS, malware, and identity misuse, are considered the most critical especially when devices are involved.

3.10.2.2. Network-Centric Security

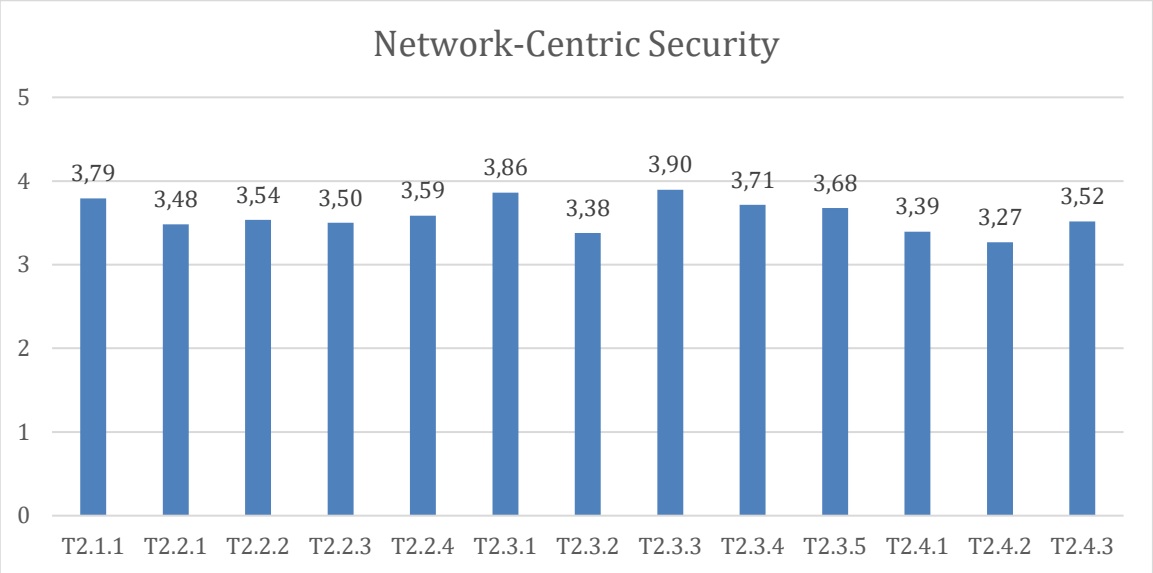


Figure 6 – Threat relevance in Network-Centric security

Almost all threats fall in the area of High relevance (average score between 3,5 and 4,5 in Figure 6). The three most critical risks are:

- T2.3.3 “Malicious code/software/activity” with average score of 3,90;
- T2.3.1 “Exploitation of software bug” with average score of 3,86;
- T2.1.1 “Erroneous use or administration of devices and systems” with average score of 3,79.

The less critical risks (average score under 3,5) are:

- T2.4.2 “Supply chain” with average score of 3,27;
- T2.3.2 “Manipulation of hardware and firmware” with average score of 3,38;
- T2.4.1 “Failures of devices or systems” with average score of 3,39;
- T2.2.1 “Signalling Traffic Interception” with average score of 3,48.

From the results, similarly to Device/IoT Centric security, it emerges that physical threats have lower relevance, while the exploitation of malicious code/tools have higher relevance. In addition, contemporary network complexity makes the erroneous use/administration an important perceived threat.

3.10.2.3. System-Centric Security

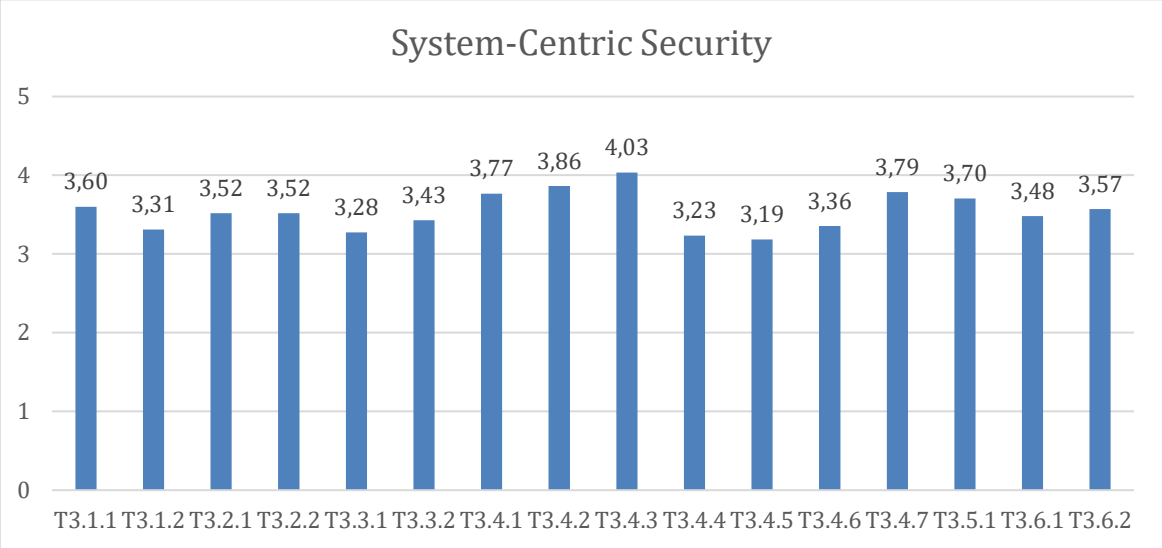


Figure 7 – Threat relevance in System-Centric security

Domain System-Centric security presents two clear clusters, where half of the threats fall in the area of High relevance (average score between 3,5 and 4,5 in Figure 7) and half in the area of Medium relevance (average score between 2,5 and 3,5 in Figure 7). Also, in this domain, as already noted in the previous ones, threats around information leakage/breaches (e.g., T3.1.1) and malicious software (e.g., T3.4.2, T3.4.3) are the most relevant. Legal aspects are also considered relevant with an average score of 3,70.

3.10.2.4. Data-Centric Security

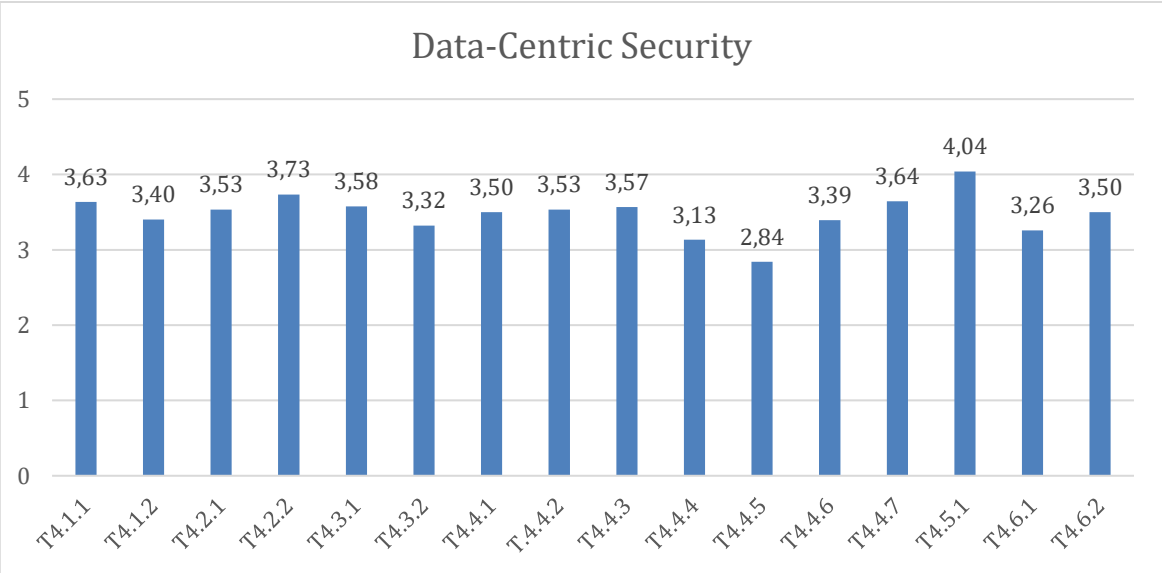


Figure 8 – Threat relevance in Data-Centric security

Many of the threats (62,5%) fall in the area of High relevance (average score between 3,5 and 4,5 in Figure 8). The three most critical risks are:

- T4.5.1 “Legal” with average score of 4,04;

- T4.2.2 “Unauthorised acquisition of information (data breach)” with average score of 3,73;
- T4.1.1 “Information leakage/sharing due to human errors” with average score of 3,63.

The three less critical risks (average score under 3,5) are:

- T4.4.5 “Misuse of assurance tools” with average score of 3,27;
- T4.4.4 “Generation and use of rogue certificates” with average score of 3,38;
- T4.6.1 “Skill shortage” with average score of 3,39.

From the results, it emerges that the data domain is often considered as a data and privacy protection domain, where threats about legal aspects of data management, and unauthorised access to data have higher relevance. Technical aspects of data protection, including tools and services for data storage are perceived of lesser relevance. The latter is probably due to the fact that the risks introduced by data management tools and services are already covered in other domains, since the data domain is increasingly horizontal to all domains.

3.10.2.5. Application-Centric Security

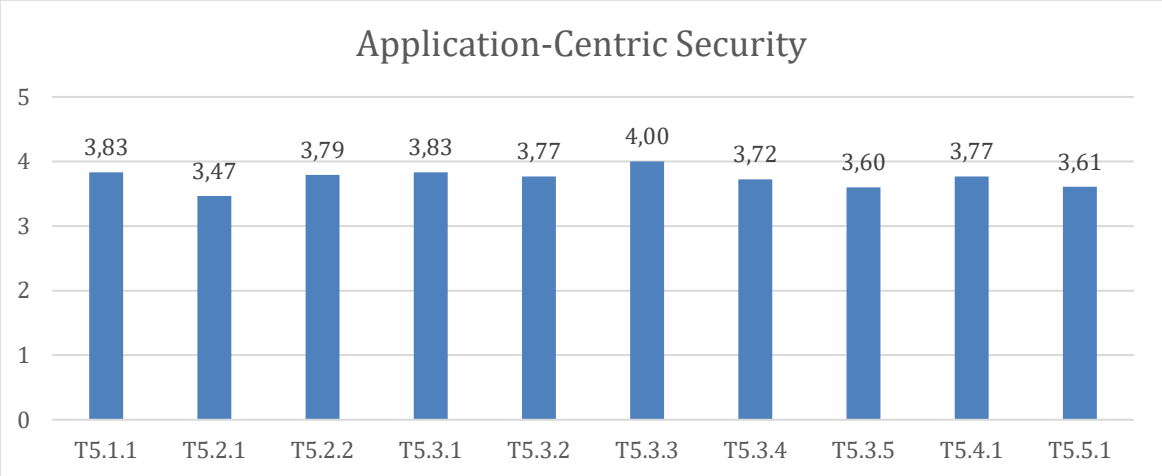


Figure 9 – Threat relevance in Application-Centric security

All threats fall in the area of High relevance (between 3,5 and 4,5 score in Figure 9), except for “T5.2.1 Interception of information” that is slightly under the 3,5 threshold in the area of Medium relevance. The most critical threat is “T5.3.3 Code Execution and Injection (unsecure APIs)“, though more or less all the threats in this area are considered of critical importance. In general, this domain shows the trends of the other domains with an increase in the coverage of the area of High relevance, due to the fact that (mobile) applications are at the core of modern services.

3.10.2.6. User-Centric Security

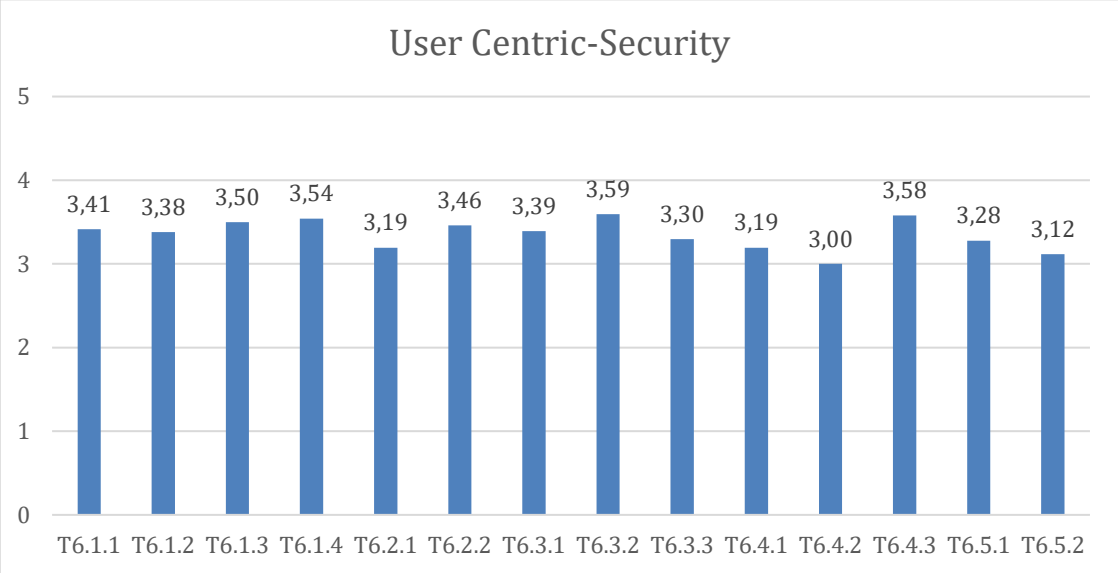


Figure 10 – Threat relevance in User-Centric security

Almost all threats fall in the area of Medium relevance (between 2,5 and 3,5 score in Figure 10) with the exception of:

- T6.3.2 State-sponsored organizations' activity with average score of 3,59;
- T6.4.3 Social responsibility/Ethics-related incidents with average score of 3,58;
- T6.1.4 Legal, reputational, and financial cost with average score of 3,54.

It then emerges that user-centric threats that are mostly concentrated on threats targeting humans are less of interest in a business-oriented scenario like the ones considered by CONCORDIA partners.

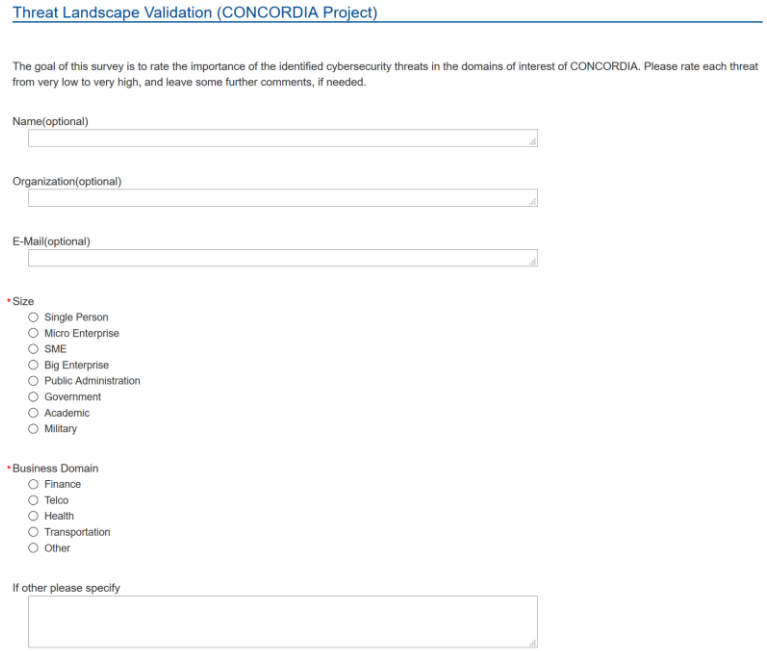
Summary. To conclude, from this first evaluation, it emerges that system threats (average score 3,78) are consider the ones entailing a higher risk, followed by application threats (average score 3,74) and device/IoT (average score 3,67), network (average score 3,59), and finally data (average score 3,48) and user (average score 3,35) threats. More in detail, user threats are considered the least risky, probably due to composition of the CONCORDIA consortium, while data threats are often perceived as impacted all domains of interest and are therefore rated slightly lower than threats applied to a specific domain. The complexity of today IT system is increasing the concerns about system-centric security, making system threats the most relevant. Applications with IoT/device threats are also considered very relevant, showing how current technology evolutions are changing the security perspective and perception.

3.10.3. External validation

The second validation step aims to extend the threat landscape validation outside the consortium. To this aim, we refined the survey in Section 4.2, to collect hints and suggestions to increase the quality of our findings. This survey, already distributed in a CONCORDIA blog post (see Section 4.4), will be also further accompanied by a

summary (HTML and PDF versions) of our deliverable. It will be distributed to members of the CONCODIA Stakeholder group.
The survey can be publicly accessed at
https://ec.europa.eu/eusurvey/runner/9eec529f-9a7d-197a-93c9-618617f22031
and is composed of two parts:

1. Information on the respondents in order to support detailed statistics on the results.



Threat Landscape Validation (CONCORDIA Project)

The goal of this survey is to rate the importance of the identified cybersecurity threats in the domains of interest of CONCORDIA. Please rate each threat from very low to very high, and leave some further comments, if needed.

Name(optional)

Organization(optional)

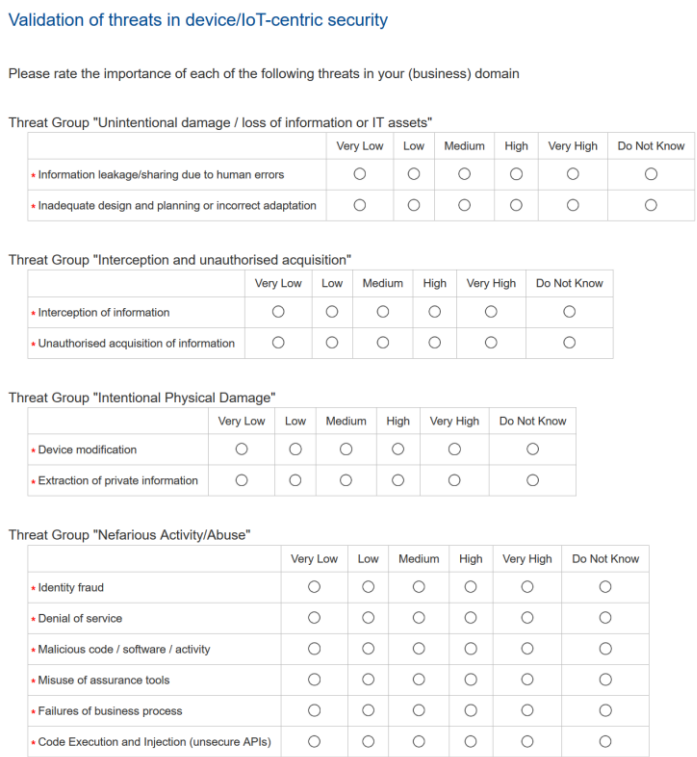
E-Mail(optional)

*Size
- Single Person
- Micro Enterprise
- SME
- Big Enterprise
- Public Administration
- Government
- Academic
- Military

*Business Domain
- Finance
- Telco
- Health
- Transportation
- Other

If other please specify

2. A set of questions for rating the relevance of each threat in Sections 3.3-3.8 from 1 (very low relevance) to 5 (very high relevance) in their specific area(s) of business.



Validation of threats in device/IoT-centric security

Please rate the importance of each of the following threats in your (business) domain

Threat Group "Unintentional damage / loss of information or IT assets"

	Very Low	Low	Medium	High	Very High	Do Not Know
* Information leakage/sharing due to human errors	○	○	○	○	○	○
* Inadequate design and planning or incorrect adaptation	○	○	○	○	○	○

Threat Group "Interception and unauthorised acquisition"

	Very Low	Low	Medium	High	Very High	Do Not Know
* Interception of information	○	○	○	○	○	○
* Unauthorised acquisition of information	○	○	○	○	○	○

Threat Group "Intentional Physical Damage"

	Very Low	Low	Medium	High	Very High	Do Not Know
* Device modification	○	○	○	○	○	○
* Extraction of private information	○	○	○	○	○	○

Threat Group "Nefarious Activity/Abuse"

	Very Low	Low	Medium	High	Very High	Do Not Know
* Identity fraud	○	○	○	○	○	○
* Denial of service	○	○	○	○	○	○
* Malicious code / software / activity	○	○	○	○	○	○
* Misuse of assurance tools	○	○	○	○	○	○
* Failures of business process	○	○	○	○	○	○
* Code Execution and Injection (unsecure APIs)	○	○	○	○	○	○

3.10.4. Dissemination material

The third step considers the production and dissemination of new material to make the content of this deliverable popularly available (e.g., blog posts, white papers) and collect as many feedbacks as possible. Some preliminary activities have been already implemented as follows.

1. We presented the first outcomes of our work in Task 4.1 at CONCORDIA Open Door event in Luxembourg, October 17, 2019. The feedback collected at the event allowed us to refine the content of our deliverable to its current content. In particular, we received different comments supporting our idea of splitting data and application in two domains. We then received specific comments on asset and threat taxonomies, as well as some relevant pointers to recent and relevant attacks.
2. On January 16, 2020, we circulated a summary of the content of this deliverable, specifically focusing on the threat taxonomy in an entry "Cybersecurity threats: trends" on the CONCORDIA blog available at https://www.concordia-h2020.eu/blog-post/cybersecurity-threats-trends/. The blog entry includes a link to the public survey in Section 4.3 and has been circulated in Twitter as well.
3. We are finalizing an HTML version of the deliverable to simplify browsing by readers and implement a community-based prioritization of the threats. The HTML version will be publicly available online and linked on the CONCORDIA web site.
4. We are finally preparing a scientific publication of the work on threat assessment and a whitepaper including our main findings and takeaways.

4. Legal Aspects

This chapter produces an overview of the already applicable and the proposed regulations at EU level pertaining to cybersecurity. As opposed to the approach taken in other parts of the present document of structuring the discussion based on the separate thematic areas, meaning, the ''network-centricity'', the ''system-centricity'', the ''data-centricity'', the ''application-centricity'' and the ''end-user centricity'', this chapter discusses the legal aspects of cybersecurity in a rather holistic manner. Taking into account that, despite the distinctive scope of each legislative act, all regulations aim ultimately at the protection of interests of individuals and society as a whole, the discussion below expands on the above-mentioned issues such as the protection of networks through the lens of the regulations presented.

Note that the discussion below revolves only around the most relevant pieces of legislation and it, therefore, does not provide for a comprehensive presentation of all EU regulations that could be deemed relevant for cybersecurity. As mentioned above, any breach of the regulations discussed below is considered to fall under the respective TG identified and discussed under the previous chapters.

4.1 The Current Regulatory Landscape: Most Relevant Applicable EU Regulations

Despite the innumerable benefits that technology has to offer to individuals, businesses and society in general, there are certain downsides that come with it.

Taking into account that the digital economy is growing at an unprecedented rate, the European Union has taken several measures to regulate the different facets surrounding it. The current section provides an overview of the applicable regulations aiming to ensure that benefits of technology are leveraged in a safe, secure and scalable manner for EU citizens and businesses. The overview provides both for Regulations such as the General Data Protection Regulation (GDPR) that are horizontally applicable across all EU Member States, as well as for regulations in the form of Directives that require a transposition in the respective legal order.

Figure 11 – EU regulatory landscape (State of play - October 2019)

Figure 11 encapsulates the state of play with respect to the current regulatory framework. The revised Payment Services Directive (PSD2)[100] entered into force on 12 January 2016 and supports innovation in the field of retail payments. The PSD2 also enhances consumer protection as well as security with respect to payment transactions. Similarly, the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) creates a framework for secure cross-border electronic transactions. On the other hand, the Directive on security of network and information systems (NIS Directive), which is the first EU-wide legislation on cybersecurity, aims at bolstering cybersecurity all across the Europe. Due to growing concerns resulting from data breaches and incidents of misuse of data, the ePrivacy Directive and the General Data Protection Regulation (GDPR) had been proposed. While the GDPR came into force 25 May 2018, the proposed ePrivacy Regulation, which will replace the ePrivacy Directive and complement the scope of the GDPR is still being discussed between the EU Institutions. The present discussion will also be touching upon newer legislations i.e. the Regulation on Free Flow of Non-Personal Data and the Cybersecurity Act which came into force on 28 May 2019 and 27 June 2019 respectively.

4.1.1 The Directive on Security of Network and Information Systems (NIS Directive)

In furtherance of the EU's Cybersecurity Strategy discussed under Chapter 1, a proposal was made for a directive that would require internet providers and operators

[100] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

of critical infrastructure [101] to provide a safe, secure and trustworthy digital environment by assigning them with clear obligations. This directive is the first EU horizontal legislation that addresses cybersecurity challenges aiming to increase the cybersecurity resilience of Member States to avoid the far-reaching consequences of cyber attacks.

Recognising the relevance of network and information systems and services in the current digital era, the Directive requires operators in critical sectors (such as banking, health, finance, transport) and enablers of information society services (such as app stores, social networks and search engines) to adopt effective risk management practices. In particular, Article 4 (1) defines 'network and information system' means: *(a)an electronic communications network within the meaning of point (a) of Article 2 of the Framework Directive; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.* While the directive provides for obligations of operators of essential services, Article 4 (4) read with Article 5(2) lays down the criteria for the identification of operators of essential service and include *"(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b)the provision of that service depends on network and information systems; and (c)an incident would have significant disruptive effects on the provision of that service."*
Annexure II of the NIS Directive provides an exhaustive list of sectors and entities that qualify as providers of essential services such as energy, transport, banking, health and digital infrastructure. With respect to the telecom sector, a Communication from the European Commission clarified that the security and notification obligation provided for under the Directive is not applicable to telecom providers.[102] However, in the event that the telecom company provides other digital services such as cloud computing, online marketplace and/or online search engine and digital infrastructure as listed in Annex II point 7 of the Directive, it would ultimately be subject to the security and notification obligation of the Directive.

In the context of the present deliverable, the sector-specific pilots provided for under Work Package 2 (WP2) of CONCORDIA relate to finance, transport e-mobility, e-heath and defence sectors, all of which fall under the scope of the NIS Directive.

Responsible parties, both at the national level as well as at EU level, have clearly been mapped out in Figure 12.

[101] Note that mobile network operators providing services in the EU are subject to Union and to Member States' national law, i.e the EU framework in the field of electronic communications (Directive 2002/21/EC) and the Electronic Communications Code (Directive 2018/1972), which replaces the EU Framework and must be transposed by Member States.

[102] Communication from the Commission to the European Parliament and the Council - Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, available at https://eur-lex.europa.eu/resource.html?uri=cellar:d829f91d-9859-11e7-b92d-01aa75ed71a1.0001.02/DOC_3&format=PDF

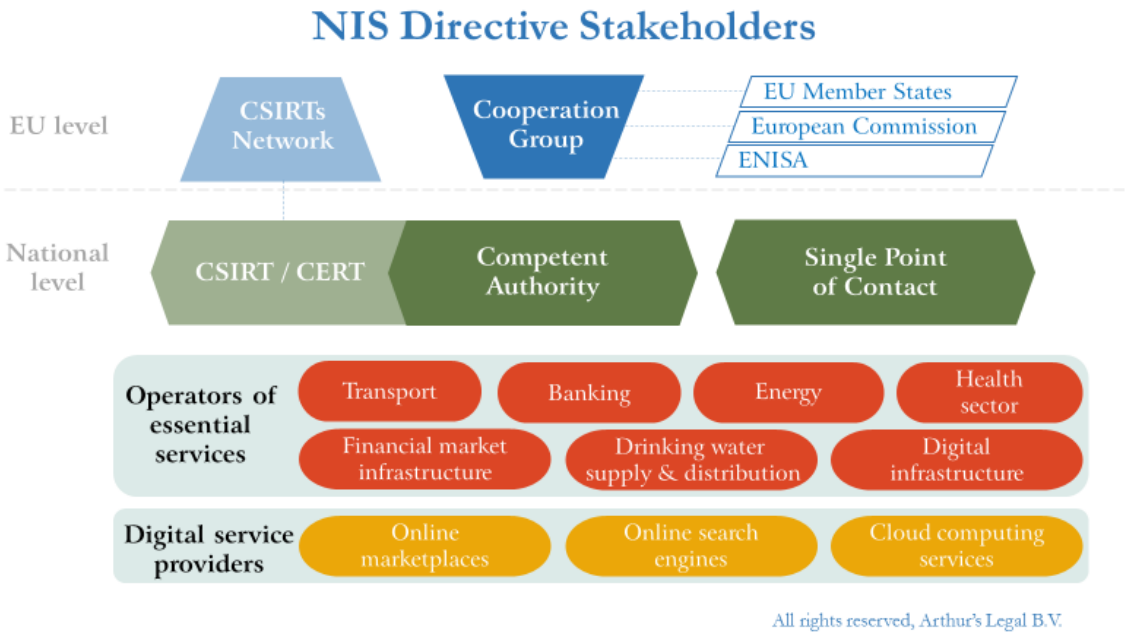


Figure 12 – Responsible actors under the NIS Directive[103]

As per the NIS Directive, operators of essential services are required to take all the necessary technical and organisational measures to ensure that risks to the security of network and information systems are managed effectively. In the event that an incident occurs which significantly impacts the continuity of the essential services that are provided, the operator must notify the competent authority or the Computer Security Incident Response Team (CSIRT). Similar notification obligations also apply to digital service providers.

In line with the objectives of the Cybersecurity Package mentioned earlier, not only does the NIS Directive focus on improving cybersecurity capabilities at a national level but it also aims at fortifying cooperation at an EU level. For this purpose, Members are required to nominate at least one national competent authority that oversees the application of the Directive within the member state and to appoint a single point of contact that is responsible to ensuring seamless cross-border cooperation and communication with other Member States. In addition, Member States are also required to set up at least one Computer Security Incident Response Team (CSIRT) to monitor threats and incidents at a national level and to devise response mechanisms.

At an EU level, the Directive creates a network of CSIRTs that fosters trust and confidence between the Member States and enables effective communication. A Cooperation Group is also established which is chaired by the Presidency of the Council of the European Union. The role of the Group is to bring together the representatives of the Member States, the European Union Agency for Network and Information Security (ENISA) and the European Commission in order to facilitate exchange of information and for strategic cooperation.

Notably, in light of NIS Directive, European Commission provided an overview of how Member States have identified operators of essential services by assessing whether

[103] Create IoT Project, Deliverable 05.05 Legal IoT Framework (Initial) available at https://european-iot-pilots.eu/wp-content/uploads/2018/02/D05_05_WP05_H2020_CREATE-IoT_Final.pdf

the methodologies for identifying such operators are consistent across Member States.[25]

4.1.2 The Regulation on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act)

A core part of the European Commission's cybersecurity package which was adopted in September 2017 was the proposal for the Cybersecurity Act[104] that was soon adopted by the EU Institutions in March 2019 and became applicable on 27th June 2019. As mentioned earlier under 1.1, in addition to the adoption of the NIS Directive, the adoption of the Cybersecurity Act was another step taken in order to fortify the cyber resilience of the EU. The two major changes introduced by the Cybersecurity Act are: 1) Establishment of a permanent mandate for the European Union Agency for Network and Information Security (ENISA) 2) Creation of a European cybersecurity certification framework. The proposal for the Act was approved by the European Parliament.

As ENISA has a pivotal role to play in reinforcing cyber resilience and response in the EU, by enacting the Cybersecurity Act, the Commission has granted the agency a permanent mandate with an additional set of tasks including facilitating EU-wide cooperation and capacity building. As per the Directive, ENISA should promote the exchange of best practices between Member States and private stakeholders, offer policy suggestions to the Commission and the Member States, act as a reference point for Union sectoral policy initiatives with regard to cybersecurity matters and foster operational cooperation, both between Member States and between the Member States and Union institutions, bodies, office and agencies.[105] The agency is also required to assist Member States with capacity building and helping them detect, prevent and respond to cyber threats. Interestingly, the Directive defines a cyber threat as "*any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons"*[106]

As far as the establishment of the European Cybersecurity Framework is concerned, the rationale behind it is two-fold. Firstly, to increase trust in ICT products, services and processes that are certified by a harmonised EU cybersecurity framework. Secondly, to avoid discrepancies between conflicting or otherwise confusing national cybersecurity schemes.[107] ENISA has a role to play with respect to the European Cybersecurity Framework envisioned, as it has been requested by the Commission to

[104] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[105] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, Recital 17

[106] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 Article 2 (8)

[107] Article 46 of the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

prepare a candidate European cybersecurity certification scheme or to review an existing European cybersecurity certification scheme on the basis of the Union rolling work programme.[108] Note that the Act also permits voluntary self-assessment by manufacturers or providers of ICT products, services and processes.

4.1.3 General Data Protection Regulation (GDPR)

The General Data Protection Regulation[109] (GDPR) is the EU's framework for regulation data protection. The Regulation came into force on 25 May 2018 and received much attention from organizations as well as governments around the world especially since the regulation applies to organisations processing personal data regardless of whether the organisation is established in the EU or not.

Article 4(1) of the regulation defines "personal data" as: *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

As far as security is concerned, given that the GDPR is user-centric, it requires organisations to take into account the state of the art. In particular, as far as the security of processing of personal data is concerned, organizations acting as data controllers and data processors are expected to consider a) related cost of implementation, b) nature and purpose of processing the data and c) the risk and impact on the rights and fundamental freedoms of individuals, before they implement the appropriate technical and organizational measures

In addition, the GDPR also introduces legal accountability under Article 5(2). The provision in the GDPR requires data controllers i.e. organisations that are processing the personal data to demonstrate that they are doing so in compliance with the principles relating to processing of personal data which entails the revival of the burden of proof at the expense of the organisations acting as data controllers. The Regulation also introduces the principle of data protection by design and by default, whereby, controllers are required to ensure that technical and organisational measures are taken from the very beginning of processing operations and during its lifetime. Use of pseudonymisation and encryption has also been suggested to avoid risks.

4.1.4 The Regulation on the Free Flow of Non-Personal Data

The enactment of the Regulation on a framework for the free flow of non-personal data[110] was the European Commission's recent move to allow the data economy to thrive and to allow public administrations and companies to freely use non-personal data without being restricted by territorial boundaries. The Regulation, which became

[108] Article 48 of the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

[109] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural people with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC OJ L 119/1

[110] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union OJ L 303/59

applicable on 28 May 2019, aims at removing all restrictions to the free movement of non-personal data within the EU. It is a key building block of the Digital Single Market and considered the most important factor for the data economy to unleash its full potential and to double its value to 4% of GDP (Gross Domestic Product) in 2020. The new measures are in line with already existing rules for the free movement and portability of personal data in the EU.[111]

It is pertinent to note that the regulation defines 'data' as data other than personal data that is defined under the GDPR. Moreover, the Regulation enshrines the principle of the free movement of non-personal data into EU law to help develop the data economy and to enhance competitiveness of the union industry. As a result, the Regulation takes a principle-based approach to ensure cooperation between Member States and also focuses on self-regulation to provide a flexible framework that caters to the changing needs of users and society and threats that may follow.

By 30 May 2021, the Regulation requires Member States to ensure that there is no provision in any law, regulation or administrative provision of a general nature that restricts data mobility directly or indirectly outside the jurisdiction of a Member State unless the restriction is justified on grounds of public safety. If a Member State is of the opinion that an existing data-localization requirement meets requirements laid down under the Regulation then it is required to notify the European Commission, pursuant to which the Commission will determine whether the provision in question is appropriate or if it should be amended or repealed.

On May 5, 2019, the European Commission published a guidance to throw light on the interactions between the Regulation and the GDPR, as both regulations approach the free movement of data within the EU from two distinct angles. While the Regulation prohibits localisation of non-personal data, the GDPR aims at maintaining a high level of protection of personal data. However, there can be situations involving mixed data sets, that is, data sets which consist of both personal as well as non-personal data, where separating the two could either be extremely tedious or economically unfeasible. As per the guidance, normally, such a mixed data set would be subject to the provisions of the GDPR and the underlying obligations of data controllers and processors.

4.1.5 Revised Payment Services Directive (PSD2)

The enactment of the revised Payment Services Directive[100] helped transform traditional methods of banking to more innovative ones. Prior to its enactment, several aspects of the payments market including internet and mobile transfers were fragmented and unregulated in the Member States. Customers were skeptical of whether any payment that they would make through a third-party service would be compatible with their banks internal policies. As a result, a need was felt to provide equivalent operating conditions to new market players, to create new methods of payment and to ensure consumer protection whilst they use the new methods of payment across the EU.

[111] Free flow of non-personal data https://ec.europa.eu/digital-single-market/en/news/free-flow-non-personal-data, per the guidance, normally, such a mixed data set would be subject to the provisions of the GDPR and the underlying obligations of data controllers and data processors, meaning, the individuals or organizations that process personal data on behalf of the controller.

The PSD2 opens the door for third party providers as well as financial technology companies and encourage the creation of new business models in the field of banking. Figure 13 reflects the addition of two new types of providers i.e. Payment initiation service providers (PISPs) and Account information service providers (AISPs).

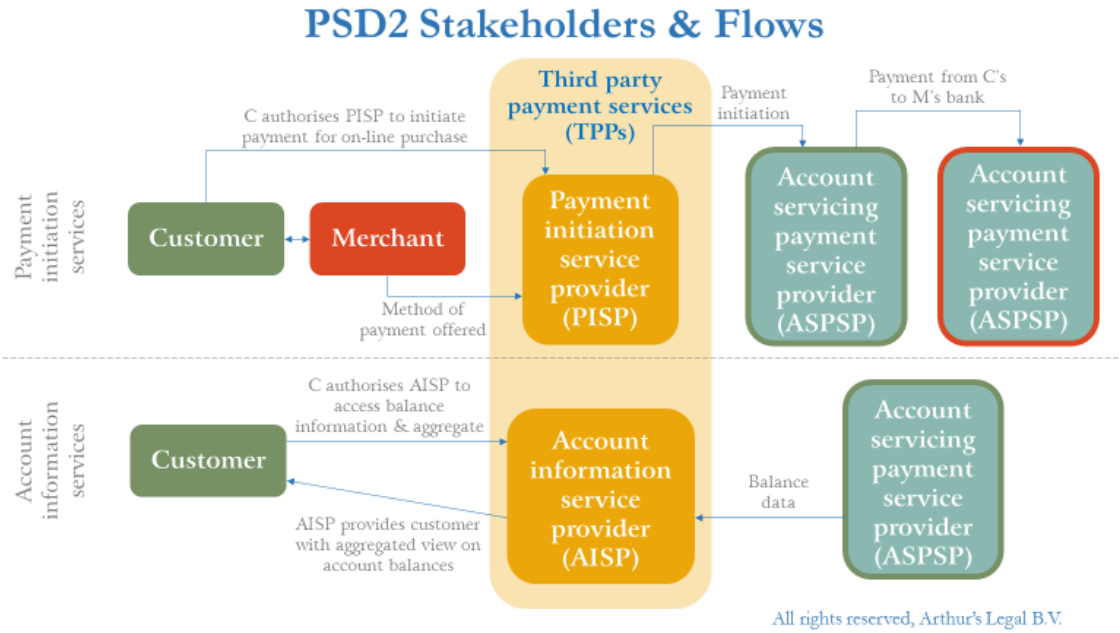


Figure 13 – PSD 2 stakeholders & flows [103]

In this context, the PISP takes the role of a facilitator by enabling the transfer of funds by assessing transaction details and then confirming whether the customer has the necessary funds in their account to go ahead with the transaction. However, in order to do so the PISP first has to obtain the explicit consent of the Account servicing payment service provider (ASPSP). On the other hand, the AISP plays the role of an aggregator of information relating to payments accounts that are held by other institutions such as banks. In order to perform this function, AISPs require access to the said payments accounts and by virtue of Article 66(5) of the PSD2, banks and ASPSPs are required to agree to data requests made by AISPs in a non-discriminatory manner.

In addition to laying down the rights, obligations and procedures relating to payment service, the directive creates a provision for incident reporting wherein major operational or security threats have to be notified to a competent authority in the home Member State of the payment service provider. Pursuant to this, the competent authority is required to provide information to the European Banking Agency (EBA) and the European Central Bank (ECB) and take necessary measures to safeguard the financial system.

On 14 September 2019, Strong Customer Authentication (SCA) was introduced in EU as a part of the PSD2 to reduce the number of instances relating to fraud and to make online payments more immune to hacks by unauthorised parties. A common way for ensuring compliance with the SCA is to rely on 3D secure, an authentication standard whereby the cardholder has to provide additional information (like a One Time Password or fingerprint authentication using their mobile phone) to complete

payment for a transaction. Low-risk transactions and transactions below €30 are exempted from SCA.[112]

4.1.6 Product Liability Directive

While technology poses several risks to personal data protection, consumers' physical safety is also an aspect that cannot be overlooked. The Product Liability Directive[113] was introduced in 1985 to provide a high and equal level of consumer safety and protection. The Directive requires producers to be liable for any damage that results from the use of their products which turn out to be defective. However, when it comes to emerging technology like Artificial Intelligence and Internet of Things, due to the technical nature of the devices and the interconnected web of parties involved in its manufacturing, establishing a link, as required by the Directive, between damage caused and defect in the device can be difficult for injured people to prove.

As the European Commission become aware of the potential gaps in the Directive, it initiated an evaluation of the Directive to assess whether it was sufficient in meeting its objectives in the present scenario, keeping in mind the technological developments. On 10 January 2017, the European Commission launched a public consultation on the directive to gauge the opinion of stakeholders on the application and performance of the directive. Subsequently, a Product Liability Conference was also organised in October 2017 to assess the preliminary results that were obtained during the evaluation of the directive. The report that was published by the Commission on those results acknowledged that concerns that were expressed by stakeholders regarding the limited definition of the term "product", the scope of damage covered and the need to reassess the notion of what would constitute a defect.[114] Currently, the Commission is expected to publish a guidance and a report on liability and security frameworks for emerging technologies. In addition, if deemed necessary, concepts like 'defect', 'damage', 'product' and 'producer' will also be updated.

Complementing the objectives of the Product Liability Directive is the General Product Safety Directive (GPSD)[115] which was enacted to ensure that only products that are safe for consumers are placed on the market. Under the Directive, a product is considered "safe" if it meets the safety requirements either under European law or the law of the Member State where the product is being sold. In addition, the GPSD requires producers to provide consumers with the necessary information to help them become aware of the inherent risks of the products in cases where such risks are not apparent and to also enable consumers to take precautions against the risks. In the same spirit, the Consumer Safety Network (CSN) was created consisting of a group of experts from all EU countries that deliberate on safety of consumer products and data

[112] Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, available at: https://eba.europa.eu/eba-publishes-opinion-on-the-implementation-of-the-rts-on-strong-customer-authentication-and-common-and-secure-communication

[113] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products OJ L 210/29

[114] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC)

[115] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety OJ L 11/4

collection. At present, the European Commission is contemplating the selection of members for a sub-group to the CSN to determine whether the current regulatory framework on product safety is in line with the changing market realities with the expanding use of connected products, artificial intelligence, internet of things and the like.

4.1.7 Radio Equipment Directive

The Radio Equipment Directive (RED)[116] creates a regulatory framework on how radio equipment can be placed on the market. It creates harmonized standards covering a wide range of topics like health, safety, use of radio spectrum and electromagnetic compatibility (EMC). Article 2(1) defines radio equipment as: "*electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination*." Further, electromagnetic disturbance has been defined as *"any electromagnetic phenomenon which may degrade the performance of equipment; an electromagnetic disturbance may be electromagnetic noise, an unwanted signal or a change in the propagation medium itself*"

The Directive creates an exhaustive list of essential requirements that should be met. This includes construction of radio equipment that:

- does not harm the network or is functioning;
- incorporates safeguards to protect personal data and privacy;
- incorporates features ensuring protection from fraud;
- supports features ensuring access to emergency services;
- supports features that enable its use by users with disabilities.

Obligations of manufacturers and distributors of radio equipment are laid down in the Directive to ensure that the radio equipment is designed in order to meet the essential requirements mentioned above. Individuals and organizations that import radio equipment from third countries are also required to comply with the provisions under the Directive. Additionally, manufacturers are also required to perform conformity assessment of the radio equipment to ensure that the radio equipment meet all the requirements laid down in the Directive before it is placed on the market.[116]

4.1.8 The Regulation on Electronic Identification and Trust Services

The eIDAS Regulation[117] acknowledges the importance of building trust in the digital environment for the purpose of economic and social development. It aims at doing so by providing a harmonized framework for secure online interaction between individuals, public authorities and businesses, thereby enhancing the efficiency of online services, whether public or private, and also increasing the efficiency of e-commerce within the EU.

[116] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC OJ L 153/62

[117] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC OJ L 257/73

Electronic identification, which can be used for business-to-business and business-to-consumer transactions, allows companies to check the identity of their customers and other businesses in an agile and seamless manner. Additionally, it enables businesses to increase their customer foothold by providing trusted identification methods in the EU Member States. However, for the purpose of cross-border transactions, mutual recognition is required by each individual Member State. This process ensures that the eID schemes in other Member States meet all the required security and quality requirements laid down under the Regulation.

The Regulation also deals with "trust services" which have been defined under Article 3(16) as "*an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services.*" As a result, a uniform European framework is created for services such as electronic signatures, electronic seals, website authentication, electronic delivery service as it ensures that they have the same legal status as traditional paper-based processes. With respect to processing data, the Regulation states that trust service providers should respect the confidentiality and security requirements under the GDPR. Furthermore, in case of breach of security and loss of integrity that has an impact on the service provided, the trust service provider is required to notify the supervisory board or the relevant body of the same within 24 hours after becoming aware of it.

Overall the eIDAS Regulation increases the level of security of transactions for companies and SMEs thereby creating efficient business processes, reducing costs, enabling safer electronic transactions that further result in increasing the trust of consumers.

4.2 The Changing Regulatory Landscape: Proposed Regulations and Upcoming Initiatives

This section points at how forthcoming changes in the current regulatory landscape by discussing briefly the proposed regulations pertaining to the scope of the present deliverable and by touching upon other upcoming initiatives, possibly, leading to proposals for new laws as depicted in Figure 14.

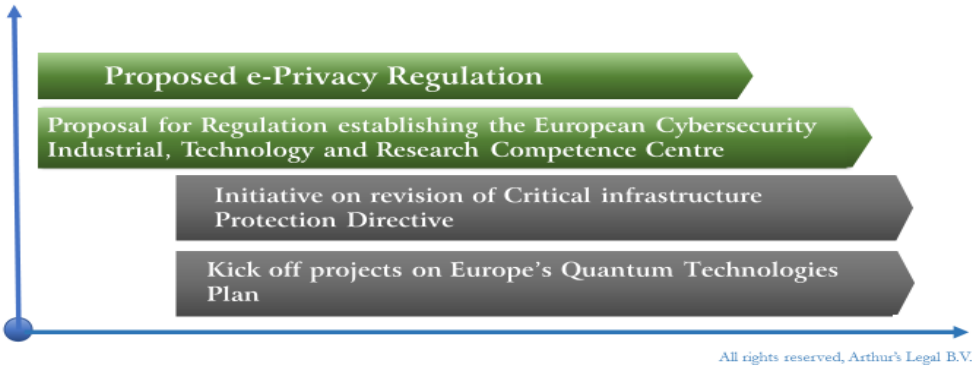


Figure 14 – The changing landscape (State of play, October 2019)

In particular, in addition to the current proposals for new regulations pertaining to cybersecurity and the scope of CONCORDIA itself to be discussed below, European Commission has launched two initiatives of relevance, namely, the reassessment of the 2008 European Critical Infrastructure Protection Directive [118] and the Quantum Technologies Flagship. The above-mentioned Directive identifies European Critical Infrastructures (ECI) and adopts a common approach for evaluating the need to enhance their protection.[119] The Directive is a key part of the European Programme for Critical Infrastructure Protection (EPCIP), the objective of which is to safeguard critical infrastructures from all kinds of threats including natural disasters, man-made and technological threats. As far as the initiatives taken by the Commission in the field of quantum technologies are concerned, on 28 October 2018, an announcement was made on the Quantum Technologies Flagship, a €1 billion initiative, which included 20 projects with focus main areas of application - computing, sensing and metrology, simulations, cryptography, and telecommunications.[120]

Furthermore, in September 2019, the European Commission initiated a public consultation for consumers and the public and a targeted consultation for experts to assess the opinion of stakeholders on Articles 3(3)(e) and (f) of the Radio Equipment Directive. The provision under question state that *"Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements: (e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected; (f) radio equipment supports certain features ensuring protection from fraud.* The questionnaire shared pursuant to the consultation contains an exhaustive list of questions with the aim of gauging whether the relevant stakeholders have trust in wireless connected devices and wearable devices and the scale of that trust.

[118] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection OJ L 345/75

[119] Evaluation of the 2008 European Critical Infrastructure Protection Directive https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1378074_en

[120] Quantum Technologies Flagship kicks off with first 20 projects https://europa.eu/rapid/press-release_IP-18-6205_en.htm

4.2.2 Regulation for a European Cybersecurity Competence Centre

In furtherance of the Cybersecurity initiatives that were announced in 2017, the European Commission announced a proposal for the creation of a Network of Cybersecurity Competence Centers[121] to bolster the EU's cybersecurity capacity and to secure its Digital Single Market. The Competence Centers will be funded by participating Member States and the EU. The overall mission of the Competence Centre is to help set up and organize National Coordination Centers Network and the Cybersecurity Competence Community and to implement cybersecurity-related financial support from Horizon Europe and the Digital Europe Programme.[122]

Through the new structure that will be created– a Competence Center at the EU level and national level competence centers – it is aimed that the proposal will strengthen the EU's cybersecurity capabilities and competencies. On one hand, the proposal is expected to facilitate coordination at an EU and national level and provide access to exiting expertise. On the other hand, it aims to encourage and accelerate standardization methods and certification schemes like the cybersecurity certification schemes provided under the Cybersecurity Act.[123]

4.2.3 ePrivacy Regulation

On 10 January 2017, lawmakers in the EU submitted a proposal for a new privacy regulation with the view of updating existing rules relating to privacy and electronic communications and building trust and security in the Digital Single Market.

Besides other things, the regulation provides new rules on cookies and the use of cookie walls, bans unsolicited electronic communication and makes provision for the use of metadata. In addition, significantly stronger obligations for privacy by default have been proposed, including end-to-end encryption (with no backdoors). However, since the publication of the first draft of the Regulation, it has undergone several amendments. The most recent draft of the Regulation which was published on 4 October 2019 contains several revised definitions and provisions. As far as metadata is concerned, the new regulation lays down instances where metadata can be processed including cases where such processing is necessary for the purpose of network management or network optimisation, for protecting the vital interests of a natural person or where the end-user has given his or her consent. An additional provision had been added to allow processing of electronic communications solely for the purpose of identifying and deleting content that constitutes child pornography provided that such processing meets certain parameters.

Currently, there are efforts that an agreement is reached as soon as possible. Nevertheless, it is probable that the adoption of the text may not take place before 2020.

---

[121] Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, 2018/0328 (COD),

[122] European Cybersecurity Industrial, Technology and Research Competence Centre https://ec.europa.eu/digital-single-market/en/european-cybersecurity-industrial-technology-and-research-competence-centre

[123] The new European cybersecurity competence centre and network http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)635518

4.3 Regulatory Mapping

Drawing upon the domains of the working groups identified under Task 4.1 as well as on the discussion captured earlier under Chapter 4, this section attempts to map the currently applicable regulations at EU level with the focus areas identified, meaning, networks, systems, data, applications and protection of end-user[124]. To this end, the mapping captured in the table below was based on the articles providing for the subject matter and scope under the respective regulation discussed. It should be made explicit that the focus area ''people'' identified does not only cover end-users, but also people, in general, acting in their other capacities (e.g. employees).

Overall, even by looking strictly into the scope of currently applicable regulations at EU level without more broadly looking into the overarching intended purposes, as reflected, for instance, in the respective Recitals, it seems that European law does provide for all domains of interest identified. As surfaced earlier, the Regulations in place assign concrete obligations to the responsible actors identified in each case, for example, of risk management. Nevertheless, it could be argued that the hyper-connectivity, the complex legal relationships allowing for it and the proliferation of harm in cyberspace do raise concerns in reality in relation to the determination of liabilities incurred (also, on the basis of contractual arrangements) and, in essence, on the actual effectiveness of the law. Notably, the issue of liability in the cyberspace, within the field of cybersecurity and the associated insurance mechanisms in place, will be further discussed under Chapter 5.

Table 33 – Applicable EU regulations and technology domain of interest

REGULATION IN DIGITAL AGE	NETWORK	SYSTEMS	DATA	APPLICATION	PEOPLE
NIS Directive	✓	✓		Impact-Based?	
Cyber Security Act	✓	✓	✓	✓	?
Free Flow Of Non-Personal Data		✓	✓	✓	✓
General Data Protection Regulation	✓	✓	✓	✓	✓
Payment Services Directive 2		✓	✓	✓	✓

[124] Although not captured in the table below, it is aimed that the Radio Equipment Directive provides mainly for network, systems and data. Similarly, it is intended that the proposed ePrivacy Regulation provides for all the focus areas identified.

Product Liability Directive[125]	?	?	?	?	✓
eIDAS Regulation	✓	✓	✓	✓	✓

4.4 Challenges and Future Trends

There is no denying that technology is growing at such an unprecedented rate that renders it challenging for regulators to take prompt action based on the length democratic processes.

As surfaced by the discussion above, the EU Regulator, however, has taken great strides to keep up with the technological developments either by introducing new legislation or by amending existing ones. Several other soft law instruments, such as guidelines have been, also, put forward by the European Commission aiming to provide concrete guidance at an implementation level, thus, better mirroring the dynamics of the marketplace. In this spirit, for example, the European Commission published in September 2017 the Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[126] to prevent cyber attacks from threatening the economy and bolster the EU's resilience to such attacks. Moreover, the Artificial Intelligence High Level Group of Experts published guidelines in 2018 listing key requirements that can make AI systems trustworthy, while the newly elected European Commission President made explicit the aim of the European Commission to propose new legislation focusing on artificial intelligence. Note that the ''Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology & Research Competence Centers and the Network of National Coordination Centres'' of direct relevance for CONCORDIA project reflects the regulatory aim to utilize skills and capacities in order to provide for better safeguards for cybersecurity in the future.

In a wider context, there are, of course, some aspects that are under discussion at an international level such as the ability of countries to make jurisdictional claim given the borderless nature of the internet. Besides making a claim, another challenge would be with respect to enforcement of the claim[127]. Interestingly, in this respect, the GDPR paves the way, in the sense that it dictates that companies outside the EU may also be required to comply with its provisions under certain circumstances. Whether this approach will be taken in other regulations as well is yet to be seen.

[125] Given the current discussions on key concepts such as the ''product'', ''damage'' and ''defect'', the scope of the Product Liability Directive is considered to be unclear.

[126] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2013:0001:FIN

[127] INTERNET & JURISDICTION GLOBAL STATUS REPORT 2019, Internet and Jurisdiction Policy Network, available at: https://www.internetjurisdiction.net/publications

5. Economic Perspectives

Cybersecurity concerns are one of the significant side effects of an increasingly interconnected world, which inevitably put economic factors into perspective either directly or indirectly. As various types of attacks are being leveraged with the democratization of Internet access, there is a greater need for companies and nations for higher protective measures concerning their cyber activities. For example, Critical National Infrastructures (CNI) are infrastructures that are crucial for the everyday life of the population of the nation. Infrastructures from different sectors can be considered as CNI, which directly affect the health of the population while others are affecting the national economy. These infrastructures should receive special attention regarding reliability and security because of their importance and the dangerous impacts if they failed.

The most dangerous threats discussed in Section 3 have also impact on the economic aspects of cybersecurity, since all of them can result, for example, in financial loss or business disruption. Such threats include, for example, botnets for conduct DDoS attacks, information leakage, and different families of malware. Besides, attacks on cloud storages, governments ICTs, and supply chain are still rising, such as sabotages, misinformation campaigns and stealing of sensitive data. Even though those threats are being the concern of academia and industry for the past years, solutions to completely solve them are not on the horizon. Also, most of the target, although have giving attention to that, are not investing sufficient budget in protecting themselves against attackers.

In a recent survey [73] concerning the reasons for vulnerabilities, almost 60% of the companies included in the survey mention that budget constraints are the reasons behind missing measures against cyber attacks. From these, 53% of the companies stated that the lack of skilled resources, namely employees, pose a danger to the cybersecurity of the company. This problem could also be caused by the lack of willingness to invest in better cybersecurity systems and personnel by the company, since the acquisition of skilled workers expensive in general. The survey mentions that tools and methods to recognize vulnerabilities and cyber threats are many times not advanced enough to meet the need in the current environment. All these factors together form a major peril to the cybersecurity of companies and their system and may be responsible for a considerable number of successful cyber attacks.

Also, it is important to mention that while most corporate business actions can be quantified, security is not straightforward to be quantified. Contrary to the popular opinion, not having suffered from a cyber-attack is not a valid indication for a secure organization. In this context, vulnerabilities in a single system can put in risk all other subsystems or directly connected systems. In addition to security aspects, one must consider safety aspects in which systems can deliberately fail (*e.g.,* due to human or natural disaster factors), jeopardizing one of the fundamental aspects of security, the availability. Nonetheless, announcing that an organization implemented a 24/7 CSIRT (Computer Security Incident Response Team) is, in fact, an indicator for security, but the indicator is limited to the capacity of its professionals only. There is a need for standards to measure and reveal the security level such that all stakeholders can understand and develop a common view.

Such standards are for instance ISO/IEC 27000 family, the The Cybersecurity Framework of the National Institute of Standards and Technology (NIST), the Control Objectives for Information and Related Technology (COBIT) of the Information Systems Audit and Control Association (ISACA), or IEC6244 of the International Electrotechnical Commission. Even though these works differently, they are following common goals. With the help of the mentioned standards, security responsible can compare themselves to other market players or even to whole industries. Committing to be certified against ISO27000 or improving one's NIST[17] tier level makes investments into security justifiable for the security responsible in an organization. What this means in detail, will be discussed in the following sections.

The cybercrime economic damages go beyond of thefts of personal/financial data or intellectual property. These attacks can cause a direct loss in the company's reputation, which may even represent a total disruption of the business. In this context, it is imperative to understand the dependencies between complex and distributed systems (e.g., supply chain), as well as security and safety risks associated with each actor.

This chapter is divided as follows. Based on increasing risk and attack vectors, a state-of-the-art concerning past EU projects focused on cyber economics is conducted as well as selected type of attacks and a case study are discussed in Section 5.1. Next, Section 5.2 presents SEConomy, a framework for the viability of economic models that take into account risks and threats attributed to the role of each stakeholder within an ecosystem. SEConomy proposes a cost-investment security analysis model based on the relationship between system attributes and their failure probabilities, which results in economic impacts. Also, a case study regarding a ransomware attack is conducted to demonstrate how SEConomy framework can be applied.

5.1. Background and Landscape

This section provides an overview of past efforts of part of the EU community in the direction of propose tools and mechanisms to handle with economic aspects of cybersecurity. This section concentrates on the project in which CONCORDIA partners were involved, which knowledge obtained can support further directions to explore different economic dimensions in the context of the CONCORDIA project. Next, an overview of selected threats is provided, where details of well-known types of attacks are provided in a way to describe how they impact the economic aspects of cybersecurity as well as investigate new markets that have been explored to amplify the damage of attacks. Finally, a case study is conducted considering the financial sector as the main stakeholder to provide an example of how attackers can impact the health of the financial sector.

5.1.1. Past EU Cybersecurity Economics Projects

SecCord [74] was FP7 coordination and support project action for the Trust and Security (T&S) research programme, running from November 2012 to October 2015. There have been five inter-related threads to its work plan that correspond to the project objectives, namely, to provide a strategic outlook of the emerging and developing T&S issues, including economic concerns. In this direction, the main contribution of SecCord was a service to projects in their later stages to translate and match their anticipated results into economically valuable outcomes, which included analysis of research to practice model (R2P) such as technology transfer and technology acceptance models (TAM). Its sister

project IPACSO [75], another coordination and support action which was running in parallel and was coordinated by the same partner, was more focused on innovation, but also had work package dedicated to economic incentives in cybersecurity. In its turn, SecCord was building on outcomes of EFFECT+, the prior coordination and support action that started in September 2010. This project was aiming to represent the broader stakeholder constituency in a trustworthy Future Internet community (at that time represented by Future Internet Assembly – FIA) and to get their opinion on the market and economics of trust. In EFFECT+ two aspects of the economics were addressed, namely effective engineering to deliver trustworthy solutions, by addressing requirements from the outset, and the cost of non-compliance.

Also, projects were focusing on investigating porting some models and conclusions from the more mature field of physical security economics to the field of cybersecurity economics. Among these projects, one of the first ones was EUSECON [76] that focused its study on how EU security policy can be understood as a collective good. While the research was more focused on EU policy and comparison with the other regions, mainly for anti-terrorist policy, some conclusions were impressive, as they can also be seen in the area of cybersecurity. They identify a trend that seeks to isolate the effects of a particular policy and deficiency of probabilistic reasoning, with a special focus on worst-case scenarios.

In such a direction, ValueSec [77] project objective was to generate a knowledge base of the status and trends in theory and practical applications of methods of economics applied to security decision making. It was combining economical and societal effects of security measures into a value function, and used new methodology framework to integrate it into a toolkit, which was later used in other projects, such as CIRAS [78], ECOSSIAN [79], PULSE [80] and NESSoS. Criteria developed in the ValueSec were especially useful for societal impact assessment. Therefore, although two pilots were focused on physical security, there was also a pilot with cybersecurity impact (ValueSec), critical infrastructure security (CIRAS), and secure software engineering (NESSoS). One of the main contributions of ValueSec, however, was to evaluate the status of different approaches and methods (e.g., from econometrics, risk assessment, operational science) and describe the potential of further development.

It is important to note that security economics research and tool development before ValueSec was rather limited either in the application domain e.g., ICT or the finance sector, or addressing only a limited threat and risk spectrum (e.g., terrorism) or a specific narrow view like that of insurance on a particular type of natural disaster. ValueSec was using econometric approaches to comparing, assessing, and pricing of risks for security planning, decision making, and management purposes bound to employ quantitative methods of decision analysis. Its results clearly show that the Internal Employee Control measure would have the most significant positive effect in terms of risk reduction. However, other indirect cost complications (including societal impact) since it intrudes into the daily lives of the employees. This is an excellent example that illustrates how cost-effectiveness cannot rely solely on technical controls. However, it needs also to take into account societal as well as the impact on individuals.

In a similiar direction than ValueSec, CIRAS project applied to critical infrastructure security and analysed standards and tools that could enhance ValueSec. Bow tie diagram that links threats and causes is used as a model to assist the risk modeling, while fault tree analysis (FTA) is a method that may be used to calculate the probability of the top event based on the probabilities of each casual event. CIRAS also contemplates the use of event tree analysis as a graphical and probabilistic method for modeling and analysis of accident scenarios, typically used to the right-hand side of the bow-tie diagram. For the initial design, Failure Mode Effects Analysis (FMEA) can be used as a method by which each potential failure is analysed to determine its results or effects on the system and to classify each

potential failure mode according to its severity. Finally, business impact analysis (BIA) provides an understanding of the criticality of key business processes, associated resources, and interdependencies that exist for an organization. CIRAS was also reusing cost-benefit analysis (CBA) functional block from ValueSec to assess economically the implications of the selected security measures. This time simulation was assuming two major incidents occur during the specified lifetime, so it goes beyond one-time-measurement.
In another project, SECONOMICS [81] was proposed to take into account individual use case features, as well as externalities, and incorporate these into cost and utility function by using simulation and other tools. Another part of the research was focused on the concept of risk, with differentiation of objective and subjective risk. Given that the project use cases were also from physical security, the trend of securitization, public attitudes, and societal acceptance were taken into account in this study, next to challenges such as allocation of competences and resources in the multilevel governance. SECONOMICS proposed to nest models of architecture into an economic setting by allowing analysts to use the tool to cover a range of trade-offs, including macro-level policy, regulatory interactions, or operational situation. It has also an option to customize existing models instead of building new ones. The key objective is stress testing across a range of outcomes. Some models use variations of game theory to capture the use and cost of shared resources, as well as regulatory intervention. Comparative statistics, controlled experiments, and media analysis are used as a qualitative method to validate a specific hypothesis. The methodology of adversarial risk analysis (ARA) is applied to the model, in order to extend traditional risk analysis with intentional attackers' threats (e.g., where dynamic attackers have simple cost benefits rules). Besides that, SECONOMICS supports the application of the case-control methodology to draw conclusions on the relationship between a risk factor and an effect by looking backward at the cases and comparing them with controls. It should be noted, however, that the main target outcome of the SECONOMICS tool is policy alignment. While some conclusions from critical infrastructure use cases are useful for CONCORDIA, such as risk modeling or trade-off modeling, the conceptualization of regulation is precise. It should be noted that the project was executed under security and society topics in FP7 when digital security was not part of the same program. Nevertheless, linking between low-level strategies for operational managers and high-level policies is easily replicable in cybersecurity.
In practical terms, the industry is often using CVSS or a similar scoring system for common vulnerability scoring system to decide which vulnerabilities must be fixed with the highest priority. University of Trento, for example, was using SECONOMICS framework as a case-control study to assess the effectiveness of CVSS as risk metrics since this was not originally meant to be used as such. To assess the state of practice, security assessment tools, as well as data sources, were analysed. The results show that it is not trivial to use different data sets to run experiments that identify the frequency with which each risk factor identifies a vulnerability, which means that, according to the experiments, the usage of CVSS base score as a metric for risk was proven to be unsatisfactory practice.

5.1.2. Overview of Selected Threat and Risks

Cybercrime-as-a-Service (CCaaS) has been indicated as one of the main models to amplify the capacity of attackers to be successful with a cyber attack, which can impact directly at all of stakeholders previously mapped (cf. Section 2.2). Currently, anyone with the minimum background can contract services or obtain tools to start sophisticated and powerful cyber attacks to a target. Besides, hackers with certain expertise can use such a model to amplify and speed-up their attacks, thus enabling vast and dangerous attacks that can, for example, reflect directly in money loss and data leaking. The rising of IoT and, consequently, the growth in the number of devices,

also expands the attack surface. The CCaaS market includes botnets to execute large Distributed Denial-of-Service, malwares and exploits on-demand to obtain advantages (e.g., crypto mining), and also solutions that focus on the propagation of misinformation (i.e., bots that simulates legitimate users to share fake news).

The advance of attacks based on Artificial Intelligence (AI) also is a critical complaint for the next years. Different steps of the cyber attacks (e.g., vulnerabilities identification and social engineering) have been automatized by using state-of-the-art artificial intelligence techniques. Based on that, the cyber attacks are become more sophisticated and can many times surpass traditional security systems. These AI-based attacks can be a threat for many stakeholders (e.g., banks and governments sectors), impacting not only by infrastructure attacks, but also by using sophisticated social engineering techniques to cause damage and/or steal sensitive data, e.g., misinformation campaigns to influence in political scenarios, information leaks, and service interruption.

Cyber weapons developed to hit industrial systems and Supervisory Control and Data Acquisition (SCADA) systems are still a threat. This kind of attack can impact directly on critical government infrastructure (*e.g.,* Venezuela blackout on March 2019) and manufacturing industries. As critical infrastructure systems are not designed to be resilient to cyber attacks, the risks are growing according to cyber attacks are evolving, and legacy systems are still being used. In the past, for example, the Stuxnet threat revealed to the world how evolved is cyberwarfare by attacking Iran's nuclear weapon development. In the same context, the cyber espionage has been impacted directly on governments in different dimensions, such as leaking of sensitive information or also influencing directly on elections by focusing the attacks (*e.g.,* social engineering and malware) in people and devices involved directly with the election process.

The supply chain of popular software is also a massive target for attackers. Cyber attacks to compromise the supply chain to hit a broad audience have been arising in recent years. This focus on corrupt libraries or other components that are part of the software to insert backdoor and create vulnerabilities in software trust by everyone. The main focus of this kind of attack is to steal sensitive information from the victims without any suspect. Finally, the Cloud Providers, mainly companies that provide cloud storage, are one of the most targets for cyber attacks. As users and companies are migrating their data to the cloud, it is normal that with that, the cyber attacks migrate together. Several approaches of Cloud-based ransomware have been identified with the primary goal of obtaining financial advantage by encrypting data from one or more customers using such kind of service.

Table 34 provides an overview of the threats that compose different types of attacks and its main goals as well as the most affected stakeholders (*i.e.,* targets). These types of attacks are relevant from an economic view since they impact directly on the business models or profits of the stakeholders. It is noted, by considering the provided information, that general threats are being explored in different contexts according to the end-target, such as a malware that can be used to infect millions of devices in order to create botnets, while can also have ransomware functions with financial interests in determined targets.

Table 34 – Examples of type of attacks and its main goals

-	Attack Type	Main Goal	Targets
Cybercrime-as-a-Service	DDoS Malware Exploits Botnets Spam/Phishing	Amplify the access of attacks to any users and improve capacity to conduct attacks	Service providers, cloud providers, governments, end-users
Nation-state hacking	Social Engineering Malware Cyber-weapons focused on ICS/SCADA systems	Cyber espionage and sabotage	Governments and large companies
AI-based attacks	Vulnerabilities exploration Social Engineering Misinformation campaigns Phishing	Automation of some phases of the attacks	Service Providers, governments, small and large companies, banks
Supply chain attacks	Compromise libraries/software Insert vulnerabilities	Stealing data from a wide audience that trust in a software	Governments, small and large companies, banks, end-users
Cloud attacks	Malware (mainly Ransomware) Exploits DDoS attacks	Stealing of sensitive data, sabotage, and financial interest	Cloud providers, service providers, banks, small and big companies

5.1.3. Case Study: Bank Sector

Cybercrime is a term associated with activities related to the misuse of computer, information system, data, and cyberspace for personal and economic gain [82]. Cybercrimes have affected not only individuals but also groups and organizations, or even society as a whole. In the banking sector, the cybercrimes are committed using online technologies to illegally transfer or remove money to different account [83]. With the enhancement in technology such as ATM, online banking, the banking sector has witnessed different forms of cybercrimes like ATM frauds, Phishing, identity theft, DDoS, cyber money laundering, and credit card frauds. The threats and security breaches have highly increased in recent years due to the reason that banking increasingly relies on computer technologies and the internet to operate its businesses and market interactions [84]. As banks adopt modern trends of doing business, they have to protect themselves against cyber-crimes [83]. In general, all these frauds are executed with the ultimate aim to gain access to the user's bank account, steal funds, and transfer money to a different account [85]. Banking fraud is a major issue being experienced globally and is continuing to prove costly to Banks and its stakeholders [86]. Figure 15 shows the possible stakeholders that are involved in the Bank cybersecurity domain and the interaction among them, which is based on the model

defined in Chapter 2. The actors are categorized into four main categories, such as exploiters, victims, security providers, and regulators. The stakeholders identified and listed below are not exhaustive and can evolve according to CONCORDIA's pilots.

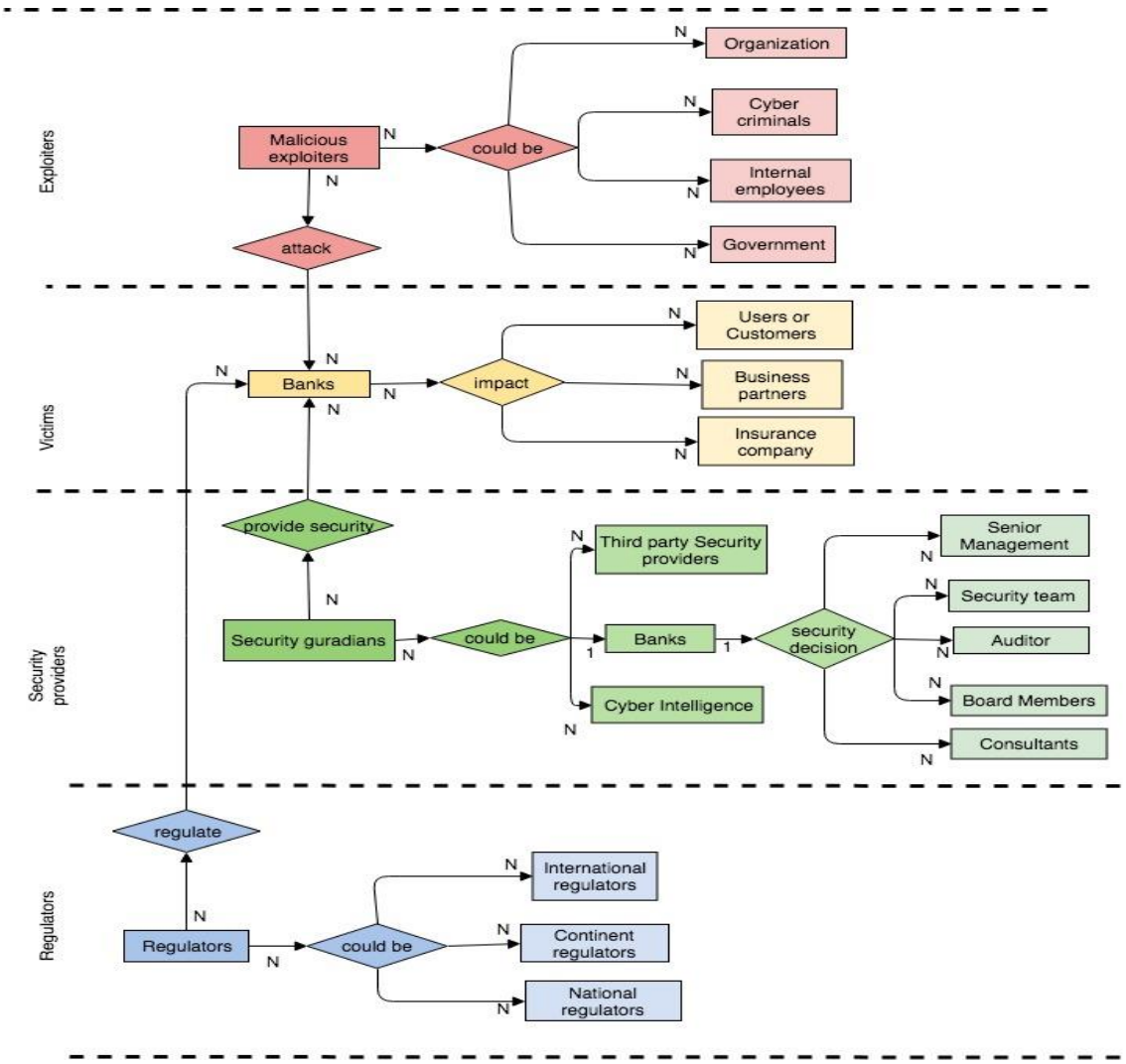


Figure 15 – Bank cybersecurity stakeholders

Malicious exploiters are usually motivated by political or financial gain or human factors such as revenge or curiosity [82]. Malicious exploiters range from the cybercriminals, internal employee, government, organization. Disgruntled internal employees are those who are working within the bank to leak out important information in order to harm the reputation of the bank. Internal employees inadvertently cause a data breach through carelessness or might intentionally cause the breach. They could be influenced by financial rewards or blackmail to steal valuable information [82]. Cybercriminals are highly organized and very knowledgeable who seek to find security holes in the system to overcome protection measures adopted by the banks for their own profit [85]. The malicious attempt could also be from the organization and government to breach the information system of the Banks.

When malicious exploiters attack the Banks, they could breach the confidentiality of user's or customer's data such as customer's bank details or bank's intellectual

property. The attack on the bank could have a direct or indirect impact on its customers, Business partners, and insurance company in terms of financial or identity fraud [82]. Customers are often concerned about privacy and identity theft. The exploiters might alter the customer's credit rating which could lead to that person's inability to secure the financial loan and could also prevent the authorized user from accessing his or her user account, data, or information. When such attacks take place, the banks are responsible for all these fraudulent activities perpetrated via the internet channel. Banks are responsible for reimbursing most customers losses [84]. Insurance company equalizes the cost when a cyber-threat event happens at an organization and also helps to prevent an attack and respond to mitigate when cybersecurity fails [87]. It helps the Banks to prepare for cyber threats by contributing to minimizing the said loss or damage and bringing the situation back to normal [88].

Security guardians help in mitigating banking frauds. They improve the existing banking system and help in removing the vulnerabilities. The security guardians could be the bank itself, third-party security provider hired by the bank to ensure security from the threats, or cyber intelligence. The security guardians within the bank could be the security team, board members, senior management, auditors, and consultants [85]. The sophistication of contemporary attacks requires a sophisticated response. The Banks ensure that they have the right resources to manage the cybersecurity risks. Therefore, the Banks increasingly look to the third-party cybersecurity solution provider to better manage the risk. Cyber intelligence could be professional external parties or internal. They obtain information about the different types of attacks targeting the organization. They assess and manage cyber risk. They enable the banks to respond to cyber threats with actionable cyber investigations and remediation [87]. The banks implement the security guideline, procedure, policy, and privacy components [84]. The security team within the bank is responsible for securing information and data. They create a cyber-threat protection strategy and build layers of security to protect the business process and data integrity. They are constantly vigilant, set to defend, and ready to respond creatively and rapidly in the event of an attack. They utilize the standards provided by the policymakers in their configuration management process and ensure compliance with frameworks and improve the security posture of their organization. Senior management could be part of the security planning process. They take input and guidance from their security team on security issues and are responsible for overall budgetary and strategic decisions [88].

Regulation in banking is the preservation of solvency and stability of the system [89]. Regulators make policies and adopt measures to protect banking platforms from cyber threats [84]. Banks must face compliance mandate or regulatory requirement, for example, the regulations such as Payment Card Industry Data Security Standard, National Institute of Standards and Technology, Cyber Essentials, EU General Data Protection Regulation. These regulations include requirements for data privacy. Banks must integrate compliance and regulations into their assessment. Regulation imposed by the regulators provide stability to the banking system and avoid the important negative consequences of panics [89]. For example, GDPR, determining strong laws and penalties, has introduced higher enforcement powers for regulators and greater privacy rights for the consumers.

5.2. Economic Analysis Approach

Cybersecurity concerns are one of the significant side effects of an increasingly interconnected world, which inevitably put economic factors into perspective either directly or indirectly. In this context, it is imperative to understand the significant dependencies between complex and distributed systems (*e.g.*, supply-chain), as well as security and safety risks associated with each actor. SEConomy is a framework to measure economic impact of cybersecurity activities in a distributed ecosystem with several actors. Through the mapping of actors, responsibilities, inter-dependencies, and risks, it is possible to develop specific economic models, which can provide in a combined manner an accurate picture of cybersecurity economic impacts.

It is imperative to understand the economics behind cybersecurity activities. For example, the United States of America (USA) released in 2018 an estimate of costs related to malicious cyber activities of around 57 and 109 billion USD for incidents appearing only in 2016 [90]. These numbers involve not only losses at the initial target and economically linked firms derived from attacks, but also incurs in costs involving the maintenance and improvement of systems security [91]. Further, Moore [92] corroborates with the U.S.A. estimate, predicting in 2018 a cost of 114 and 124 billion USD in 2019, representing an increase of 8% for one country only. While cost numbers are not precise on a global scale, there are estimates that predict costs related to cybersecurity activities to exceed 1 trillion USD cumulatively for the five years from 2017-2021 [2], taking into account the growing number of Internet of Things (IoT) devices.

Systems often fail because organizations do not consider the full costs of failure, which includes two critical categories: security (prevention of malicious activities) and safety (prevention of accidents or faults) [93]. Security investments are typically complex because malicious activities typically expose externalities as a result of underinvestment in cybersecurity, *i.e.*, they usually exploit vulnerabilities unforeseen in the design space. Safety, however, originates from requirements, which take systems failures due to unexpected events (*i.e.,* natural disaster or human failures) into account to prevent the loss of lives. In a setup where major actors want to minimize costs while maximizing security and safety aspects [18, 25], it is essential to understand all key cybersecurity impacts or the lack thereof within a specifically determined economy [94].

5.2.1. Background and Related Work

Although reasons behind cyber attacks can be widely diverse, ranging from identity phishing and information security breaches to the exploiting of vulnerabilities on Critical National Infrastructures (CNI), it is notorious that these attacks have become increasingly driven by financial motives. Therefore, the related work focus here is on models analyzing economic aspects behind cyber attacks. For this reason, the United States Department of Defense declares the cyberspace as the fifth dimension of defense areas, complementing the traditional land, water, sea, and air warfare dimensions [95].

A purely economic analysis was released in 2018 by the U.S. White House [96] revealing estimates of economic impacts in the year of 2016, the year in which one of the largest Distributed Denial-of-Service (DDoS) attack was launched on the content

provider Dyn-DNS, which interrupted the delivery of content for significant Internet services (*e.g.,* Twitter, PayPal, and Spotify) for a few hours. These numbers corroborate with the influence of cyber attacks in the economy (whether it is a nation or large private organizations).

The AFCEA, which is a non-profit organization serving military, government, industry and academia, presented a discussion on cybersecurity economics in a practical framework [97]. The framework guides private organizations and the U.S. government highlighting principles to guide investments mapping risks their associated economic impacts. Threats are categorized according to its complexity *i.e.,* sophisticated or not and its mission criticality *i.e.,* define how certain vulnerability could impair a service/process.

Concerning the mapping of risks and threats (without a direct analysis of economic impacts), the National Institute for Standards and Technology (NIST) developed a model for guiding the investment in cybersecurity countermeasures. Specifically, NIST's Special Publication 800-37 [98] [99] and 800-53 [100] define the Cyber security Risk Management Framework (RMF) including a method for assessing the implementation of controls to mitigate risk. Although 800-37 and 800-53 do not present an analysis directly related to economic aspects, the NIST framework to classify risks, as well as the AFCEA mapping of risks, allows for the establishment of economic models based on threats.

Moore [95] discusses under economic directions impacts of cyber attacks in a national context. He bases the analysis of attacks on Critical National Infrastructures that could harm or collapse its economy. Also, Moore puts those principles into perspective, which motivate these attacks and policy options to prevent or respond to attacks. Thus, he proposes regulatory options to overcome barriers in cybersecurity, such as safety regulation, post liability, and others. According to the knowledge of the authors economically-driven frameworks for a suitable and detailed assessment are not yet in place.

Aiming at the evaluation of economic risks, Rich *et al.* [101] proposes a proactive model to simulate economic risks of CNI's with integrated operations, *i.e.*, that links many vendors, suppliers into the same ecosystem. Thus, the authors seek to map inter-dependencies amongst actors to establish a causal relation, which can then be used to estimate economic risk under various scenarios. However, despite of providing a view on the inter-dependencies between the actors, the proposed model does not consider problems that may later occur because of a rush to attain initial economic gains [86].

5.2.2. SEConomy Framework

In ecosystems involving different actors ensuring certain security/safety levels is not a straightforward task. Due to the number of participants potentially managing sensitive information or critical tasks, the risk assessment of a supply chain, for example, becomes complicated [2, 7]. The framework proposed in Figure 16 takes into consideration the economic analysis of complex systems by structuring to five stages of mapping and modeling, allowing the creation of economic models with fine-grained estimates.

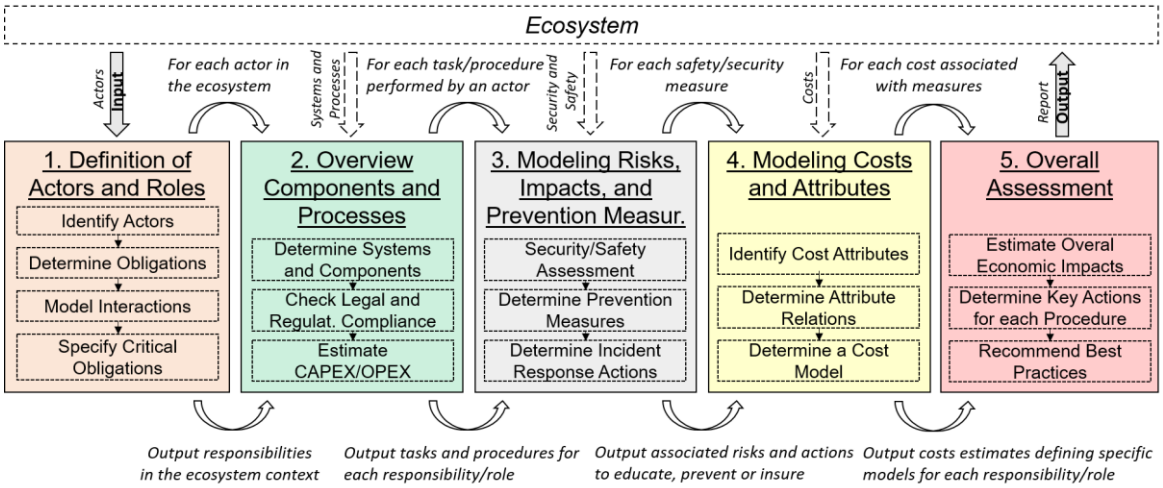


Figure 16 – SEConomy framework

Stage 1 is concerned with the definition of actors and their functions, whose interactions should be mapped as well as which critical functions should be specified. Stage 2 to determines which systems/components and processes are performed by these actors and their legal implications for an initial attribution of investment and operating costs. Based on the mapping of actors, systems, and processes, Stage 3 is responsible for the production of risk models and possible impacts as well as preventive and training measures based, for example, on NIST risk assessment guides 800-37 and 800-53 [15, 14]. Stage 4 takes into consideration this risk analysis to map costs in a fine-grained manner, i.e., for each risk of each task performed by each actor previously mapped. Lastly, Stage 5 gathers outputs of Stage 4 to a produce general feedback in terms of overall economic impacts, the determination of improvement actions, and best practices.

5.2.2.1. Definition of Actors and Roles

It is possible to consider as input, for example, the production chain of an aircraft system as a complex ecosystem that requires an assurance of security and safety levels based on a detailed risk analysis of all its major control components. A comparative between Airbus and Boeing supply-chains [102] have shown, for example, that the manufacture of the wide-body Airbus A300 and Boeing 737 aircraft involves multiple suppliers from 30 and 67 countries, respectively. Hence, it is essential in Stage 1 to identify all actors involved in the supply chain, and their roles (and determination of which tasks/functions are critical).

Figure 17 shows as a first step the identification of actors involved (*e.g.,* producers of flight control systems, software for engines) as well as their obligations and interactions with other actors. In this regard, Boeing and NIST defined a guideline on cybersecurity supply-chain risk management [85], where the organizations that provide software for their aircrafts must undergo a rigorous inspection process.

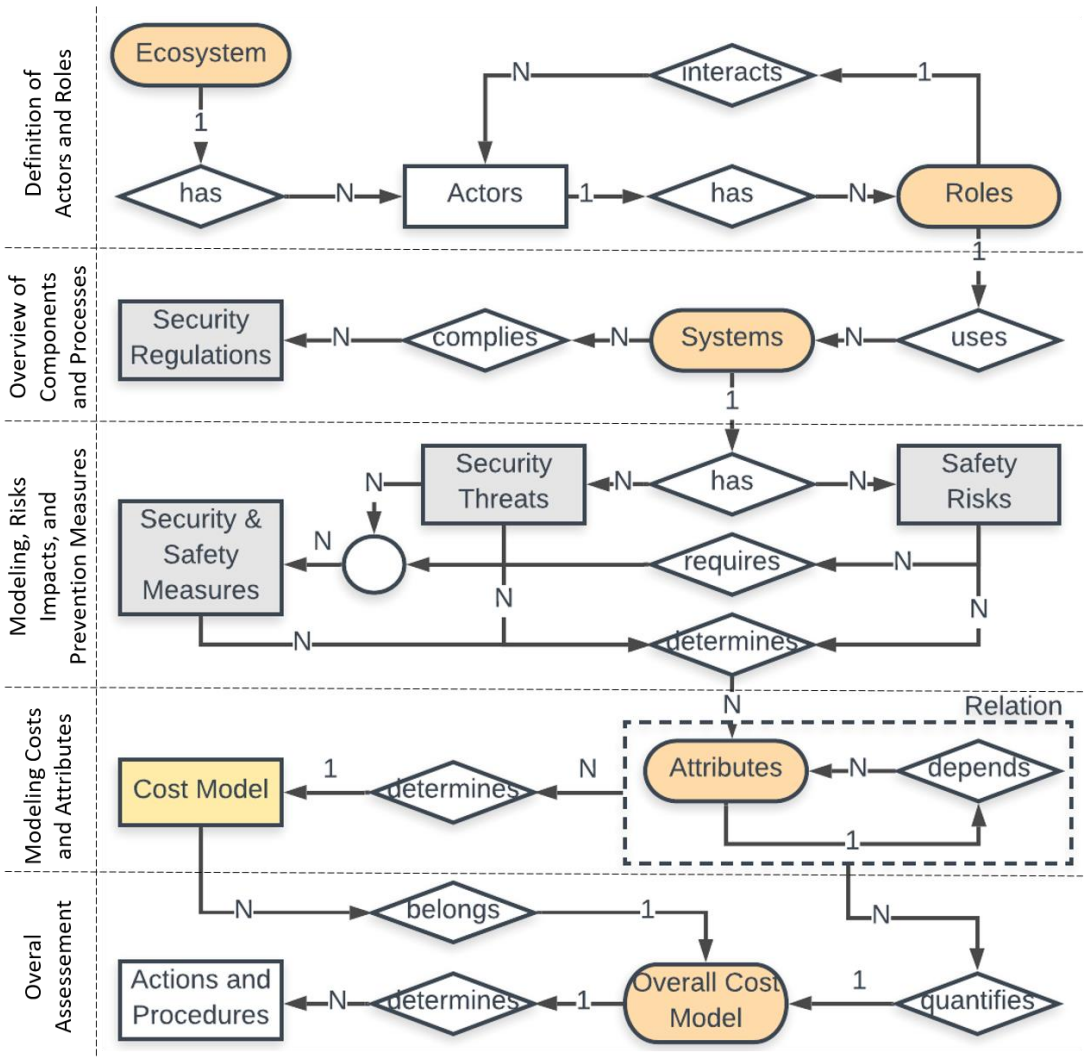


Figure 17 – SEConomy entity-relation model between stages

5.2.2.2. Overview of Components and Processes

Among the actors' obligations, it is necessary to identify the ones whose roles involve critical processes/systems and components. In the case of the aviation sector, these include producers of navigation and communication systems, traffic collision avoidance, and Fly-By-Wire (FBW) systems [85]. The mapping of systems and components is crucial for the analysis of risk, which involves not only technical, but also human aspects. For example, critical systems require not only a guarantee of safety and security aspects, but also whether actors operating these systems can monitor and react. Also, these systems should comply with security and safety regulations/recommendations, which measurably lead to implications of Capital or Operational Expenditures (CAPEX/OPEX). For example, the Airbus A320 FBW system uses five different computers running four flight control software packages to ensure reliability/availability [99], complying with the U.S.A. Federal Aviation Administration agency requirements for safety matters in the design of FBW systems.

5.2.2.3. Modeling Risks, Impacts, and Prevention Measures

As presented in Figure 17, each system requires an analysis of its potential security/safety threats, and measures to respond to these threats. A rational approach in defining what is "appropriate" involves *(a)* identification of risks by examining

potential vulnerabilities and their chances of a successful exploitation, *(b)* the cost of these results if vulnerabilities are exploited, and (c) the cost of mitigating vulnerabilities. The analysis of threats/risks can be based, for example, on frameworks such as the NIST 800-37/800-53 [15, 14]. Also, it is necessary to determine measures to be taken in response to each threat and their associated costs. For example, the ROI (Return On Investment) of proactive approaches (education/training of personnel, prevention, and redundancy of critical systems) is a better economic alternative than reactive approaches (active monitoring and recovery). However, the remaining difficulty is to determine efficiently thresholds for CAPEX and OPEX.

5.2.2.4. Modeling Costs and Attributes

The challenge of this stage is to translate risks and several measures of security in terms of costs, which includes the mapping of interdependence between failures. In this regard, such correlations can be mapped as the correlation between two Bernoulli random variables (A, B) [103]:

$$MD(A,B) = p_X = \frac{p_X - p_A * p_B}{\sqrt{p_A(1-p_A) * p_B(1-p_B)}} \quad (1)$$

pA and *pB* provide the probability of failure in a system A and B, respectively. *pX* describes the probability of a failure in both A and B. The SECeconomy approach is based on the ROSI (Return On Security Investment) model [104] that determines the cost/benefit ratio related to security strategies [95, 105]: Threat exposure Costs (*Tcosts*) in Eqn. (2) estimates the total cost of vulnerabilities given their probable occurrences within a time frame $deltaT(prob\,(Nocurrences)/time)$:

$$TEC(A,B) = \Delta T * \left(\sum_{i=1}^{N_{Threats}} ThreatCost * MD(A,B) \right) \quad (2)$$

There are two significant challenges to quantify vulnerability costs in Eqn. (2): *(a)* economic impacts of vulnerabilities identified (*ThreatCost*) and *(b)* potential impacts given by *MD(A,B)* on the *K* dependent systems. However, impacts on dependencies are equally not straightforward to be estimated, because the failure of one component may not always lead to the failure of another dependent system (*e.g.,* the use of a layered defense or a "sufficient" redundancy level may reduce such risks). For example, a failure in a fuel control subsystem may not always impair an aircraft's turbine, because a redundancy level of computers exists to provide input for the FBW and, typically, more than one turbine is used in a commercial wide/narrow-body aircraft.

These costs are mapped based on proactive and reactive measures. The Proactive Mitigation Cost (PMC) presented in Eqn. (3) is relatively simpler than the reactive costs. This is because the risk vector is foreseen in assessment guides/frameworks, and their mitigation actions and associated *ProactiveCost* are taken into account at

$$PMC(A) = \sum_{i=1}^{N_{Threat}} \Delta T * (ProactiveCost + InsuranceCost) \quad (3)$$

system design time. Additionally, it is possible to include an *InsuranceCost* that allows the recovery of unforeseen costs.

The Reactive Mitigation Cost (RMC) are challenging to be estimated, since these failures or vulnerabilities are typically originated from unforeseen design aspects, implying on a *ReactiveCost* to mitigate the threat and its consequences on potentially connected systems. However, the cost of reactive mitigation do not always present a linear relation with time, *i.e.*, the longer the time to perform a reactive measure not always mean that its cost will be higher. For example, in case of a vulnerability in which an attacker gains privileged access to a private network, this does not always imply that the longer time, the higher the victim's monetary loss. However, in case of a DDoS attack, there is a temporal relation taking into account that the greater the time a content provider do not provide service, the greater will be the economic damage on the victim.

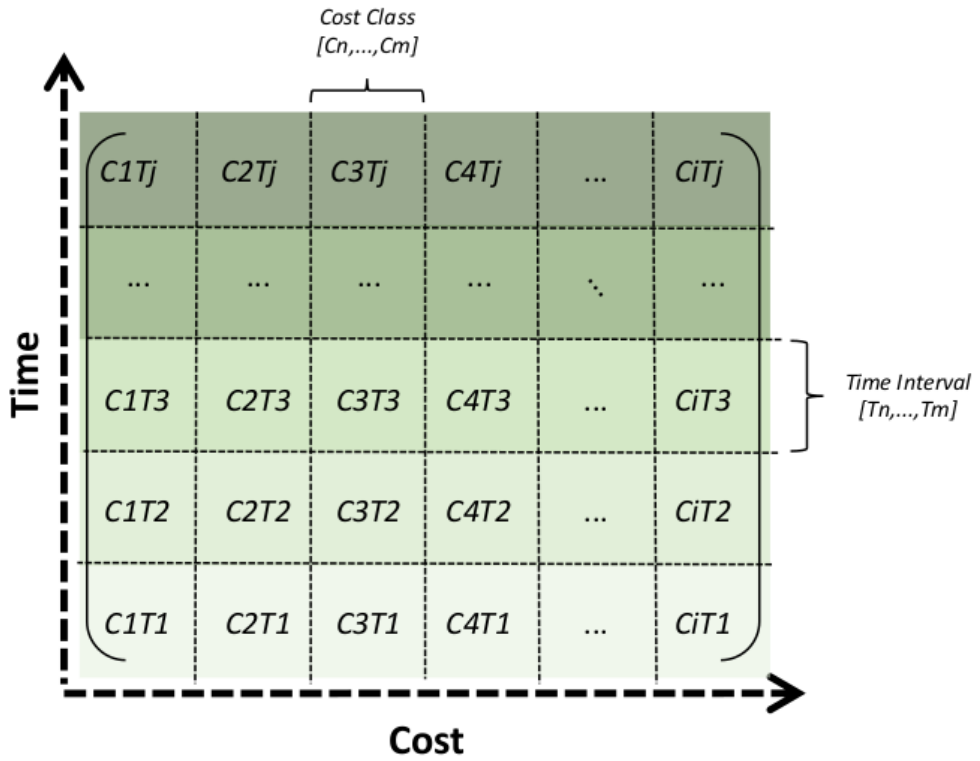


Figure 18 – MTC matrix describing time-cost classes, where C_1T_1 classes represent a cost function $f(x, y)$

Previous work proposed a type of fuzzy model, which translates local dynamics in different state space regions represented by linear models. Based on their proposal, it is defined in SEConomy different classes of RMC costs C_i in function of time T_j, whereas each class has its own cost function. Similarly to PM_{costs}, there is also the alternative to adopt an insurance model to cover potential impacts of subsystems or directly connected systems. Further, the cost of a reactive measure (and potential effects dependent systems) can be mapped in the *MTC* matrix (Figure 18). On the one hand, data breaches are not time-sensitive, but may incur in high costs depending on how sensitive is the exposed information. Hence, a data breach could occur in a time T_1 with a cost C_i, in which *i* would define the relevance of the exposed information. On the other hand, a DDoS attack is time-sensitive meaning that the longer is the time

without providing services (*i.e.,* higher T_j imply in higher C_i), the higher is the economic damage expressed by the time-cost category function.

In detail, a typical fuzzy rule defined is expressed by an Event-Condition-Action rule, where the action is expressed by a function:

$$If\ x\ is\ C\ and\ y\ is\ T\ Then\ Z = f(x,y) \tag{4}$$

C and T are fuzzy categories and *z=f(x,y)* is the function determined for that $C_iT_i$category in the matrix. Further, C and T are defined, respectively, in terms of cost and time, in which C_iT_i classes are associated with a linear cost function in the *MTC* matrix. Cost classes are defined as $C_i = [C_n, C_m]$, where *n* and *m* belongs to $R \geq 0$ and Time C_z, ..., C_w, where *z* and *w* correspond to a class time interval defined in *N*.For example, a *RMC* that happened during a time interval "T1", can be associated, depending on the involved systems, with a cost category C_1 defined as "low cost". Thus, a $C_1T_1$is associated with a cost function of $z = f(C_1, T_1)$, which describes a price category. As previously stated, a C_1T_1 category could express, for example, a data breach. Thus, time-cost relations can be expressed in terms classes of costs functions mapped in the MTC matrix (*cf.* Fig. 5) . However, to foretell the economic impact on dependent systems, which relies on the probabilistic dependence of Eqn. (1), it is necessary to consider failures/vulnerabilities which can trigger cascading failures on correlated systems/subsystems potentially impairing the functioning of the entire system, *c.f.* Eqn. (5).

$$RMC(A,B) = \sum_{i=1}^{\mathrm{N}_{System}} \left(\sum_{i=1}^{\mathrm{N}_{Threat}} \underbrace{MD(A,B)}_{\substack{\text{Probability of} \\ \text{Cascade Failures}}} * \overbrace{MTC[C_i][T_j]}^{\substack{\text{Cost Function} \\ \text{f(x,y)}}} \right) \tag{5}$$

To benchmark the security investments is necessary to take into account initial investments in security (*i.e., PMC* proactive measures) of a system in a given time-frame *Δ*T (*e.g.,* monthly), multiplied by the risks, threats which the system is exposed (T_{cost}) considering its probable occurrence (*RMC*). Finally, Eqn. (6) calculates ROSI for a single system taking as input Threat (T_{cost}), Mitigation (M_{cost}), and initial investments in security.

$$ROSI = \sum_{i=1}^{\mathrm{N}_{System}} \frac{(T_{costs} * RMC) - PMC}{PMC} \tag{6}$$

In the last stage, it is necessary to calculate the overall economic impact based on ROSI from all *S* systems, required by *R* roles of *A* actors. Therefore, as illustrated in Figure 17, the *N* economic models will define an overall estimate of costs for the entire ecosystem, as illustrated by Algorithm 1.

Algorithm 1: Overall Economic Assessment (OEA)

```
1 begin
2     for each Actor ∈ Ecosystem:
3         for each Role ∈ Actor:
4             for each System ∈ Role:
                  /* Correlation between linked systems in Equation 1  */
5                 p(x) ← dependence(System, ∀ linkedSystems)
                  /* Estimate exposure costs in Equation 2             */
6                 threat_costs ← T_costs(A, p(x))
                  /* Estimate mitigation (Proactive and Reactive) costs
                     in Equation 3                                     */
7                 mitigation_costs ← PMCcosts(A)
8                 mitigation_costs ← RMCcosts(A, p(x))
                  /* Get Overal Economic Assessment (OEA) in Equation 4
                     */
9                 OEA ← ROSI(threat_costs, mitigation_costs, InitSecCost)
```

5.2.3. Case Study: Ransomware

Ransomware is a type of malware which tries to extort money from its victim. There are generally two courses of action ransomware takes: either it will try to encrypt all (or all important) files on every machine it infects, using an encryption key to which only the ransomware operator has the decryption key; or it will lock a device making it unusable for the legitimate user. An overlay screen is shown in both cases, detailing the fact that a ransomware infected the device and including steps on how to pay a ransom to the operator (generally using cryptocurrency), with the promise to decrypt the data again or making the device useable again after successful payment [106]. The device locking type of ransomware is usually only effective on mobile devices like smartphones and tablets. As companies primarily suffer from the data encryption type of ransomware and have less problems just replacing an infected phone or tablet, the rest of this document focuses on encrypting ransomware.

In this case study, SEConomy framework to determine *(a)* the actors and roles, *(b)* components and process, and *(c)* risks and impacts of a ransomware attack in a company. Based on that, the different costs involved can be calculated in order to provide an overall economic assessment.

5.2.3.1. Actors and Roles

First and foremost, the central actor of this model is a company that wants its business protected from cyber threats. This could be any business, both industrial (*e.g.*, a goods manufacturer or a processing plant) venture and non-productive industry enterprise (*e.g.*, retailer or web service provider). The only limitation on the type of business is that the company would have an IT infrastructure at all over which it manages at least parts of its business or associated bureaucracy or correspondence, which should be valid for most modern ventures today. The company has an intent to keep its business running and fulfill all contractual obligations with its customers and business partners.

Next, an insurance issuer is trying to sell cyber insurance to the company. The issuer tries at the same time to be profitable, give fair risk-based premiums to insurance

buyers while keeping its own risk low, and have premiums low enough so the company will buy its insurance product. If an insured company suffers a ransomware attack, the insurance needs to pay out the covered damages.

A competitor of the company was introduced into the model to represent the fact that the company is trying to survive in a competitive market and cannot only build on a monopoly position with zero risk of setbacks following business impacts due to ransomware attacks. The competitor does not only work as a business antagonist of the company, but it also might want to benefit from the insurance of the same type as the company, which it expects to have a fair premium directly related to its incident risk and not influenceable by the company.

Finally, an evil actor in the ecosystem is the malware operator who is trying to make money by attacking the IT infrastructure of both the company and its competitor with its ransomware, trying to extort money. The malware operator does operate outside of legality and, as such, does not have any obligations to anyone, including the fact that even if a company pays the ransom after being attacked, the malware operator does not necessarily hand out decryption keys or give back access to data. It is worth to note that this analysis does not consider the malware operator in details such as its own return on investment or cost of building malware, it is only assumed to be an entity able to conduct a malware attack and succeed based on whether the information security level of its victim is enough to prevent the attack or not.

5.2.3.2. Components and Processes

As there is not verified secure software infrastructure stack used in real-world business applications, this analysis assumes that the complexity of software in use is increasing together with the number of exploitable security threats. For example, the EternalBlue exploit in 2017 affected all Microsoft Windows-based operating systems, which a vast majority of businesses use on their employee's machines and many also in their server infrastructure. That single exploit led to two big waves of ransomware attacks, WannaCry and NotPetya. Both attacks could be prevented by having installed regular operating system updates. A successful ransomware attack on the company would result in data loss and business discontinuity.

The insurance issuer offers insurance against ransomware attacks to the company, fixing a premium depending on its assessment of the company's IT security. Depending on the jurisdiction under which the insurance operates, parts of the premium will flow to counter insurance. However, as we want to model the risks and obligations of the company primarily, it is just assumed that this and similar legal obligations of the insurer are just included in the premium.

As part of the insurance contract, the company is obligated to give accurate and comprehensive self-assessment about its IT infrastructure and security to the insurer. Based on this report, the insurance company fixes the insurance premium for the company. The malware operator tries to attack the company with its ransomware. The success of this attack depends on the actual IT security of the company, which might differ from the security self-assessment reported to the insurer, whether intentional or not. Intentional might happen as part of the moral hazard problem detailed earlier. As most countries have no general compliance regulations about information security

yet, it is assumed that the company does not have to go further in information security obligations than the assessment to the insurance company.

However, the company can try to improve its premium by implementing risk assessment improvements as given by the insurance self-assessment procedure (*e.g.*, the insurance might lower its premium for the same coverage if the company appoints a security manager), and it can try to reduce the risk of a successful attack by implementing some security best practices, which might or might not overlap with the incentives set by the insurance company.

5.2.3.3. Risks, Impacts, and Prevention Measures

Modeling impacts of specific security tactics and prevention measures are difficult as, for most options, there is no existing research or data available about how a specific action affects the information security of a company, and more specifically, how it would reduce the risk of a ransomware attack. An extensive study about which points of a cyber insurance self-assessment do influence the security level by how much seems not available, as is not a comprehensive study of all possible security best practices. Therefore, this part focuses on measures correctly able to prevent ransomware attacks (not necessarily exclusive to ransomware), which are also known to work in practice.

First, the regular and timely application of security updates to software is a key measure that would have prevented ransomware infection for victims of both WannaCry and NotPetya mentioned earlier. Besides, personnel cybersecurity training is important since ransomwares can also spreads by exploiting the humans with access to the target (e.g., phishing emails and social engineering). Therefore, not only the application of software updates but also the existence of an automated business process and responsible person or team for it is essential. Then, the central action which offsets any ransomware attack and reduces the damage to a minimum if done right is the implementation of regular offsite backups of all data and computer infrastructure. Here as well, there should be an automated business process ensuring regular backups and testing restoration as well as a responsible person or team.

Having a single complete and up-to-date backup of all business data might not be enough to survive a ransomware attack. This is because the ransomware might already have been present at the time the backup is made and has already encrypted or deleted some data which found into the backup in its altered state. A good strategy would be to have multiple snapshots of different points in time, for example, doing retention of daily backups for a determined period.

Another procedure that reduces the ransomware infection risk is a switch to more secure operating systems, for example, from Microsoft Windows to GNU/Linux-based operating systems. This is not an easy measure and includes considerably more effort to implement, to the point of potentially requiring a redesign of the whole business logic. Therefore it is not seen as an option to implement for most businesses. However, it should be included in the security assessment by a cyber insurance issuer to give lower premiums to users of more secure operating systems.

5.2.3.4. Costs and Attributes

According to the 2017 Accenture report [90], the average annualized cybercrime cost weighted by attack frequency amounts to $88,496 for each company, which serves as an estimation of the overall threat exposure cost. This figure includes the possibility that a company could suffer from several ransomware attacks in the same year. The number depends directly on the size and also the type of business, but it is a starting point for estimating potential losses. To the best of the author's knowledge, there seems to be no study that sets the annual loss due to ransomware infection concerning the business size, or rather, its revenue, which would help with much better estimation. Such a report, which includes reported data from 254 companies, also finds that, on average, it takes a company 23.1 days to recover from a ransomware infection; it does, however, not state precisely at which point a company deems the incident as resolved. Taking such information into account, different costs can be calculated in order to obtain the overall estimation of costs, as presented in the rest of this section.

5.2.3.4.1. Proactive Mitigation Cost

For the mitigation strategy of doing regular backups of business data, as mentioned in Section 4.3, the cost of renting backup storage comes at the price of $480 USD per 10TB of data [106]. The 10TB is in the order of magnitude which companies are found to have as business data on average: A report of 2018 [107] gives a median amount of business data of 11.1TB, while their 2017 report did find a lower 6TB median.

Based on these numbers, a proactive mitigation cost (PMC) of $48 per TB of data can be calculated, which does not include recurring cost for backup software and the non-recurring cost of setting up a business workflow for automated backups. For the cost of backup software, some backup solution vendors include or bundle their software solution with storage space, which means the cost per data already includes the software cost. Even in the case when the company has full backups available, it might not be able to resume business as usual after a ransomware attack immediately. Usually, many time needs to be spent replaying the backups, doing attack vector forensics and recovering data not backed up (which was generated between the last clean backup and the infection). There is, however, not any detailed data available about the recovery time of a company after suffering from ransomware infection in the case of available backups. It is therefore assumed this kind of downtime can be neglected, or more precisely, would be already included in the average daily revenue.

The idea of having multiple backup snapshots, as discussed before, would, of course, multiply the storage size needed; on the other hand, redundancy reduction techniques such as incremental backups minimize the overhead of multiple backups. For the calculation of backup storage costs, it is assumed that the total amount of data for all snapshots stored is included in the amount of data used in the calculation.
Finally, to the best of the author's knowledge, there seems to be no data available on the cost of a real-world cyber insurance premium. The same is for the amount of coverage which cyber insurance gives. For both, only a variable is used in the further examination.

5.2.3.4.2. Reactive Mitigation Cost

Reactive mitigation of a ransomware infection includes the cost of fixing or replacing the computer infrastructure, probably hiring an external security consultant, and, most importantly, loss due to business discontinuity.

The attack cost due to business discontinuity is assumed to be linear in downtime, that is the time until the company has recovered from an attack and can continue its daily business. From the average recovery time of 23.1 days mentioned before, we can calculate the discontinuity cost as 23.1 times the average daily revenue to get an estimate of the expected loss. More generally, the reactive mitigation cost (RMC) can be calculated as expected downtime times average daily revenue. As an example, from the data by [106], if a single hotel of the Marriot chain would suffer from a ransomware attack resulting in 23.1 days downtime, with their daily sales volume of $9,095.59 USD the lost revenue would accord to $210,108.129 USD.

On the other hand, if the company has cyber insurance which covers all or part of the loss due to business discontinuity, the reactive mitigation cost would be much lower. For example, if cyber insurance covers a fixed 90% of revenue lost during downtime, the reactive mitigation cost can be set to 0.1 times the downtime times expected daily revenue.

5.2.3.4.3. ROSI

For estimating whether investing in a security measure would outweigh its cost for the company, the Return On Security Investment (ROSI) can be calculated. The following calculations are done for a timeframe of a year, meaning the backup cost is yearly cost, and downtime is given in days per year. For simplification, the reference timeframe has already been eliminated in the following formulas.

To estimate the proactive measure of doing data backups, the *ROSI* can be calculated as:

$$ROSI_{backups} = \frac{downtime[d] * daily\ revenue[\$/d] - data[TB] * backup\ cost[\$/TB]}{data[TB] * backup\ cost[\$/TB]} \quad (1)$$

In Equation 1, downtime is given in days *[d]* and refers to the time period during which the company was unable to generate revenue due to a ransomware attack; daily revenue of the company is given as dollars per day *[$/d]*; the amount of data which the company needs to protect is measured in terabytes *[TB]*, and the backup cost is given in dollars per terabyte of data *[$/TB]*. The term downtime times daily revenue is the reactive mitigation cost (RMC) in the *ROSI* calculation, while the term data times the backup cost is the proactive mitigation cost (PMC).

If the company has a cyber insurance against ransomware attacks, the *ROSI* in case of a ransomware attack with a constant coverage factor (*e.g.*, 90% of downtime losses) needs to be calculated with an additional term in the PMC to make up for the part which is not covered by the insurance and has to be absorbed by the company in any case:

$$ROSI_{insurance} = \frac{RMC - (PMC + (1 - coverage\ factor) * RMC)}{PMC + (1 - coverage\ factor) * RMC} = \frac{coverage\ factor * RMC - PMC}{PMC + (1 - coverage\ factor) * RMC}$$

$$= \frac{coverage\ factor * downtime[d] * daily\ revenue[\$/d] - insurance\ cost[\$]}{insurance\ cost[\$] + (1 - coverage\ factor) * downtime[d] * daily\ revenue[\$/d]} \quad (2)$$

In Equation 2, the *PMC* term is extended by an amount depending on the *RMC* and the coverage factor. The *RMC* again is downtime times daily revenue, whereas the *PMC* for cyber insurance can be taken as the insurance cost given in dollars.

An interesting question now is whether the company is still incentivized to invest in backups when it already has cyber insurance. For this, we calculate the *ROSI* for doing backups in the case where insurance is present as:

$$ROSI_{backups|insurance} = \frac{insurance\ cost[\$] + (1 - coverage\ factor) * downtime[d] * daily\ revenue[\$/d] - (PMC_{backups} + insurance\ cost[\$])}{PMC_{backups} + insurance\ cost[\$]}$$

$$= \frac{(1 - coverage\ factor) * downtime[d] * daily\ revenue[\$/d] - data[TB] * backup\ cost[\$/TB]}{data[TB] * backup\ cost[\$/TB] + insurance\ cost[\$]} \quad (3)$$

In Equation 3, the *RMC* term needs to include the insurance cost, as the existence of insurance is given and needs to be paid independent of whether the company is doing backups also, and we are only interested in the return on backups. The *PMC* now amounts to the total of both backup and insurance *PMC*.

Whether a *ROSI* is profitable means that the fraction is bigger than one, thus, the profit is bigger than the investment. To achieve such a *ROSI* bigger than one, we can calculate the relationship between backup cost, insurance cost and expected loss given a fixed insurance coverage factor as:

$$ROSI_{backups|insurance} > 1 \Rightarrow (1 - coverage\ factor) > \frac{insurance\ cost[\$] + 2 * data[TB] * backup\ cost[\$/TB]}{downtime[d] * daily\ revenue[\$/d]} \quad (4)$$

In Equation 4, the result from Equation 3 is rearranged to get the coverage factor term on the left side. Therefore, *(1 – coverage factor)* is the part of the downtime loss, which is not covered by the insurance, and therefore the company would have to pay by itself. Explained more intuitively, this means that the sum of insurance and double backup cost should be smaller than the remainder of the downtime loss not covered by insurance. The factor two in front of the backup cost comes from the fact that the term appears in both numerator and denominator of the *ROSI* calculation; meaning that we care about the excess cost of losses over backup cost versus backup cost, and not just the relationship between downtime loss and backup cost.

The opposite question, whether a company would still buy cyber insurance when having a backup system in place, cannot be answered by this model, because as discussed above, the remaining cost of a ransomware infection when doing regular backups is assumed to be negligible due to the lack of real-world data.

5.2.3.5. Overall Economic Assessment

For the existing data points given before, we can try to find a numerical value for the formula in the previous section. The *ROSI* for doing backups with 23.1 days downtime, daily revenue of $ 9,095.59 USD, 11.1TB of business data, and backup cost of $48 USD per TB, we get a *ROSI* equal to 393.35.

The formula for calculating ROSI when using cyber insurance is limited upper independent of insurance cost by the fraction *c/(1-c)*, where c is the coverage factor. This means insurance with coverage of 90% can get a maximum ROSI of 9 when the insurance cost is at *zero*. However, given the assumptions made for the two ROSI formulas, insurance cannot come close to backups. An insurance coverage, which gives an attractive ROSI, coverage needs to be close to 100%; or instead of a constant factor switched to fixed baseline retention, possibly dependent on annual insurance cost.

For the particular case of cyber insurance with full coverage, with the given downtime and daily revenue, to get the same *ROSI* as with backups the insurance cost would need to be a mere $532.80 USD (per year), which equals the cost of backups for 11.1TB of data used above.

5.2.4. Summary

The predictions for 2019 are emphatic in affirm that the Cyber-crime-as-a-Service are stronger than ever [1]. This model is one key factor for the growth of the cybercrime ecosystem and, consequently, can impact negatively in the global and local economy. The misinformation campaigns around the world (e.g., Russia playbook [95]and Brazil`s presidential race), as well as the nation-state hacking, are becoming as an emergency for the next few years. Also, the number of IoT attacks is rising faster as the IoT networks are becoming a reality. Thus, the academia and industry should spend efforts to analyse not only risks for companies and its stakeholders but also the impacts of those threats on the economy and society as a whole. Most of such impacts may be reduced by increasing the investments in protection services, adequate cybersecurity planning for companies (e.g., risk analysis and training of response teams), and education of the end-users.

As support for the planning and decision process for cybersecurity, the SEConomy framework was introduced to detail economic estimates for security measures in complex distributed systems. Such framework can be used for stakeholders, as those mapped in Section 2 (e.g., the bank and telecom sectors), to evaluate the drawbacks and advantages of cybersecurity approaches, taking into account their business models and risks involved. Thus, such a framework is an initial step to define an overall model for economic perspectives verifications.

However, although SEConomy can provide estimates based on historical events and probabilities, failures and vulnerabilities in critical systems typically result in failures of sub-components or related systems, impacting the overall costs. For example, despite all recent technological advances, the introduction of a new warning component in the Boeing 737 Max caused two accidents with hundreds of fatalities [91]. Specialists stated that a software failure (*i.e.,* not properly implemented/tested) in the Angle-Of-Attack (AOA) sensors were triggering the flight control system to push the nose of the aircraft down repeatedly. In this regard, the calculation of risks through mutual vulnerability exposure along with other horizontal (i.e., subsystems of a system) and vertical (i.e., systems of other actor relations) is a complex task of potential security and safety consequences.

6. Summary

This deliverable presented a first report on cybersecurity threats and attacks, as well as a first outlook on their trends, focusing on the domains of interest for CONCORDIA, namely, network-centric, system-centric, application-centric, data-centric, user-centric, IoT/Device-centric security. All activities and analysis that are built around the threat reporting process in this deliverable have been considered from technological, legal, and economics perspectives. Technological perspective (Chapter 3 and Appendices A.1-A.6) discussed the status of cybersecurity, evaluating new trends in cybersecurity and focusing on emerging threats and evolving attacks. The legal perspective (Chapter 4) discussed the legal implications of cybersecurity, the regulatory environment and resulting obligations (e.g., NIS Directive and GDPR). The economic perspective (Chapter 5) approach mapped the cybersecurity actors, responsibilities, inter-dependencies, and risks, developing specific economic models.

This deliverable is the starting point for a deeper analysis on current threat landscape, which will be analysed in D4.2 (due M24) and D4.3 (M36), and will contribute to the CONCORDIA roadmap in Task T4.4. Future work in the three different areas of this deliverable are shortly discussed in the following.

6.1 Technical Views

From a technical standpoint, future work will build on activities discussing emerging threats and evolving attacks in Chapter 3 and Appendices A.1-A.6. First of all, the list of emerging threats and evolving attacks will be maintained to capture new discovered threats and attacks and manage crosscutting aspects of the threat landscape. Furthermore, future work (towards D4.2 due in M24) will concentrate on gaps and challenges with respect to identified threats and attacks. Finally, future work (towards D4.3 due in M24) will provide a set of guidelines, research actions, and an overview of existing countermeasures. To assess the completeness and soundness of the activities, we will build on the competences of partners in CONCORDIA, benefiting from their direct contributions and providing an incremental validation of the deliverable findings through questionnaires with relevant stakeholders inside and outside the project. Technical results will also contribute to the overall cybersecurity roadmap envisioned under T4.4.

6.2 Legal Views

From a legal standpoint, future work will entail identifying obligations relating to privacy and cybersecurity under applicable EU laws, including the NIS Directive and the GDPR. Pursuant to this and in line with the scope of the associated T4.2 on Legal aspects, a landscape will be created to capture the current organisational practices implemented by the partners regarding cybersecurity to the extent, of course, that these practices can be disclosed. The creation of such a landscape will be based on inputs received from consortium partners and they will be incorporated under D4.2. [128] Subsequently, a gap analysis will identify the discrepancies between regulatory expectations and the actual practices put in place by the consortium partners. Lastly, in the context of the work to be performed for D4.3, recommendations will be produced to bridge the gap between the state-of-play with the state-of-the-art

[128] Note that consortium partners may contribute to the creation of such a landscape by providing, for instance, high level information on the overall approach taken regarding the organizational aspects of cybersecurity.

in order to facilitate an organisational culture for cybersecurity in a principle based, and future-proof manner.

6.3. Economic Views

As the presented SEConomy is a new framework for estimating costs in complex distributed systems, refinement of the cost estimation models for specific applications becomes required. Thus, future work will run this refinement as well as the proposal of cyber-insurance models capable of covering the mitigation of threats not foreseen in design. Also, more tangible outcomes are expected in the form of SEConomy-based tools to support the cybersecurity economics and risks analysis. In addition, SEConomy will be applied in different use cases such as Finance, Telco, and e-Health sectors, with specific models and stakeholders from each sector for economic estimates. Besides that, models to estimate the real costs for the deployment and operation of cybersecurity solutions will be investigated. This includes the economic analysis of solutions based on different technologies, such as Network Functions Virtualization (NFV), Software-defined Networking (SDN), and cloud. Further investigations will be conducted directly with partners stakeholders to evaluate the impacts of cybersecurity approaches in the context of real-scenarios (e.g., telecom and financial sector). Such an evaluation can indicate future directions to validate SEConomy framework as well as support an overall model for economic perspectives verifications.

References

[1] P. Pagani, *Cyber Defense Magazine (CDM),* Cyber Defense Media Group, 2019.

[2] H. Österle e B. Otto, «Consortium Research: A Method for Researcher-Practitioner Collaboration in Design-Oriented IS Research,» *Business & Information Systems Engineering,* vol. 2, n. 5, pp. 283-293, October 2010.

[3] F. Xia, L. T. Yang, L. Wang e A. Vinel, «Internet of Things,» *International Journal of Communication Systems 25 (September 2012),* vol. 9, pp. 1101-1102, 2012.

[4] C. A. Ardagna, E. Damiani, J. Schutte e P. Stephanow, «A Case for IoT Security Assurance,» in *Internet of Things (ITTCC)*, Springer Link, 2017, pp. 175-192.

[5] C. A. Ardagna, R. Asal, E. Damiani e Q. Vu, «From Security to Assurance in the Cloud: A Survey,» in *ACM Computing Surveys (CSUR)*, August, 2015.

[6] M. Anisetti, C. A. Ardagna, F. Gaudenzi e E. Damiani, «A semi-automatic and trustworthy scheme for continuous cloud service certification,» *IEEE Transactions on Services Computing,* 2017.

[7] M. Anisetti, C. A. Ardagna, F. Gaudenzi, E. Damiani e G. Jeon, «Cost-effective deployment of certified cloud composite services,» *Journal of Parallel and Distributed Computing,* vol. 135, 2019.

[8] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi e J.-P. Seifert, «Practical Attacks Against Privacy and Availability in4G/LTE Mobile Communication Systems,» *ArXiv,* vol. abs/1510.07563, 7 August 2015.

[9] S. Hussain, O. Chowdhury, S. Mehnaz e E. Bertino, «LTEInspector: A Systematic Approach forAdversarial Testing of 4G LTE,» *Network and Distributed Systems Security (NDSS) Symposium 2018,* February 2018.

[10] M. Chlosta, D. Rupprecht, T. Holz, Pöpper e Christina, «LTE Security Disabled—Misconfiguration inCommercial Networks,» in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019.

[11] G. Pék, L. Buttyan e B. Bencsáth, «A Survey of Security Issues in Hardware Virtualization,» *ACM Computing Surveys (CSUR),* vol. 45, pp. 45, 3, Article 40, June 2013.

[12] B. Williams, «Virtualization System Security,» IBM X-Force Advanced Research, 2010.

[13] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica e M. Zaharia, «Above the Clouds: A Berkeley View of Cloud Computing,» *University of California at Berkeley UCB/EECS-2009-28, February,* vol. 28, February 2009.

[14] P. Mell e T. Grance, «The NIST definition of cloud computing,» 2011.

[15] S. Chandna, R. Singh e F. Akhtar, «Data Scavenging Threat in Cloud Computing,» *International Journal of Advances In Computer Science and Cloud Computing,* 2014.

[16] B. Albelooshi, K. Salah, T. Martin e E. Damiani, «Experimental Proof: Data Remanence in Cloud VMs,» *IEEE 8th International Conference on Cloud Computing (CLOUD) 2015,* 2015.

[17] N. Fernandes e O. C. M. B. Duarte, «XNetMon: A Network Monitor for Securing Virtual Networks,» *IEEE International Conference on Communications,* pp. 1-5, 2011.

[18] A. van Cleeff, W. Pieters e R. Wieringa, «Security Implications of Virtualization: A Literature Study,» in *International Conference on Computational Science and Engineering*, Washington DC, USA, 2009.

[19] Y. Demchenko, P. Membrey, P. Grosso e C. Laat, «Addressing Big Data Issues in Scientific Data Infrastructure,» in *Proc. of CTS 2013*, San Diego, CA, USA, May, 2013.

[20] C. A. Ardagna, P. Ceravolo e E. Damiani, «Big Data Analytics as-a-Service: Issues and challenges,» in *Proc. of the 3rd International Workshop on Privacy and Security of Big Data (PSBD 2016)*, Washington, VA, USA, December, 2016.

[21] D. Eckhoff e C. Sommer, «Driving for Big Data? Privacy Concerns in Vehicular Networking,» *Security & Privacy, IEEE,* vol. 12, n. 1, pp. 77-79, January 2014.

[22] R. Lu, H. Zhu, X. Liu, J. K. Liu e J. Shao, «Toward Efficient and Privacy-Preserving Computing in Big Data Era,» *Network, IEEE,* vol. 28, n. 4, pp. 46-50, July 2014.

[23] D. Wu, M. J. Greer, D. W. Rosen e D. Schaefer, «Cloud Manufacturing: Strategic Vision and State-of-the-Art,» *Journal of Manufacturing Systems,* vol. 32, n. 4, pp. 564-579, 2013.

[24] K. E. Martin, «Ethical issues in the big data industry,» *MIS Quarterly Executive,* vol. 14, p. 2, 2015.

[25] H. V. Jagadish, J. Gehrke, A. Labrinidis, Y. Papakonstantinou, J. M. Patel, R. Ramakrishnan e C. Shahabi, «Big Data and Its Technical Challenges,» *Communications of the ACM,* vol. 57, n. 7, pp. 86-94, 2014.

[26] H. R. Ekbia, M. Mattioli, I. Kouper, G. Arave, A. Ghazinejad, T. Bowman, V. R. Suri, A. Tsou, S. Weingart e C. R. Sugimoto, «Big Data, Bigger Dilemmas: A Critical Review,» *Journal of the Association for Information Science and Technology,* vol. 66, n. 8, pp. 1523-1545, 2015.

[27] M. Anisetti, C. Ardagna, E. Damiani e G. Polegri, «Test-Based Security Certification of Composite Services,» *ACM Transactions on the Web,* vol. 13, pp. 1-43, February 2019.

[28] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici e M. Ochoa, «Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures,» *ACM Computing Surveys,* vol. 52, pp. 1-40, March 2019.

[29] A. Kellett, «Trends and Future Directions in Data Security—2015 Vormetric Insider Threat Report,» Vormetric Data Security, 2015.

[30] P. H. Meland, M. Asim, D. Ayed, F. Dalpiaz, E. Félix, P. Giorgini, S. Gonzáles, B. Lempereur e J. Ronan, «Security and Trustworthiness Threats to Composite Services: Taxonomy, Countermeasures, and Research Directions,» in *Brucker A.D., Dalpiaz F., Giorgini P., Meland P.H., Rios E. (eds) Secure and Trustworthy Service Composition*, vol. 8900, Springer, Cham, 2014.

[31] M. Evans, L. Maglaras, Y. He e H. Janicke, «Human Behaviour as an aspect of Cyber Security Assurance,» *Security and Communication Networks 9(17),* 2016.

[32] T. Holz, N. Pohlmann, E. Bodden, M. Smith e J. Hoffmann, «Human-Centered. Systems Security,» Bochum, 2016.

[33] I. Corradini e E. Nardelli, «Building Organizational Risk Culture in Cyber Security: The Role of Human Factors,» in *Advances in Human Factors in Cybersecurity*, vol. 782, Springer, Cham, 2019.

[34] N. Sohrabi Safa, R. Von Solms e L. Futcher, «Human aspects of information security in organisations,» *Computer Fraud & Security,* pp. 15-18, 2016.

[35] A. Vieane, G. Funke, R. Gutzwiller, V. Mancuso, B. Sawyer e C. Wickens, «Addressing Human Factors Gaps in Cyber Defense,» in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2016.

[36] A. Rashid, G. Danezis, H. Chivers, E. Lupu, A. Martin, M. Lewis e C. Peersman, «Scoping the Cyber Security Body of Knowledge,» *IEEE Security & Privacy,* vol. 16, n. 3, pp. 96-102, 2018.

[37] H. Aldawood e G. Skinner, «Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering,» in *2019 Cybersecurity and Cyberforensics Conference (CCC)*, May 2019.

[38] M. Courtney, «States of cyber-warfare,» *Engineering & Technology,* vol. 12, n. 3, pp. 22-25, 2017.

[39] R. Hughes, «NATO and Cyber Defence,» in *Atlantisch Perspectief*, 2009, p. 33.

[40] C. S. Yoo, «Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures,» in *Cyberwar: Law and Ethics for Virtual Conflicts*, 2015, pp. 15-3.

[41] C. Everett, «The lucrative world of cyber-espionage,» *Computer Fraud & Security,* vol. 7, pp. 5-7, 2009.

[42] B. Watkins, «The impact of cyber attacks on the private sector,» Association for International Affair, 2014.

[43] M. Bressler e L. Bressler, «Protecting your company's intellectual property assets from cyber-espionage,» *Journal of Legal, Ethical, and Regulatory Issues,* vol. 18, n. 1, p. 21, 2015.

[44] A. Garg, J. Curtis e H. Halper, «Quantifying the financial impact of IT security breaches,» *Information Manaement & Computer Security,* vol. 11, n. 2, pp. 73-84, 2003.

[45] E. Gal-Or e A. Ghose, «The Economic Consequences of Sharing Security Information,» in *Economics of information security*, Boston, MA, 2004.

[46] S. Chai, M. Kim e H. Rao, «Firms' information security investment decisions: Stock market evidence of investors' behavior,» *Decision Support Systems,* vol. 50, n. 4, pp. 651-661, 2011.

[47] L. Gordon, M. Loeb e L. Zhou, «The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?,» *Journal of Computer Security,* vol. 19, n. 1, pp. 33-56, 2011.

[48] V. Richardson, M. W. Watson e R. E. Smith, «Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches,» *Journal of Information Systems,* 2019.

[49] Z. He, T. Frost e R. Pinsker, «The Impact of Reported Cybersecurity Breaches on Firm Innovation,» *Journal of Information Systems,* 2019.

[50] P. Rosati, M. Cummins, P. Deeney, F. Gogolin, L. Van der Werff e T. G. Lynn, «The effect of data breach announcements beyond the stock price: Empirical evidence on market activity,» *International Review of Financial Analysis,* vol. 49, pp. 146-154, 2017.

[51] C. Scherer e H. Cho, «A Social Network Contagion Theory of Risk Perception,» *Risk analysis : an official publication of the Society for Risk Analysis,* vol. 23, n. 2, pp. 261-267, 2003.

[52] V. Bakir, «Media and risk: Old and new research directions,» *Journal of Risk Research,* vol. 13, n. 1, pp. 5-18, 2010.

[53] I. Chung, «Social Amplification of Risk in the Internet Environment,» *Risk analysis : an official publication of the Society for Risk Analysis,* vol. 31, n. 12, pp. 1883-1896, 2011.

[54] W. Gharibi e M. Shaabi, «Cyber Threats In Social Networking Websites,» *International Journal of Distributed and Parallel Systems,* vol. 3, 2012.

[55] E. Toch, C. Bettini, E. Shmueli, L. Radaelli, A. Lanzi, D. Riboni e B. Lepri, «The Privacy Implications of Cyber Security Systems: A Technological Survey,» *ACM Computing Surveys,* vol. 51, n. 2, p. 36, 2018.

[56] H. Ye, X. Cheng, M. Yuan, L. Xu, J. Gao e C. Cheng, «A survey of security and privacy in big data,» in *2016 16th international symposium on communications and information technologies (iscit)*, 2016.

[57] P. Bhat e K. Dutta, «A Survey on Various Threats and Current State of Security in Android Platform,» *ACM Computing Surveys,* vol. 52, pp. 1-35, February 2019.

[58] M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe, P. Scharre, T. Zeitzoff, B. Filar, H. Anderson, H. Roff, G. Allen, J. Steinhardt, C. Flynn e S. HÉigeartaigh, «The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation,» *ArXiv,* february 2018.

[59] M. Shafahi, L. Kempers e H. Afsarmanesh, «Phishing through social bots on Twitter,» *2016 IEEE International Conference on Big Data (Big Data),* 2016.

[60] C. Shao, G. L. Ciampaglia, O. Varol, A. Flammini e F. Menczer, «The spread of fake news by social bots,» pp. 96-104, 2017.

[61] C. Shao, G. L. Ciampaglia, O. Varol, A. Flammini, F. Menczer e K.-C. Yang, «The spread of low-credibility content by social bots,» *Nature Communications,* vol. 9, n. 1, p. 4787, 2018.

[62] A. Bessi e E. Ferrara, «Social bots distort the 2016 U.S. Presidential election online discussion,» *First Monday,* vol. 21, n. 11-7, 2016.

[63] F. Brachten, M. Mirbabaie, S. Stieglitz, O. Berger, S. Bludau e K. Schrickel, «Threat or Opportunity? - Examining Social Bots in Social Media Crisis Communication».

[64] A. Nowak, P. Lukowicz e P. Horodecki, «Assessing Artificial Intelligence for Humanity: Will AI be the Our Biggest Ever Advance ? or the Biggest Threat [Opinion],» *IEEE Technology and Society Magazine,* vol. 37, n. 4, pp. 26-34, 2018.

[65] Y. Duan, J. Edwards e Y. Dwivedi, «Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda,» *International Journal of Information Management,* vol. 48, pp. 63-71, 2019.

[66] D. Helbing, B. Frey, E. Hafen, J. van den Hoven, G. Gigerenzer, R. Zicari, A. Zwitter e Y. Hofstetter, «Will Democracy Survive Big Data and Artificial Intelligence?,» *In Towards Digital Enlightenment,* pp. 73-98, 2019.

[67] E. Flaspöler, A. Hauke, P. Pappachan, D. Reinert, B. T., N. Henke e R. O. D. Beeck, «The human machine interface as an emerging risk,» EU-OSHA (European Agency for Safety and Health at Work), Luxembourg, 2009.

[68] C. Ciborra, «The Labyrinths of Information: Challenging the Wisdom of Systems,» OUP, Oxford, 2002.

[69] C. Kruse, B. Frederick, T. Jacobson e D. K. Monticone, «Cybersecurity in healthcare: A systematic review of modern threats and trends,» *Technology and Health Care,* vol. 25, n. 1, pp. 1-10, 2017.

[70] H. Kupwade Patil e R. Seshadri, «Big Data Security and Privacy Issues in Healthcare,» *2014 IEEE International Congress on Big Data,* pp. 762-765, 2014.

[71] J. Sametinger e J. W. Rozenblit, «Security Challenges for Medical Devices,» *Communications of the ACM,* vol. 58, n. 4, pp. 75-82, 2015.

[72] A. Humayed, J. Lin, F. Li e B. Luo, «Cyber-Physical Systems Security -- A Survey,» *IEEE Internet of Things Journal,* vol. 4, n. 6, pp. 1802-1831, 2017.

[73] E. Global, «Swiss Organization Better Prepared to Predict and Resist Cyber-attacks but Still a Long Way to go: EY Global Information Security Survey,» 2017. [Online]. Available: https://www.ey.com/ch/en/newsroom/news-releases/news-release-ey-swiss-organizations-better-prepared-to-predict-and-resist-cyber-attacks. [Consultato il giorno 12 June 2019].

[74] SecCord Project, «SECurity and trust COoRDination and enhanced collaboration,» [Online]. Available: https://cordis.europa.eu/project/rcn/105977/factsheet/es. [Consultato il giorno 27 November 2019].

[75] IPACSO Project, «Innovation Framework for ICT Security,» [Online]. Available: https://ipacso.eu/. [Consultato il giorno 27 November 2019].

[76] M. Brzoska, R. Bossong e E. van Um, «Security Economics in the European Context: Implications of the EUSECON Project,» *Economics of Security Working Paper Series,* vol. 58, 2011.

[77] VALUESEC Project, «Mastering the Value Function of Security Measures,» [Online]. Available: https://cordis.europa.eu/project/rcn/97989/factsheet/en. [Consultato il giorno 27 November 2019].

[78] CIRAS Project, «Critical Infrastructure Risk Assessment Support,» [Online]. Available: http://www.cirasproject.eu/. [Consultato il giorno 27 November 2019].

[79] ECOSSIAN Project, «European Control System Security Incident Analysis Network,» [Online]. Available: https://ecossian.eu. [Consultato il giorno 27 November 2019].

[80] PULSE Project, «Platform for European Medical Support During Major Emergencies,» [Online]. Available: http://www.pulse-fp7.com. [Consultato il giorno 27 Novembre 2019].

[81] SECONOMICS Project, «Socio-economics meets Security,» [Online]. Available: http://seconomicsproject.eu/. [Consultato il giorno 27 November 2019].

[82] B. Arief, M. B. Adzmi e T. Gross, «Understanding cybercrime from its Stakeholders Perspectives: Part 1–Attackers,» *IEEE Security & Privacy,* vol. 13, pp. 71-76, February 2015.

[83] S. Dzomira, «Electronic Fraud (Cyber Fraud) Risk in the Banking Industry,» *Risk Governance and Control: Financial Markets and Institutions,* vol. 4, pp. 16-26, 2014.

[84] U. M. e W. Fuadi, «A Method for Evaluating Information Security Governance (ISG) Components in Banking Environment,» *Journal of Physics: Conference Series,* vol. 812, pp. 12-31, 2017.

[85] S. Robert, T. Vijay e Z. Tim, «NIST Best Practices in Cyber Supply Chain Risk Management,» US Resilience Project, 2016.

[86] S. Dynes, E. Goetz e M. Freeman, «Cyber Security: Are Economic Incentives Adequate?,» in *Critical Infrastructure Protection*, Springer, 2007, pp. 15-27.

[87] M. Camillo, «Cyber Security: Risks and Management of Risks for Global Banks and Financial Institutions,» *Journal of Risk Management in Financial Institutions,* vol. 10, pp. 196-200, 2017.

[88] A. R. Raghavan e L. Parthiban, «The Effect of Cybercrime on a Bank's Finances,» *International Journal of Current Research & Academic Review,* vol. 2, pp. 173-178, January 2014.

[89] X. Vives, «Regulatory Reform in European Banking,» *European Economic Review,* vol. 35, pp. 505-515, 1991.

[90] K. Richards, R. LaSalle, M. Devost, F. van den Dool e J. Kennedy-White, «2017 Cost of Cyber Crime Study,» Ponemon Institute LLC, 2017.

[91] M. Brencht e T. Nowey, «A Closer Look at Information Security Costs,» in *The economics of Information Security and Privacy*, Springer, 2013, pp. 2-24.

[92] S. Morgan, «2019 Official Annual Cybercrime Report,» Herjavec Group, 2019.

[93] S. Moore, «Gartner Forecasts Worldwide Information Security Spending to Exceed 124 million in 2019,» Gartner, 2018.

[94] J. Bauer e M. Van Eeten, «Introduction to the Economics of Cyber security,» *Communications and Strategies,* vol. 81, pp. 13-22, 2011.

[95] T. Moore, «The Economics of Cyber Security: Principles and Policy Options,» *International Journal of Critical Infrastructure Protection (IJCNIP),* vol. 3, pp. 103-117, 2010.

[96] WhiteHouse, «The Cost of Malicious Cyber Activity to the U.S. Economy,» 2018. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. [Consultato il giorno 3 June 2019].

[97] AFCEA, «The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment,» AFCEA International Cyber Committee, 2013.

[98] A. J. Kornecki e K. Hall, «Approaches to Assure Safety in Fly-By-Wire Systems: Airbus vs. Boeing,» in *IASTED Conference on Software Engineering and Applications*, Cambridge, 2004.

[99] C. McGuffin e P. Mitchell, «On Domains: Cyber and the Practice of Warfare,» *International Journal,* vol. 69, n. 3, pp. 394-412, 2014.

[100] Joint Task Force Transformation Initiative, «Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life

Cycle Approach,» National Institute of Standards and Technology (NIST), 2014.

[101] E. Rich, J. Gonzalez, Y. Qian, F. Sveen, J. Radianti e S. Hillen, «Emergent Vulnerabilities in Integrated Operations: A Proactive Simulation Study of Economic Risk,» *International Journal of Critical Infrastructure Protection,* vol. 2, pp. 110-123, 2009.

[102] T. C. Horng, «A Comparative Analysis of Supply Chain Management Practices by Boeing and Airbus: Long-term Strategic Implications,» Massachusetts Institute of Technology, Massachusetts, 2006.

[103] P. Y. Chen, G. Kataria e R. Krishnan, «Correlated Failures, Diversification, and Information Security Risk Management,» *MIS quarterly,* pp. 397-422, 2011.

[104] W. Sonnenreich, J. Albanese e B. Stout, «Return On Security Investment (ROSI) - A Practical Quantitative Model,» *Journal of Research and practice in Information Technology,* vol. 38, p. 45–52, 2006.

[105] BBC, «Boeing Admits it `Fell Short` on Safety Alert for 737,» BBC News, 2019.

[106] C. P. Gibson e S. M. Banik, «Analyzing the Effect of Ransomware Attacks on Different Industries,» in *nternational Conference on Computational Science and Computational Intelligence (CSCI 2017)*, Las Vegas, USA, 2017.

[107] Varonis Systems, «2018 Varonis Data Risk Report,» Varonis Inc, 2018.

[108] S. Choi e M. E. Johnson, Do Hospital Data Breaches Reduce Patient Care Quality?, 2019.

[109] J. Jiang e G. Bai, «Evaluation of Causes of Protected Health Information Breaches,» *JAMA Internal Medicine,* vol. 179, 2019.

[110] I. Butun, P. Österberg e H. Song, «Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures,» *IEEE Communications Surveys & Tutorials,* vol. PP, pp. 1-1, 2019.

[111] M. Park, H. Oh e K. Lee, «Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective,» *Sensors,* vol. 19, p. 2148, 2019.

[112] A. Maiti, M. Jadliwala, J. He e I. Bilogrevic, «Side-Channel Inference Attacks on Mobile Keypads using Smartwatches,» *IEEE Transactions on Mobile Computing,* vol. PP, 2018.

[113] A. Sarkisyan, R. Debbiny e A. Nahapetian, «WristSnoop: Smartphone PINs prediction using smartwatch motion sensors,» in *Proceedings of the 2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, Rome, 2015.

[114] S. Chakraborty, W. Ouyang e M. Srivastava, «LightSpy: Optical eavesdropping on displays using light sensors on mobile devices,» in *Proceedings of the 2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, USA, 11-14 December 2017.

[115] R. Bassil, A. Chehab, I. Elhajj e A. Kayssi, «Signaling oriented denial of service on LTE networks,» in *Proceedings of the 10th ACM international symposium on Mobility management and wireless access*, 2012.

[116] Y. Xia, Y. Liu, H. Chen e B. Zang, «Defending against vm rollback attack,» in *Proceeedings of the 42nd IEEE International Conference on Dependable Systems and Networks Workshops*, 2012.

[117] F. Rocha, T. Gross e A. van Moorsel, «Defense-in-depth against malicious insiders in the cloud,» in *Proceeedings of the IEEE International Conference on Cloud Engineering (IC2E'13)*, 2013.

[118] Y. Zhang, A. Juels, A. Oprea e M. K. Reiter, «Homealone: Co-residency detection in the cloud via side-channel analysis,» in *Proceeedings of the IEEE Symposium on Security and Privacy (SP'11)*, 2011.

[119] Y. Zhang, A. Juels, M. K. Reiter e T. Ristenpart, «Cross-VM side channels and their use to extract private keys,» in *Proceeedings of the ACM Conference on Computer and Communications Security*, 2012.

[120] M. Weiß, B. Heinz e F. Stumpf, «A cache timing attack on AES in virtualization environments,» in *Proceedings of the International Conference on Financial Cryptography and Data Security*, 2012.

[121] G. Irazoqui, M. S. Inci, T. Eisenbarth e B. Sunar, «Fine grain cross-VM attacks on xen and VMware,» in *Proceeedings of the International Conference on Big Data and Cloud Computing*, 2014.

[122] Y. Yarom e K. Falkner, «FLUSH+ RELOAD: A high resolution, low noise, L3 cache side-channel attack,» in *Proceeedings of the USENIX Security Symposium*, 2014.

[123] G. Irazoqui, M. S. Inci, T. Eisenbarth e B. Sunar, «Seriously, get off my cloud! cross-VM RSA key recovery in a public cloud,» IACR Cryptology ePrint Archive, 2015.

[124] C. Maurice, C. Neumann, O. Heen e A. Francillon, «C5: Cross-cores cache covert channel,» in *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2015.

[125] J. Xiao, Z. Xu, H. Huang e H. Wang, «A covert channel construction in a virtualized environment,» in *Proceeedings of the ACM Conference on Computer and Communications Security*, 2012.

[126] P. Pessl, D. Gruss, C. Maurice, M. Schwarz e S. Mangard, «DRAMA: Exploiting DRAM addressing for cross-CPU attacks,» in *Proceeedings of the USENIX Security Symposium*, 2016.

[127] B. Albelooshi, K. Salah, T. Martin e E. Damiani, «Experimental Proof: Data remanence in cloud VMs,» in *Proceedings of the International Conference on Cloud Computing*, 2015.

[128] S. Shafieian, M. Zulkernine e A. Haque, «Attacks in Public Clouds: Can They Hinder the Rise of the Cloud?,» in *Cloud Computing*, 2014, pp. 3-22.

[129] L. Shi, Y. Wu, Y. Xia, N. Dautenhahn, H. Chen, B. Zang e J. Li, «Deconstructing Xen,» in *Proc of NDSS*, 2017.

[130] J.-R. Yeh, H.-C. Hsiao e A.-C. Pang, «Migrant Attack: A Multi-resource DoS Attack on Cloud Virtual Machine Migration Schemes,» in *11th Asia Joint Conference on Information Security (AsiaJCIS)*, 2016.

[131] S. T. King e P. M. Chen, «SubVirt: Implementing malware with virtual machines,» in *In Proceeedings of the IEEE Symposium on Security and Privacy*, 2006.

[132] A. Desnos, E. Filiol e I. Lefou, «Detecting (and creating!) a HVM rootkit (aka BluePill-like),» *Journal in Computer Virology,* pp. 23-49, 2011.

[133] A. Jasti, P. Shah, R. Nagaraj e R. Pendse, «Security in multi-tenancy cloud,» in *Proceeedings of the IEEE International Carnahan Conference on Security Technology*, 2010.

[134] S. Checkoway e H. Shacham, «Iago attacks: Why the system call API is a bad untrusted RPC interface,» *International Conference on Architectural Support for Programming Languages and Operating Systems - ASPLOS,* pp. 253-264, 2013.

[135] M. Kandias, N. Virvilis e D. Gritzalis, «The insider threat in cloud computing,» in *Proceeedings of the International Workshop on Critical Information Infrastructures Security*, 2011.

[136] F. Rocha e M. Correia, «Lucy in the sky without diamonds: Stealing confidential data in the cloud,» in *Proceeedings of the IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W'11)*, 2011.

[137] C. Li, A. Raghunathan e N. K. Jha, «Secure virtual machine execution under an untrusted management OS,» in *Proceeedings of the 3rd IEEE International Conference on Cloud Computing*, 2010.

[138] E. Damiani, «Toward Big Data Leak Analysis,» *Proceedings of the Privacy and Security of Big Data Workshop (PSBD 2015), IEEE Big Data Conference,* 1-3 November 2015.

[139] S. Aditham e N. Ranganathan, «A novel framework for mitigating insider attacks in big data systems,» *2015 IEEE International Conference on Big Data,* 2015.

[140] G. Li, P. Zhu, J. Li, Z. Yang, N. Cao e Z. Chen, «Security Matters: A Survey on Adversarial Machine Learning».

[141] Z. Mengchen, B. An, Y. Yu, S. Liu e S. J. Pan, «Data Poisoning Attacks onMulti-Task Relationship Learning,» in *Proc. of the The Thirty-Second AAAI Conferenceon Artificial Intelligence (AAAI-18)*, 2018.

[142] S. Yi, T. Erpek, Y. E. Sagduyu e J. H. Li, «Spectrum Data Poisoning with Adversarial Deep Learning,» *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM),* 2018.

[143] B. Li, Y. Wang, A. Singh e Y. Vorobeychik, «Data poisoning attacks on factorization-based collaborative filtering,» in *Proceedings of the 30th International Conference on Neural Information Processing Systems (NIPS'16)*, 2016.

[144] D. Zügner, A. Akbarnejad e S. Günnemann, «Adversarial Attacks on Neural Networks for Graph Data,» in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD '18), 2018*, 2018.

[145] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka e G. Lo Iacono, «All your clouds are belong to us: security analysis of cloud management interfaces,» in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop (CCSW '11)*, 2011.

[146] J. Huang, D. M. Nicol e R. H. Campbell, «Denial-of-Service Threat to Hadoop/YARN Clusters with Multi-Tenancy,» *IEEE International Congress on Big Data,* 2014.

[147] E. R. Osawaru e R. A. Ariyaluran Habeeb, «A Highlight of Security Challenges in Big Data,» *International Journal of Information Systems and Engineering (online),* vol. 2, n. 1, April 2014.

[148] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom e M. Hamburg, « Meltdown: reading kernel memory from user space,» in *Proceedings of the 27th USENIX Conference on Security Symposium (SEC'18)*, 2018.

[149] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz e Y. Yarom, «Spectre Attacks: Exploiting Speculative Execution,» in *Proc. of the 40th IEEE Symposium on Security and Privacy (S\&P'19)}*, 2019.

[150] S. De Capitani di Vimercati, S. Foresti, G. Livraga e P. Samarati, «Data privacy: Definitions and techniques,» *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 20, n. 6, pp. 793-817, 2012.

[151] P. Orduña, A. Almeida, U. Aguilera, X. Laiseca, D. López-de-Ipiña e A. Gómez-Goiri, «Identifying'Identifying Security Issues in the Semantic Web: Injection attacks in the Semantic Query Languages,» *VI Jornadas Científico-Técnicas en Servicios Web y SOA (JSWEB 2010p.),* pp. 43-50, September 2010.

[152] N. Ben Mustapha, H. Zghal, M.-A. Aufaure e H. Ben Ghezala, «Enhancing semantic search using case-based modular ontology,» in *Proceeding of the 2010 ACM Symposium on Applied Computing*, 2010.

[153] M. Collins, M. Theis, R. Trzeciak, J. Strozer, J. Clark, D. Costa, T. Cassidy, M. Albrethsen e A. Moore, «Common Sense Guide to Prevention and Detection of Insider Threats (5th ed.),» Pittsburgh, PA, 2016.

[154] M. Reddy, M. Keeney, E. Kowalski, D. M. Cappelli e A. P. Moore, «Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,» Pittsburgh, PA, 2005.

[155] E. Kowalski, T. Conway, S. Keverline, M. Williams, D. M. Cappelli, B. Willke e A. P. Moore, «Insider threat study: Illicit cyber activity in the government sector,» 2008.

[156] L. F. Fischer, «Characterizing information systems insider offenders,» in *Proceedings of the Conference of the International Military Testing Association*, 2003.

[157] E. Shaw, K. Ruby e J. Post, «The Insider threat to information systems: The psychology of the dangerous insider,» *Security Awareness Bulletin,* vol. 2, pp. 1-10, 1998.

[158] M. Keeney, E. Kowalski, A. P. Moore, T. Shimeall e S. Rogers, «Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors,» Washington DC, 2005.

[159] G. Magklaras e S. Furnell, «Insider Threat Prediction Tool: Evaluating the probability of IT misuse,» *Computers & Security,* vol. 21, pp. 62-73, 2002.

[160] G. Jabbour e D. A. Menascé, «Stopping the insider threat: The case for implementing autonomic defense mechanisms in computing systems,» in *Proceedings of the International Conference of Information Security and Privacy*, 2009.

[161] M. Bishop, S. Engle, S. Peisert, S. Whalen e C. Gates, «Case studies of an insider framework,» in *Hawaii International Conference on System Sciences*, Los Alamitos, CA, 2009.

[162] C. W. Probst e J. Hunker, «The Risk of Risk Analysis And its Relation to the Economics of Insider Threats,» Springer, 2010, pp. 279-299.

[163] J. Predd, S. L. Pfleeger, J. Hunker e C. Bulford, «Insiders Behaving Badly,» *Security & Privacy, IEEE,* vol. 6, n. 4, pp. 66-70, 2008.

[164] M. Anisetti, C. A. Ardagna, R. Asal, L. Comi, E. Damiani e F. Gaudenzi, «A Knowledge-Based IoT Security Checker,» in *Proc. of the 2nd Workshop on Fog-to-Cloud Distributed Processing (F2c-DP)*, Turin, Italy, August, 2018.

[165] N. Zhang, K. Yuan, M. Naveed, X. Zhou e X. Wang, «Leave Me Alone: App-Level Protection against Runtime Information Gathering on Android,» in *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, 2015.

[166] U. Fiore, F. Palmieri, A. Castiglione, V. Loia e A. De Santis, «Multimedia-based battery drain attacks for Android devices,» in *Proceedings of the 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC'14)*, 2014.

[167] S. oeplau, Y. Fratantonio, A. Bianchi, A. Bianchi, C. Kruegel e G. Vigna, «Execute This! Analyzing Unsafe and Malicious Dynamic Code Loading in Android Applications,» in *Proceedings of the Network and Distributed System Security Symposium*, 2014.

[168] N. Hardy, «The Confused Deputy (or why capabilities might have been invented),» *ACM SIGOPS Operating Systems Review 22,* vol. 4, pp. 36-38, October 1988.

[169] R. Schlegel, K. Zhang, X.-y. Zhou, M. Intwala, A. Kapadia e X. Wang, «Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones,» in *Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS)*, 2011.

[170] S. Johnson, K. Bowers, L. Gamman, L. Tisdall e A. Warne, «Theft of Customers' Personal Property in Cafés and Bars,» in *Problem-Oriented Guides for Police*, 2010, p. 60.

[171] S. G. Wakeling, P. Hannay e Z. Baig, «A review of data breaches and losses that occurred from laptops that were stolen or otherwise misplaced in 2015 and 2016,» in *The Proceedings of 15th Australian Information Security Management Conference*, Perth, Western Australia, 5-6 December, 2017.

[172] R. Mahajan, D. Wetherall e T. Anderson, «Understanding BGP misconfiguration,» *ACM SIGCOMM Computer Communication Review,* vol. 32, n. 4, pp. 3-16, 2002.

[173] O. Nordström e C. Dovrolis, «Beware of BGP attacks,» *Computer Communication Review,* vol. 34, pp. 1-8, 2004.

[174] V. Pappas, D. Wessels, D. Massey, S. Lu, A. Terzis e L. Zhang, «Impact of Configuration Errors on DNS Robustness,» *ACM SIGCOMM Computer Communication Review,* vol. 34, n. 4, 2004.

[175] F. Cuppens, N. Cuppens-Boulahia e J. Garcia-Alfaro, «Detection and removal of firewall misconfiguration,» in *Proceedings of the 2005 IASTED International Conference on Communication, Network and Information Security*, 2005.

[176] B. Eshete, A. Villafiorita e K. Weldemariam, «Early Detection of Security Misconfiguration Vulnerabilities in Web Applications,» *2011 Sixth International Conference on Availability, Reliability and Security,* 2011.

[177] A. Continella, M. Polino, M. Pogliani e S. Zanero, «There's a Hole in that Bucket!: A Large-scale Analysis of Misconfigured S3 Buckets,» in *Proceedings of the 34th Annual Computer Security Applications Conference*, 2018.

[178] E. Schultz, «A framework for understanding and predicting insider attacks,» *Computers & Security,* vol. 21, n. 6, pp. 526-531, 2002.

[179] P. Turner, W. Polk e E. Barker, «Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance,» National Institute of Standards and Technology, 2012.

[180] B. Danev, H. Luecken, S. Capkun e K. Eldefrawy, «Attacks on physical-layer identification,» in *Proceedings of the third ACM conference on Wireless network security*, 2010.

[181] V. Khanna, E. Kim e Y. Lu, «CEO Connectedness and Corporate Fraud,» *The Journal of Finance,* vol. 70, n. 3, pp. 1203-1252, 2015.

[182] A. Etzioni, «Geo. J. The Private Sector: A Reluctant Partner in Cybersecurity,» in *Int'l Aff. 15*, 2014, p. 69.

[183] P. Tobin, M. Mckeever, J. Blackledge, M. Whittington e B. Duncan, «UK Financial Institutions Stand to Lose Billions in GDPR Fines: How can They Mitigate This?,» in *Br. Account. Financ. Assoc. Scottish Area Gr. Annu. Conf.*, BAFA, Ed. a cura di, Aberdeen, 2017.

[184] P. Voigt e A. Bussche, «Enforcement and Fines Under the GDPR,» in *The EU General Data Protection Regulation (GDPR)*, Springer, Cham, 2017, pp. 201-217.

[185] M. Lesk, «Cybersecurity and Economics,» *IEEE Security & Privacy,* vol. 9, n. 6, pp. 76-79, 2011.

[186] J. J. Cordes, «An overview of the economics of cybersecurity and cybersecurity policy,» 2011.

[187] B. Kaplan, «Selling Health Data,» *Cambridge quarterly of healthcare ethics : CQ : the international journal of healthcare ethics committees,* vol. 24, n. 03, pp. 256-71, 2015.

[188] M. Huesch, M. Ong e B. D. Richman, «Could Data Broker Information Threaten Physician Prescribing and Professional Behavior?,» *SSRN Electronic Journal,* 2015.

[189] H. Berghel, «Equifax and the Latest Round of Identity Theft Roulette,» *Computer,* vol. 50, n. 12, pp. 72-76, 2017.

[190] R. Langner, «Stuxnet: Dissecting a Cyberwarfare Weapon,» *IEEE Security & Privacy,* vol. 9, n. 3, pp. 49-51, 2011.

[191] C. Bronk e E. Tikk-Ringas, «The Cyber Attack on Saudi Aramco,» *Survival,* vol. 55, n. 2, pp. 81-96, 2013.

[192] V. Joubert, «Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?,» NATO Defense College, 2012.

[193] J. F. Brenner, «Eyes wide shut: The growing threat of cyber attacks on industrial control systems,» *Bulletin of the Atomic Scientists,* vol. 69, n. 5, pp. 15-20, 2013.

[194] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. J. Shimeall e L. Flynn, «Common sense guide to mitigating insider threats,» 2012.

[195] P. Wang, R. Angarita e I. Renna, «Is this the era of misinformation yet: combining social bots and fake news to deceive the masses,» in *Companion Proceedings of the The Web Conference 2018*, 2018.

[196] C. Shao, G. Ciampaglia, O. Varol, K. Yang, A. Flammini e F. Menczer, «The spread of low-credibility content by social bots,» *Nature communications,* vol. 9, n. 1, pp. 1-9, 2018.

[197] E. Ferrara, O. Varol, C. Davis, F. Menczer e A. Flammini, «The rise of social bots,» *Communications of the ACM,* vol. 59, n. 7, pp. 96-104, 2016.

[198] Y. Boshmaf, I. Muslukhov e K. Beznosov, «The socialbot network: when bots socialize for fame and money,» in *Proc. of the 27th annual computer security applications conference* , 2011.

[199] C. Shao, P. Hui, L. Wang, X. Jiang, A. Flammini, F. Menczer e G. Ciampaglia, «Anatomy of an online misinformation network,» *PloS one,* vol. 13, n. 4, 2018.

[200] C. Davis, O. Varol, E. Ferrara, A. Flammini e F. Menczer, «Botornot: A system to evaluate social bots,» in *Proc. of the 25th international conference companion on world wide web*, 2016.

[201] C. Cai, L. Li e D. Zengi, «Behavior enhanced deep bot detection in social media,» in *Proc. of the IEEE International Conference on Intelligence and Security Informatics (ISI 2017)*, 2017.

[202] S. Kudugunta e E. Ferrara, «Deep neural networks for bot detection,» *Information Sciences,* 2018.

[203] S. Cresci, M. Petrocchi, A. Spognardi e S. Tognazzi, «Better safe than sorry: an adversarial approach to improve social bot detection,» in *Proc. of the 10th ACM Conference on Web Science 2019*, 2019.

[204] Ö. Sandıkcı e A. Ekici, «Politically motivated brand rejection,» *Journal of Business Research,* vol. 62, n. 2, pp. 208-217, 2009.

[205] J. J. Angel e D. M. McCabe, «The Business Ethics of Short Selling and Naked Short Selling,» *Journal of Business Ethics,* vol. 85, n. 1, pp. 239-249, 2009.

[206] D. W. Mccormick e J. C. Spee, «IBM and Germany 1922–1941,» *Organization Management Journal,* vol. 5, n. 4, pp. 214-223, 2008.

[207] S. M. Rao e J. B. Hamilton III, «The effect of published reports of unethical conduct on stock prices,» *Journal of Business Ethics,* vol. 15, n. 12, pp. 1321-1330, 1996.

[208] F. M. Chee, «An Uber ethical dilemma: examining the social issues at stake,» *Journal of Information, Communication and Ethics in Society,* vol. 16, n. 3, pp. 261-274, 2018.

[209] M. Ahsan, «Entrepreneurship and Ethics in the Sharing Economy: A Critical Perspective,» *Journal of Business Ethics,* pp. 1-15, 2018.

[210] B. Srinidhi, J. Yan e G. K. Tayi, «Allocation of Resources to Cyber-Security: The Effect of Misalignment of Interest between Managers and Investors,» *Decision Support Systems,* vol. 75, pp. 49-62, 2015.

[211] H. Meng, V. Thing, Y. Cheng, Z. Dai e L. Zhang, «A survey of Android exploits in the wild,» *Computers & Security,* vol. 76, pp. 71-91, 2018.

APPENDIX A: Main Attacks

The scope of this appendix is to present major attacks that affected each of our domains of interest. The attacks are grouped based on the main exploited threats.

A.1 Attacks related to Device/IoT-Centric Security

In the following, the main attacks affecting Device/IoT domain are reported. We note that the threat description is available in Section 3.3.3.

- **Threat T1.1.1: Information leakage/sharing due to human errors:** In medical sector IoT applications are very critical as also pointed out by Choi et al. [108] that showed how data breach in hospital can impact on the 30-day mortality rate. According to Jiang et al. [109] most breaches in hospitals were triggered by employee mistakes or unauthorised disclosures. Given the nature of the information, the impact on privacy is of paramount importance. In some cases, sensor channels are protected, but the aggregation nodes at the edge were not. Employee mistakes can reveal them or generate a weakness that can potentially reveal them [109]. Installation phase is also critical in IoT since in most of the cases it the only moment where human intervention can activate security features or configure secure connections with the rest of the network. It can be complex to remediate to a human error at this phase.
- **Threat T1.1.2: Inadequate design and planning or incorrect adaptation:** Many attacks partially involve this threat to trigger another one, like in the case of botnets. Examples of security attacks generated by an inadequate design are the ones that involves CloudPets' toys, that are designed without considering any Bluetooth security features, so that everyone within range can connect to them, and send and receive commands and data.[129] Given the nature of these devices, adaptation and fixing strategy are almost not applicable. One example of wrong design of IoT device deployment is the one related to the device of refrigeration/heating-ventilation and air-conditioning of HVAC vendor that has remote access to monitor the environmental temperature. These devices were used in 2015 to generate data breach on a retail's network. More than the vulnerabilities of the devices, the problem was the decision of having such devices on the same network with POS services.[130] Similar issues are quite common in medical facilities that uses IoT devices for their specific capabilities without having network segmentation of them from other devices. The result is that any local device can end up having a global impact.[131]
- **Threat T1.2.1: Interception of information:** Recently Amazon Smart Ring IoT devices was discovered by BitDefender to be vulnerable to password interception since they handle the exchange of the WiFi password in plain text

[129] How This Internet of Things Stuffed Animal Can Be Remotely Turned Into a Spy Device https://www.vice.com/en_us/article/qkm48b/how-this-internet-of-things-teddy-bear-can-be-remotely-turned-into-a-spy-device

[130] IoT Hack Connected To Target Breach https://www.mocana.com/blog/2014/02/05/iot-hack-connected-target-breach

[131] Health care's huge cybersecurity problem https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation

format over an http channel.[132] A security vulnerability in BMW's Connected Drive system allowed researchers to unlock the vehicles affected without the car keys. The researchers were able to impersonate BMW servers and send, over the public cellular network, remote unlocking instructions to vehicles. The problem was fixed adding HTTPS encryption to the connection and ensures that the car only accepts connections from a server with the correct security certificate. More recently VPNFilter similarly to BlackEnergy malware intercepted communication from SCADA systems used in manufacturing and the maintenance of infrastructure to sniff out credentials attacking routers.[133]

- **Threat T1.2.2: Unauthorised acquisition of information:** Some traditional networking attacks can have a role in IoT given the vulnerabilities of networking devices currently used in IoT environment. For instance, the sinkhole attack (or blackhole attack) is obtained via an attacker that declares himself to have a high-quality route/path allowing him to do manipulate all packets passing through it. Another type of attack to the network is the selective forwarding attack where the attacker can selectively forward/drop packets. The wormhole attack is obtained recording packets at one location in the network and tunnelling them to another location having the scope of influencing perceived network behavior distort statistics and impacting the routing functionalities.
- **Threat T1.3.1: Device modification:** An attacker may be able to exploit firmware upgrade (requiring or not physical access) by maliciously replacing the device's firmware influencing its operational behavior. For example, an attacker can obtain a periodical report the energy consumption of a specific device could adding a piece of malicious code to the firmware. This information can be then used to infer if a home or an enterprise is active or not. In other cases, the fact that the firmware upgrade can be complex in IoT environment lead to the situation in which firmware has not been properly maintained and updated. This scenario opens to vulnerabilities that might be exploited by attackers to replace the firmware on the device remotely. For instance, the Foscam wireless cameras were vulnerable to firmware replacement allowing full camera control.[134] IoT is also exposed more than other systems to physical cloning attack. Butun et al. [110] described a number of scenarios where clone attack impacts IoT and the relative detection countermeasure.
- **Threat T1.3.2: Extraction of private information:** Park et al. focused on the attack on information on IoT Sensors including the ones requiring physical access [111]. In many cases physical access permits to bypass security protections and access to the device having the scope of tampering it to extract private information or to modify firmware to have a privileged shadow access. Additional examples are the side channel attacks on sensors data. Maiti et al. describe side channel attack on mobile keypads using smartwatches [112]. Sarkisyan et al. study PIN prediction using smartwatch motion sensor [113].

[132] Ring Video Doorbell Pro Under the Scope https://labs.bitdefender.com/2019/11/ring-video-doorbell-pro-under-the-scope/
[133] VPNFilter: New Router Malware with Destructive Capabilities https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware
[134] How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old https://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/

Chakraborty et al. describe optical eavesdropping on the display of a mobile device via light sensors [114].

- **Threat T1.4.1: Identity fraud:** In 2015 Moose infected a device using brute force attacks through Telnet and set up a SOCKS and HTTP proxy. In 2018, Guardzilla, an IoT camera, used the same hard-coded keys on devices as it did for its AWS storage server. This is an example of IoT threat that allows impersonification via access key of the cloud backend service.[135]
- **Threat T1.4.2: Denial of service:** In Finland, a DDoS attack took down the heating systems of at least two housing blocks in the city of Lappeenranta, leaving their residents without heating in sub-zero temperatures for more than a week.[136] Apparently the source of this attack was a Mirai botnet.
- **Threat T1.4.3: Malicious code/software/activity:** The Puerto Rican Electric Power Authority (PREPA) in 2009 suffered a series of power theft incidents related to its smart meter deployment. The attack was quite complex and exploited different threats. For instance, it requires physical access (TG1.3), and it probably implies malicious insiders that understand the hardware functionalities. The main exploited vulnerability was discovered later in 2010 and was injection of false data mainly at installation phase.[137] This is considered a serious security issue for IoT devices especially in correlation with malicious insider. IoT is also the preferred target for Botnet based malware. Recently a new variant of Gafgyt malware targets small office and home routers exploiting well known vulnerabilities. It is in competition with JenX botnet and in case of double infection they are programmed to disable each other.[138] Jeep Cherokees was discovered to be vulnerable to an attacker that may be miles away yet capable of sending commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission.[139] IoT_Reaper, also known as "the Reaper," is variant of Mirai Linux that utilizes at least ten old and well-known vulnerabilities in IoT. Given the difficulties in updating IoT even old vulnerabilities can be very effective. Recently cryptominers start considering IoT devices, more for the fact that they are quite easy to tamper than for their computational power even if devices such as Alexa and mobile phones (android OS via ADB.Miner) have non-negligible computational capabilities. More recently, these types of malware used blockchain-based DNS to make them more difficult to track, like Fbot.
- **Threat T1.4.4: Misuse of assurance tools:** Given the IoT peculiarities such assurance tool is in most of the cases not implemented but there is a non-negligible effort in order to have them in place in the near future. Therefore, more attacks will become available in the future.

[135] Security flaws let anyone snoop on Guardzilla smart camera video recordings
https://techcrunch.com/2018/12/27/guardzilla-security-camera-flaws/
[136] DDoS Attack Takes Down Central Heating System Amidst Winter In Finland
https://thehackernews.com/2016/11/heating-system-hacked.html
[137] Puerto Rico smart meters believed to have been hacked – and such hacks likely to spread
https://www.smart-energy.com/regional-news/north-america/puerto-rico-smart-meters-believed-to-have-been-hacked-and-such-hacks-likely-to-spread/
[138] This aggressive IoT malware is forcing Wi-Fi routers to join its botnet army
https://www.zdnet.com/article/this-aggressive-iot-malware-is-forcing-wi-fi-routers-to-join-its-botnet-army/
[139] Hackers Remotely Kill a Jeep on the Highway—With Me in It
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

- **Threat T1.4.5: Failures of business process:** Examples of business process failures are the ones that imply poorly-designed technical workflows like for instance save sensor data in multiple copies and in a not protected location or keep them locally even after having transferred them. Other failures refer to business-specific processes where IoT devices are manufactured with non-reliable or non-security components and the manufacturing process has no requirements on assurance which is a supply chain vulnerability. According to TrapX most of the healthcare organizations are vulnerable to medical device hijacking also called "medjacking", which in many cases imply failures on the business process connected with sensors or on the procurement process.[140]
- **Threat T1.4.6: Code execution and injection (unsecure APIs):** SQL injections are bigger danger to the IoT than traditional networks. They are in many cases at the basis of most of the Botnet since SQL injection can lead to privilege escalation quite straightforward. In many cases the target is a smartphone that controls devices like in the cases of the XSS and SQL injection of Belkin devices and WeMo app.[141] Recently Carlo Gavazzi SmartHouse version 6.5.33 was discovered to suffer from cross site request forgery along with both reflective and persistent XSS vulnerabilities.[142]
- **Threat T1.5.1: Violation of laws or regulations:** See Chapter 4.
- **Threat T1.6.1: Skill shortage:** No recent attacks have been reported.

A.2 Attacks related to Network-Centric Security

In the following, the main attacks affecting Network domain are reported. We note that the threat description is available in Section 3.3.4.

- **Threat T2.1.1: Erroneous use or administration of devices and systems:** A human error caused a mobile internet outage for millions of users. Due to a human error (wrong software configuration) during the migration of the packet gateway, clients of one operator were not able to use mobile data. Mobile switches were affected by this incident. A rollback was successfully executed to resolve the issue.[143] Misconfigured, Open DNS Servers has been used in Record-Breaking DDoS Attack. The attackers abused improperly configured or default-state DNS servers, also known as open DNS resolvers.[144]
- **Threat T2.2.1: Signaling traffic interception:** An attacker by simply having a signaling network access (e.g. by simply renting a global title on the market) can sent crafted messages to retrieve location information of the network node on which a target subscriber is connected. An attacker can alter current subscriber's location and profile to receive mobile terminating or mobile originating calls, SMS, or data traffic. Hostile SS7 Update Location enables

[140] Medjacking: The newest healthcare risk? https://www.healthcareitnews.com/news/medjacking-newest-healthcare-risk
[141] Assessing the Severity of SQL Injection Threats to IoT Security https://www.smartdatacollective.com/assessing-severity-sql-injection-threats-iot-security/
[142] Carlo Gavazzi SmartHouse 6.5.33 XSS / Cross Site Request Forgery https://packetstormsecurity.com/files/155508/ZSL-2019-5543.txt
[143] Annual Report Telecom Security Incidents 2018 https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2018
[144] Misconfigured, Open DNS Servers Used In Record-Breaking DDoS Attack https://www.darkreading.com/attacks-breaches/misconfigured-open-dns-servers-used-in-record-breaking-ddos-attack/d/d-id/1139433

subscriber SMS interception by simulating a fake MSC which will then receive the SMS for this targeted subscriber. Interception of SMS messages could enable adversaries to obtain authentication codes used for multi-factor authentication. In [145] SS7 has been exploited to intercept two-factor authentication codes sent to online banking customers, allowing them to empty their accounts. The exploitation of SS7 design weaknesses to obtain a victim's location, harvest their messages, and listen in on calls was demonstrated in 2014.[146] Other examples are the demonstration in [147] and [148]. O2 in Germany confirmed that some customers in Germany have had their accounts drained by attackers that used SS7 to intercept and redirect mTANs to their own phones. [149] In [150], an attempted Data interception attacks using SS7 was reported.

- **Threat T2.2.2: Data session hijacking:** A data session hijacking was achieved by performing GTP attacks.[151] In 2014, attackers hijacked a portion of online traffic from a set of 19 ISPs, with the goal of stealing cryptocurrency from a group of users.[152] In April 2017, Rostelecom, a Russian ISP, leaked dozens of routes pertaining to IP addresses that belong to major financial services firms. The Russian ISP 'originated' 137 prefixes, 37 of which belong to financial, e-commerce, and payment services, like Mastercard, Visa, Forti, Alfabank. For 7 minutes, global traffic to these services was redirected via the Rostelecom network.[153] In 2018, a BGP hijack was used to divert traffic to Google from subscribers living in the west of the USA, via Russia, to China, allegedly intentionally and for espionage purposes.[154]
- **Threat T2.2.3: Traffic eavesdropping:** To conduct such an attack, attackers would need to have the proper equipment to capture and store the radio communication between the cellular mobile device and the base station. False Base Station (FBS), Rogue Base Station (RBS), International Mobile Subscriber Identifier (IMSI) Catcher or Stingray can be used for traffic eavesdropping

[145] After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/
[146] White hats do an NSA, figure out LIVE PHONE TRACKING via protocol vuln https://www.theregister.co.uk/2014/12/26/ss7_attacks/
[147] Tobias Engel, "SS7: Locate. Track. Manipulate", 2014, https://imsicatcher.info/article/ss7-locate-track-manipulate/
[148] "SS7 Attack Discovery" , Positive Technologies, 2016 https://www.ptsecurity.com/upload/corporate/ww-en/products/documents/ss7/PT-TAD-Product-Brief-eng.pdf
[149] Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer https://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504
[150] Tunnel Vision : Malicious data interception via SS7 https://www.adaptivemobile.com/blog/malicious-data-interception-via-ss7
[151] HITB2014AMS – Day 2 – On Her Majesty's Secret Service: GRX & A Spy Agency https://www.corelan.be/index.php/2014/05/30/hitb2014ams-day-2-on-her-majestys-secret-service-grx-a-spy-agency/
[152] Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins https://www.wired.com/2014/08/isp-bitcoin-theft/
[153] Rostelecom Route Leak Targets E-Commerce Services https://blog.thousandeyes.com/rostelecom-route-leak-targets-ecommerce-services/
[154] OK Google, why was your web traffic hijacked and routed through China, Russia today? https://www.theregister.co.uk/2018/11/13/google_russia_routing/

(passive and active) by exploiting security weaknesses in mobile networks. With mobile network evolution from 2G until 5G more security features have been added. However, the use of fake base station remains still possible and this issue is under discussion within the 3GPP SA3 to define a possible way to detect fake base station. The security enhancements provided with 5G network limit the type of information that can be gathered by using a fake base station. At least until 4G by using fake base station it is possible to retrieve the user IMSI, because device authenticates itself via its unique subscriber identity. This means that the fake BS can request the IMSI and gets it. 5G specifications provide the necessary mechanisms for protecting a user privacy and the subscriber's identity should have to be encrypted to prevent attacks from fake base station. Moreover, even in the current 5G there are some identification information transmitted from the device which are still unencrypted. This data can be captured by a fake BS and used to determine the class of devices, some hardware components, models and operating system. The info can be useful for attackers if they are looking for a specific custom device. An attacker can change the category of the target device so that the base station only provides 2G/3G connections. This will make the device vulnerable to other attacks specific to 2G/3G. In passive attacks, the false base station records and analyses the mobile radio signal of legitimate connections between the operator network and the targeted mobiles. The attacker can decode the network identifier of the targeted mobiles and possibly decrypt the communication content if it was encrypted using a vulnerable cipher algorithm. In an active attacker, the attacker is on the path of the communication between a targeted mobile and the legitimate network with a false base station used in a man-in-the-middle setup. The false base station impersonates the radio signal of a legitimate mobile network and forces the mobile device to connect to it by using a higher power signal. In the meantime, the false base station connects to the legitimate network by impersonating the targeted mobile. In 3G network, a false base station can relay the network authentication signaling to the intercepted mobile and ask the network to use either no security or vulnerable security algorithms. Examples of broken 2G cryptographic algorithms are A5/1 and A5/2. In addition, using a rogue base station broadcasting at a high-power level, an attacker can force a user to downgrade to either GSM or UMTS. For example, using a fake BS once IMSI of a target user has been obtained it could be possible to modify the 4G SDR based network code to degrade the 4G service completely forcing the device to look for another cell in the 3G frequencies or 2G [155]. Another way to perform downgrade attacks are reported in the paper "Practical attacks against privacy and availability in 4G/LTE mobile communications" [8]. Recently at the DefCon Security Conference in Las Vegas 2019, a team of researchers from Blackberry displayed how the calls can be hacked by cyber criminals.[156]

- **Threat T2.2.4: Traffic redirection:** An active domain name system (DNS) redirect attack, referred to as aLTEr has been recently demonstrated by researchers from Ruhr-Universität Bochum and New York University Abu

[155] Israel Accused of Planting Mysterious Spy Devices Near the White House http://fakebts.com/author/pedro/

[156] Hackers Could Decrypt Your GSM Phone Calls https://www.wired.com/story/gsm-decrypt-calls

Dhabi. [157] It allows an attacker to perform man-in-the-middle attacks to intercept communications and redirect the victim to malicious websites using DNS spoofing. This attack works by taking advantage of a design flaw within the LTE network: the data link layer (or layer 2) of the LTE network is encrypted with AES-CTR but it is not integrity-protected. This means an attacker can modify the bits even within an encrypted data packet, which later decrypts to a related plaintext. As a result, the attacker is posing as a cell tower to the victim, while pretending to be a subscriber to the real network.

- **Threat T2.3.1: Exploitation of software bugs:** Many attacks based on vulnerability exploitation have been reported against core and access networks. A massive attack was launched toward the end of 2016, main target was Deutsche Telekom Access Network and its Infrastructures. A cyber-attack that infected nearly one million routers used to access Deutsche Telekom Internet service was part of a campaign targeting web-connected devices around the globe. [158] The devices were vulnerable Customer Premises Equipment (CPE), and according to the telecommunications company, impacted customers were unable to connect to the Internet. Software vulnerabilities are also used to penetrate the network infrastructures by APT (Advanced Persistent Threat).[159] As described by Cybereason, the "Soft cell" operation started by exploiting a vulnerability in an unpatched IIS publicly-facing server from which the attackers gathered information about the network and propagated across the network. Recently it was also identified the Simjacker attack which exploit a vulnerability of a SIM Card technology, called S@T Browser. The key issue with the S@T Browser technology is that its default security does not require any authentication, and as a result the attacker is able to execute functionality on the SIM card with the aim to 'take over' the mobile phone to retrieve and perform sensitive commands. The location information of thousands of devices was obtained over time without the knowledge or consent of the targeted mobile phone users.[160]
- **Threat T2.3.2: Manipulation of hardware and firmware:** The Meltdown and Spectre vulnerabilities introduced the world to the power of hardware-level weaknesses. [161] The recently discovered LoJax [162] malware and the Hacking Team UEFI Rootkit are two of the most well-known examples of firmware attacks. In both examples, the malware targeted the system's UEFI firmware. These attacks took advantage of specific vulnerabilities and many other vulnerabilities have been discovered over the past few years in UEFI and

[157] Protecting against the latest LTE network attacks https://blogs.cisco.com/security/protecting-against-the-latest-lte-network-attacks
[158] New Mirai Variant Targets Routers, Knocks 900,000 Offline https://threatpost.com/new-mirai-variant-targets-routers-knocks-900000-offline/122155/
[159] Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
[160] New Simjacker vulnerability exploited by surveillance companies for espionage operation https://simjacker.com/
[161] Spectre and Meltdown explained: A comprehensive guide for professionals https://www.techrepublic.com/article/spectre-and-meltdown-explained-a-comprehensive-guide-for-professionals/
[162] LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/

related components. However, in some cases attackers do not need to exploit a vulnerability at all to install their malicious implants. Older systems and even some recent servers lack basic protections like signed firmware updates. These attacks can apply to virtually any devices that can be compromised with malware. While malware represents a common attack vector, research has shown that firmware can also be exploited remotely. This attack vector has a lot to do with the growing set of networking options found within UEFI components themselves. The standard UEFI codebase now includes a rich set of network capabilities for Ethernet, WiFi, and even Bluetooth that allow the firmware to communicate remotely and even perform a full HTTP boot from a remote server across the Internet. Eclypsium researchers found that in some cases the update over the Internet functionality was downloaded unverified and in the clear. The host would try to contact a remote update server using plain HTTP without SSL or any verification. This means that simple man-in-the-middle or other redirection techniques (e.g. DNS/ARP/route poisoning) could be used to modify the response returned to the client and exploit the vulnerability. As a result, the research showed that one could remotely deliver malicious code resulting in buffer overflows and arbitrary code execution just by checking if a newer version of the firmware exists.[163]

- **Threat T2.3.3: Malicious code/software/activity:** One of the most important technology in the network environment is the Software Define Network (SDN). SDN technology aims to replace the physical network by using a decoupled Data plane-Control plane architecture controlled by software. Although no specific malware attack has been already public announced, ETSI Security experts published the "ETSI GS NFV-SEC 003: Network Functions Virtualization (NFV); NFV Security; Security and Trust Guidance", where malware is indicated as one of the main threat vectors. Also, Academia and independent researchers are investigating the topic. As an example of such investigations, in 2016, during the Black Hat event, it was presented a paper "attacking SDN infrastructure: are we ready for the next-gen networking?". [164] The paper describes how malware can attack and damage SDN infrastructures. Two uses case have been presented: the first one shows how to infect the SDN Control Plane at Build-time and the second one how to infect the SDN Control plane at run time. Another example of malware spread that impacted the network functions was Wannacry, a ransomware crypto-worm that targeted computers running the Microsoft Windows operating system on May 2017. Once installed in a computer, thanks to its worm behavior, it had the capabilities to spread into the local networks compromising the functionality of the network. Telefonica was impacted by this attack[165].Malware spread can impact also the endpoint network asset. As a recent example, during June 2019 a new variant of malware was detected which aim to wipe the firmware of IoT devices in attacks reminiscent of the old BrickerBot malware that destroyed millions of devices back in 2017. This new variant is named Silex, it works by trashing an

[163] Remote UEFI Attacks https://eclypsium.com/2018/08/27/uefi-remote-attacks/
[164] ATTACKING SDN INFRASTRUCTURE: ARE WE READY FOR THE NEXT-GEN NETWORKING? https://www.blackhat.com/docs/us-16/materials/us-16-Yoon-Attacking-SDN-Infrastructure-Are-We-Ready-For-The-Next-Gen-Networking.pdf
[165] What is the WannaCry Ransomware Attack? https://www.upguard.com/blog/wannacry

IoT device's storage, dropping firewall rules, removing the network configuration, and then halting the device[166].

- **Threat T2.3.4: Remote activities (execution):** In 2018 Hackers targeted mobile phone networks around the world aiming to obtain CDR records.[159] The threat actor was attempting to steal all data stored in the active directory, compromising every single username and password in the organization, along with other personally identifiable information, billing data, call detail records, credentials, email servers, geo-location of users, and more. The attack began with a web shell running on a vulnerable, publicly-facing server, from which the attackers gathered information about the network and propagated across the network. The threat actor attempted to compromise critical assets, such as database servers, billing servers, and the active directory. The hackers created privileged accounts to easily regain access later, and in one case even set up a VPN connection to easily tunnel back into the network.
- **Threat T2.3.5: Malicious code - Signaling amplification attacks:** An attack consists of malicious users who take advantage of the signaling overhead required to setup and release dedicated bearers to overload the signaling plane by repeatedly triggering dedicated bearers' requests. A botnet of infected mobile devices could be used to generate a signaling amplification attack by forcing each terminal to constantly establish and release IP connections with an external server [115]. A piece of malware could also trigger mobile phones to reboot at the same time, thereby potentially overloading the Evolved Packet Core (EPC) with registrations once they come back up. It is also necessary to consider that, Home Subscriber Server (HSS) is also involved in a significant number of signaling processes at the EPC; thus, can as well suffer from signalling amplification attack. Such saturation of the EPC could potentially also occur legitimately due to the overwhelming amount of traffic and frequent reconnections of billions of Machine to Machine (M2M) nodes. Amplification attacks exploiting Network Time Protocol (NTP) and DNS signalling are reported in [167].
- **Threat T2.4.1: Failures of devices or systems:** A system failure caused a mobile internet, telephony and SMS outage for thousands of users. A software bug occurred in the SPR (Subscriber Profile Repository) server. Following the repeated instability of the equipment, the signalling traffic increased and the STP (Signalling Transfer Point) platforms became overloaded. As a result, end users had difficulties to access mobile internet services as well as voice and SMS services. The vendor responded by fully restoring the functionality of the SPR equipment. To stop the avalanche of signalling messages, the 3G and 4G networks were partially shut off and all subscribers were located on the 2G network.[143] A system failure caused a mobile internet outage for millions of users. A software bug occurred in the Internal system component Software Deployment Manager (SDM) leading to the degradation of user authorisation for mobile data and mobile voice. As a result, end users had difficulties to access mobile services, both voice and data. Also, customers abroad were affected (roaming services). Mobile switches and mobile user registers were affected by

[166] New Silex malware is bricking IoT devices, has scary plans https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/
[167] See https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

this bug. The provider removed the obstacles in accessing the services and for the prevention of similar incidents in the future, a mitigation plan was created in collaboration with software vendors.[168] System failure caused disruption in, both mobile and fixed, telephony and internet services as well SMS/MMS services, affecting millions of users. Outage of several network components used for delivering DSL in the subscriber access network resulted in the disruption of mobile and fixed telephony and internet access. The provider responded by raising the capacity of the remaining network components. A subsequent software upgrade resolved the issue.[168]

- **Threat T2.4.2: Supply chain:** In 2018, several examples of supply chain attacks have been identified, including tampering with chipsets [169] and vulnerabilities in AMD processors.[170] A recent case of "supply chain attacks" is the "NotPetya" malware. It spreads to systems that had a specific accounting software installed. The investigation of the incident revealed that the threat actor behind the attack compromised the infrastructure of the software provider, tampered the software, and pushed the tampered version of the software to the provider's clients as a legitimate software update. The software update essentially installed the "NotPetya" malware on the victim-machines. Another case is a backdoor dubbed ShadowPad. It was injected into a network management software suite and was pushed through a software update to the respective systems that had the software installed. The attack was spotted when a company using the software observed suspicious domain name lookup requests. Such a backdoor could potentially allow the threat actor behind the attack to load malware on the victim systems and/or exfiltrate data.[171]
- **Threat T2.4.3: Software bug:** Multiple vulnerabilities were found by security researchers in 4G routers manufactured by several companies, with the flaws exposing users to information leaks and command execution attacks.[172]

A.3 Attacks related to System-Centric Security

In the following, the main attacks affecting System domain are reported. We note that the threat description is available in Section 3.3.5.

- **Threat T3.1.1: Information leakage/sharing due to human errors:** Information leakage due to misconfiguration has been reported in many studies in literature and by CSA as one of the major sources of security issues.

[168] Annual Report Telecom Security Incidents 2017 – enisa, https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017/at_download/fullReport

[169] Security researcher claims Via C3 x86 CPUs contain hidden 'God mode' https://www.computing.co.uk/ctg/news/3060992/security-researcher-claims-via-c3-x86-cpus-contain-hidden-god-mode

[170] 13 flaws found in AMD processors, AMD given little warning https://www.networkworld.com/article/3262976/security/13-flaws-found-in-amd-processors-amd-given-little-warning.html

[171] ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world

[172] 4G Router Vulnerabilities Lets Attackers Take Full Control https://www.bleepingcomputer.com/news/security/4g-router-vulnerabilities-let-attackers-take-full-control/

In 2017, a misconfigured AWS Simple Storage Service (S3) cloud storage bucket exposed detailed and private data.[173] In 2018, a server misconfiguration (public access) exposed the Elasticsearch database owned by Exactis to a massive breach containing highly personal data.[174] Again, in 2018, a misconfigured rsync server for backup permitted unauthenticated data transfer to any rsync client exposing, Level One Robotics customers' data (including Volkswagen, Chrysler).[175] Another famous example refers to Verizon customer accounts data beaches due to misconfiguration of S3 buckets. Other human errors can lead to system outage like in the case of the famous AWS employ error that took server offline.[176] AWS said that it has not had to fully reboot these S3 systems for several years, and the program has grown extensively since then, causing the restart to take longer than expected.

- **Threat T3.1.2: Inadequate design and planning or incorrect adaptation:** Examples of inadequate planning refers to the lack of controls on backups, and data cloning for internal management processes. Accenture inadvertently left a massive store of private data across four unsecured Amazon S3 buckets, exposing highly sensitive passwords and secret decryption keys (this type of attacks is also relevant for data-centric security in Section 3.6). S3 buckets contained data that could be downloaded without a password by anyone just knowing the web addresses of the server.[177] Similarly, data that belong to Honda Connect App were exposed online. Researchers form Kromtech Security Center discovered the data stored on two unsecured, publicly accessible and unprotected Amazon AWS S3 Buckets.[178] In 2018, more than 120 million unique identification numbers issued by the Brazilian Federal Reserve to Brazilian citizens were exposed on unprotected S3 Bucket.[179] The problem was that the server was treated as accessible web server, while it should be protected. In 2019, Voipo, a Voice over Internet Protocol (VoIP) telecom company, exposed millions of unencrypted customer call logs and credentials on an Elasticsearch database.[180] The problem was again inadequate planning since it was declared that the server exposed was a development server having no security features enabled. Migration process can be also considered a source of serious threats for visualization, where migration is normally handled automatically for the sake of dynamic load balancing. During live migration, an attacker at malicious hypervisor may falsely advertise available resources to migrate the compromised VM to the trusted hypervisor. This is a malicious

[173] See https://www.forbes.com/sites/thomasbrewster/2017/12/19/120m-american-households-exposed-in-massive-consumerview-database-leak/#59144ada7961
[174] See https://www.wired.com/story/exactis-database-leak-340-million-records/
[175] See https://www.upguard.com/breaches/short-circuit-how-a-robotics-vendor-exposed-confidential-data-for-majormanufacturing-companies
[176] See Amazon explains big AWS outage, says employee error took servers offline, promises changes https://www.geekwire.com/2017/amazon-explains-massive-aws-outage-says-employee-error-took-servers-offline-promises-changes/
[177] See https://www.zdnet.com/article/accenture-left-a-huge-trove-of-client-passwords-on-exposed-servers/
[178] Personal data of over 50,000 Honda Connect App leaked https://www.hackread.com/personal-data-of-over-50000-honda-connect-app-leaked/
[179] Exposed S3 bucket compromises 120 million Brazilian citizens https://www.scmagazine.com/home/security-news/exposed-s3-bucket-compromises-120-million-brazilian-citizens/
[180] See https://www.zdnet.com/article/voipo-database-exposed-millions-of-call-and-sms-logs-system-data/

activity exploiting a wrongly designed migration process. Other examples refer to VM rollback. For instance, while restoring a VM from a snapshot to a previous state, the security features enabled in the actual state can be disabled. VM rollback can be exploited by an attacker even using a brute-force approach [116]. VM cloning can be used to copy and move a VM without revealing to the user that the VM has been cloned in multiple instances. VM cloning can be also executed for the legitimate scope of backup. In this case the backup location must be secured for intromission or copy even not intentional. Another example of wrongly designed process is the one related to Apache CloudStack (version before 4.5.2), which does not properly preserve VNC passwords when migrating KVM virtual machines (CVE-2015-3252), exposing to attacks at credential level.

- **Threat T3.2.1: Interception of information:** Attacks aiming to intercept data exchanged in internal or external communications involving the system at every level have been proposed in the past. At cloud level most of the attacks refer to applications deployed on the cloud. More details are available in Section 3.7. Considering virtualization layer, the recent foreshadow vulnerability (CVE-2018-3646) that affects XenServer allows an attacker to create a speculative side channel and steal data in VMRAM from other non-trusted VMs on the same physical server. Other attacks can exploit the cold boot of VM memory snapshot to capture sensible data or read the memory exchanged by different VMs [117]. Zhang et al. [118] used Prime+Probe technique on L2 cache to detect co-location on Xen. Monitoring L1 cache timing, Zhang et al. [119] extracted the ElGamal secret key that is used for GNU Privacy Guard decryption performed in another VM, while Weiß et al. [120] extracted AES keys of a VM running on an ARM Cortex-A8 processor. Irazoqui et al. [121] demonstrated a side-channel attack to recover AES keys in Xen and VMWare. Yarom et al. [122] used a flush and reload approach to observe shared pages of Intel X86 processor to extract private keys across multiprocessor and multicore running VMs. A related technique called Prime+Probe was adopted by Inci at el. [123] to monitor L3 cache in order to extract noisy data from Amazon E2 VM and use it to obtain RSA encryption key. Other approaches try to setup a covert-channel attack. Maurice et al. [124] used the same Prime+Probe approach for LLC-based covert channel. Xiao et al. [125] presented a memory deduplication-based covert-channel attack which is faster than L2 cache-based attacks. Another type of attack is the rowhammer attack across VMs exploiting memory de-duplication to obtain, for instance, a side channel and a covert channel [126]. Most of the above attacks use malicious actions or malware as vectors to exploit the vulnerability.
- **Threat T3.2.2: Unauthorised acquisition of information (data breach)***:* In general data breach is the main goal of an attack and therefore most of the attacks can be related to data breach. A famous example that refers to a cloud service is the Dropbox data breach in 2014[181] that permitted the discovery of private file transfer links. More recently, another data breach targeted Amazon

[181] Dropbox and Box leak files in security through obscurity nightmare https://www.techrepublic.com/article/dropbox-and-box-leak-files-in-security-through-obscurity-nightmare/

Black Friday, where details about amazon e-commerce was exposed.[182] These attacks also link to application-centric domain in Section 3.7. The famous VENOM vulnerability (CVE-2015-3456) at virtualization layer that affects Qemu can potentially lead to data breach as well. It allows an attacker to break out a VM, execute code on a host machine, and access all the other VMs on the host. A potential data breach was also reported as connected to VMware and Dell EMC storage as a service technology and a trio of critical vulnerabilities (CVE-2017-15548, CVE-2017-15549, and CVE-2017-15550). A set of potential data breaches are related to attacks on VM images focused on extracting data from the VM image file at rest. Similar to this, but more sophisticated, is the VM data remanence attack. Data remanence was experimented by Albelooshi et al. [127] to see if physical representation of digital data remains on the physical device even after its removal. We refer to Section 3.6 for additional attacks specifically on the data domain.

- **Threat T3.3.1: Configuration poisoning:** The case of Capital One attack is an example of multiple deliberate configuration poisoning of both firewall and S3 bucket to expose data.[183] In 2017 National Credit Federation exposed its customers data due to an intentional poisoning of AWS S3 bucket configured for public access under a subdomain. As a side note, the company did not react immediately to this potential breach due to the difficulties of updating device firmware (see threats in Section 3.3.3). In 2019, Ascension, a data and analytics company, database was exposed on a publicly accessible elastic search database apparently due to a poisoned backup process. Again in 2019, a massive government data set belonging to the Oklahoma Department of Securities (ODS) was left unsecured on a storage server (based on an open access rsync) exposing millions of sensitive files.[184]
- **Threat T3.3.2: Business process poisoning:** A famous example of BPC attack was the one of Bangladesh Central Bank, which resulted in losses of up to US$81 million poisoning the SWIFT protocol for money transfer using a piggybacking approach. This is more at application level, but similar concepts can be exploited at cloud/virtualization level. Considering the cloud environment, the business process implementation in cloud is a preferred target for compromising since it is much less visible than a normal business process and the attacker activities can be more complex to detect. Another example refers to VM relocation. It can be exploited explicitly poisoning the process to target a malicious server, where memory snapshot is enabled [128]. Other examples in threat T3.1.2 that are relative to inadequate design and planning or incorrect adaptation can be exploited also via ad hoc poisoning of cloud/virtualization processes.
- **Threat 3.4.1: Identity fraud:** In a virtualized environment, privilege escalation can be even more dangerous than in a physical environment because of multitenancy and the hierarchical structure of administrator privileges. In addition, VMM is a crucial target for usurpation-based misappropriation, due

[182] Amazon hit with major data breach days before Black Friday https://www.theguardian.com/technology/2018/nov/21/amazon-hit-with-major-data-breach-days-before-black-friday

[183] Capital One Data Breach Impacts 100 Million Customers https://divvycloud.com/capital-one-data-breach/

[184] Unprotected Government Server Exposes Years of FBI Investigations https://thehackernews.com/2019/01/oklahoma-fbi-data-leak.html

to its role in virtualization, as well as to the presence of vulnerabilities that allow guest-OS users the potential to execute arbitrary code on the host OS.[185] Timehop had a data breach due to compromised admin credentials that were used to enter their Cloud.[186] Deloitte experienced a major data breach due to weak identity, credential and access management or its Azure account in 2017. More recently, in 2018, a German student hacked data protected by weak passwords.[187] Generally speaking, 2017 was the year of the rise of cloud account-targeted campaigns, in particular for Microsoft Office 365 accounts. Another example of account hijacking was presented as a PoC in 2018. It was based on compromises of Microsoft live accounts via subdomain hijacking.[188]

- **Threat T3.4.2: Denial of service:** Both on cloud and virtualization the main scope of the attacker is to exploit the sharing of resources. In virtualization, examples of attacks are the ones that focused on the hypervisor crash. A VM may corrupt the hypervisor memory and cause the hypervisor to crash leading to DoS (CVE-2018-7542 on Xen via NULL pointer dereference).[189] Resource starvation can be exploited to violate the availability of the hypervisor via uncontrolled resource allocation [129]. In cloud, the concept is very similar due to the idea to share services among different users and tenants. However, some DoS attacks in cloud also target the API exposed by the different cloud layers. Yeh et al. [130] presented a multi-resource DoS attack on cloud VM migration schemes.
- **Threat T3.4.3: Malicious code/software/activity:** The Zepto variant of the Locky ransomware spreads via cloud services such as Microsoft OneDrive, Google Drive and Box by sharing a malicious file with potential victims. Similarly, CloudSquirrel attack establishes a connection with its command and control hosted in Dropbox. Historical examples of hyperjacking are the SubVirt [131] that installs a hypervisor below the host OS and controls the VM and the Blue Pill [132] that exploits hardware extensions in the virtualization enabled CPUs and runs an infected system into a VM. In the work of Jasty et al. [133], VM hoping has been demonstrated by maliciously gaining an access to different VMs.
- **Threat T3.4.4: Generation and use of rogue certificates:** This threat is usually at the basis of other more complex attacks as discussed in the previous threats. As an example, BIG-IP and BIG-IQ do not properly regenerate certificates and keys when deploying VM image on AWS, Azure or Verizon cloud service, which makes multiple instances to share the same certificates and keys. It causes the disruption of services eventually leading to information leak (CVE-2016-2084).

[185] Common Vulnerabilities and Exposures (2012) CVE-2012-2450. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2450.
[186] Timehop discloses July 4 data breach affecting 21 million https://techcrunch.com/2018/07/09/timehop-discloses-july-4-data-breach-affecting-21-million/
[187] German Man Confesses to Hacking Politicians' Data, Officials Say https://www.nytimes.com/2019/01/08/world/europe/germany-hacking-arrest.html
[188] PoC Exploit Compromises Microsoft Live Accounts via Subdomain Hijacking https://threatpost.com/poc-exploit-compromises-microsoft-live-accounts-via-subdomain-hijacking/138719/
[189] A Methodology for Determining Forensic Data Requirements for Detecting Hypervisor Attacks https://pdfs.semanticscholar.org/4e09/697e99b107f11f90ca563160d4be95bb90c2.pdf

- **Threat T3.4.5: Misuse of assurance tools:** The complexity of the current cloud systems makes the poisoning of assurance tools critical to cover unauthorised access to large amounts of personally identifiable data. No recent attacks have been reported.
- **Threat T3.4.6: Failures of business process:** In general, there are a number of attacks that exploit shadow IT. Some of them rely with the usage of apps installed on mobile devices or on free services used by one or more company employee, for instance, to fulfil a temporal need. In many of the cases, these services are used just few times and then forgotten, without taking care of updates and new security issues discovered. Reports on attacks exploiting shadow IT are not frequent, since they are not easy to be discovered; however, every attack that is caused by an employee using a vulnerable service against company regulations in terms of adoption of abnormal usage can be considered relevant to this threat. NormShield reports on breaches caused by third parties. This can be considered as a superset of the Shadow IT based attacks including also app misuse in some cases.
- **Threat T3.4.7: Code execution and injection (unsecure APIs):** A famous attack dates back to 2010. An Amazon cross-site scripting (XSS) bug enabled credential theft. Another famous attack was the one of US Internal Revenue Service (IRS) in 2015, which exposed a great amount of record via a vulnerable API ("Get Transcript"). More recently, a vulnerability of Facebook API was exploited resulting in the generation of an access token that had the permissions of the Facebook mobile app, not for the viewer, but for the other Facebook user. This also links back to account hijacking. Considering virtualization level, and specifically the management interface injection vulnerability can be exploited. For example, CSS vulnerability (CVE-2012-5050) in VMware vCenter Operations before 5.0.x allows remote attackers to inject arbitrary web script to take control of vCenter". The Iago attack [134] is an example of virtualization level API call from kernel perspective. Supposing to have a malicious kernel, it can make an application to act against its interests by communicating with it, since applications generally do not check return values from the kernel.
- **Threat T3.5.1: Violation of laws or regulations data:** See Chapter 4.
- **Threat T3.6.1: Skill shortage:** Examples of attacks that ground on skill shortage can be found in TG3.1. The main problem is the wrong "lift-and-shift" approach in moving traditional ICT to the cloud, where missing skills play a significant role.
- **Threat T3.6.2: Malicious insider:** A famous example of malicious insider was the 2018 Tesla saboteur. The sabotage included the use of false usernames to make changes to the code used in the Tesla Manufacturing Operation System Cloud, as well as exporting large amounts of highly sensitive data to unknown third parties. Another example of malicious insider that can be also linked to failure of business process was discovered in 2018 and refers to an engineer that was found guilty of stealing navy secrets via personal Dropbox account.[190] Considering virtualized environments, a compromised management interface can be used to exploit vulnerabilities by a privileged user (CVE-2016-9603,

[190] Engineer Found Guilty of Stealing Navy Secrets via Dropbox Account https://www.bleepingcomputer.com/news/legal/engineer-found-guilty-of-stealing-navy-secrets-via-dropbox-account/

CVE-2017-2615), having the scope to attack the hypervisor like the compromising CIA, DMA attack exploiting the direct channel between hypervisor and the HW, VM sprawl attack aimed to violate the hypervisor availability. In addition, management interface can be directly accessed by a malicious insider [135] [136] leading to attacks on the VMs [137].

A.4 Attacks related to Data-Centric Security

In the following, the main attacks affecting Data domain are reported. We note that the threat description is available in Section 3.3.6.

- **Threat T4.1.1: Information leakage/sharing due to human errors:** Information leakage due to misconfiguration has been reported in many studies in literature. BinaryEdge [191] showed how erroneous system misconfigurations led to weaknesses in Redis, MongoDB, Memcache and ElasticSearch. The same study comments how very often these technologies are meant to be installed in private environments, providing weak default security configurations (e.g., no authentication or encryption), privileging performance. Other attacks have been reported with unauthorised sharing of sensitive and confidential information.[192] The data breach targeting Equifax[61] in 2017 was one of the widest breaches ever. Hackers took advantage from a well-known bug that was exploited due to the fact that the Equifax system was not up to date. The hackers stolen names, birthdates, Social Security numbers, addresses, and driver license numbers for 145.5 million Americans plus approximately 200,000 credit card numbers, and affected more than 100 million credit users worldwide. [193] Targeted phishing attacks are rapidly increasing and are relevant for both data and user domains.[74] Cyber criminals target rich individuals and top-management people that have access to sensitive data, as well as public authorities that handle personal identifiable information.[194] [195] Also, a shift from consumer to enterprise targets has been observed and driven by profit.[61] [74] Business email compromise (BEC) scams[196] is a financial fraud also called CEO fraud that aims to reduce the effort of a phishing attack. Before sending an attack, the cyber-criminals identify the preferred victim in the business (e.g., someone from the finance department), and send a fraudulent email, impersonating the CEO or CFO. PIR Bank in Russia lost $920,000 due to an outdated, unsupported cisco router that was used as a trojan horse to reach the core of the bank.[197] A similar issue happened to British Airways, where an outdated version of Modernizr Javascript library was exploited to steal

[191] Data, Technologies and Security - Part 1 http://blog.binaryedge.io/2015/08/10/data-technologies-and-security-part-1/
[192] Dropbox Security Bug Made Passwords Optional For Four Hours, http://techcrunch.com/2011/06/20/dropbox-security-bug-made-passwords-optional-for-four-hours/
[193] Data Breach https://www.malwarebytes.com/data-breach/
[194] Malwarebytes LABS, Cybercrime tactics and techniques: Q2 2018 https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf
[195] KrebsOnSecurity, The Year Targeted Phishing Went Mainstream, https://krebsonsecurity.com/2018/08/the-year-targeted-phishing-went-mainstream/
[196] Symantec, BEC Scams Remain a Billion-Dollar Enterprise, Targeting 6K Businesses Monthly, July 2019 https://www.symantec.com/blogs/threat-intelligence/bec-scams-trends-and-themes-2019
[197] Data Breach Investigations Report 2019, https://enterprise.verizon.com/resources/reports/dbir/

customer data.[197] [198] MongoDB, a major open source NoSQL database, was the target of different attacks. In 2015, [199] three students from University of Saarland in Germany at the Centre for IT Security found that the default installation of MongoDB running at TCP port 27017 was freely available for read and write operations. More recently, in 2017, hackers have wiped more than 26k MongoDB again exploiting its default configuration permitting connections from the Internet.[200] A rise in attacks to Hadoop components, such as Hadoop YARN, Redis, and ActiveMQ has been observed. The goals of these attacks can be different, from cryptomining to ransomware and data wiping.[201] [202] [203] A company affiliated to FedEx was breached due to an unsecure Amazon S3 server and resulted in data exposed on the internet.[74] Similarly, data from 221 LA County was accidentally exposed due to a misconfigured S3 cloud server.[74]

- **Threat T4.1.2: Inadequate design and planning or incorrect adaptation:** It has been shown how the replication approach taken by Hadoop framework can backfire:[204] a corrupted application could destroy all replicas. Damiani [138] claims that Hadoop redundancy could even be a non-linear risk booster for Big Data leakages. Also, Aditham [139] shows how the design of the Hadoop Distributed File System (HDFS) could introduce security problems. HDFS, which is the basis of many storage systems, originally, cannot tolerate the failure of Namenode, as proved in real scenarios.[205] Finally, NIST reported a scenario where digital rights management (DRM) techniques were not built to scale and caused system failures.[206] [207] In 2017, Amazon AWS and, in particular,

[198] A simple fix could have saved British Airways from its £183m fine
https://www.wired.co.uk/article/british-airways-data-breach-gdpr-fine
[199] 40,000 UnProtected MongoDB Databases Found on the Internet
https://thehackernews.com/2015/02/mongodb-database-hacking.html
[200]More than 26,000 vulnerable MongoDB databases whacked by ransomware
https://www.zdnet.com/article/mongodb-ransacking-starts-again-hackers-ransom-26000-unsecured-instances/
[201] Securonix Threat Research:Detecting Persistent Cloud Infrastructure/Hadoop/YARN Attacks Using Security Analytics:Moanacroner, XBash, and Others https://www.securonix.com/web/wp-content/uploads/2019/01/Securonix_Threat_Research_Moanacroner_XBash.pdf
[202] Hadoop coop thrown for loop by malware snoop n' scoop troop? Oh poop
https://www.theregister.co.uk/2019/01/24/hadoop_malware_attack/
[203] Securonix Threat Research: Detecting Persistent Cloud Infrastructure/Hadoop/YARN Attacks Using Security Analytics: Moanacroner, XBash, and Others https://www.securonix.com/securonix-threat-research-detecting-persistent-cloud-infrastructure-hadoop-yarn-attacks-using-security-analytics-moanacroner-xbash-and-others/
[204] How Your Hadoop Distribution Could Lose Your Data Forever
http://www.smartdatacollective.com/michelenemschoff/193731/how-your-hadoop-distribution-could-lose-your-data-forever
[205] See "Notes by Facebook engineering" in https://www.facebook.com/notes/facebook-engineering/under-the-hood-hadoop-distributed-filesystem-reliability-with-namenode-and-avata/10150888759153920
[206] NIST Special Publication 1500-4. Use case: consumer digital media (examples: Netflix, iTunes, and others).
[207] Xiao Zhang, "A Survey of Digital Rights Management Technologies", see
http://www.cse.wustl.edu/~jain/cse571-11/ftp/drm.pdf

its S3 storage, suffered a major outage.[208] [209] This outage was due to the fact that to fix a performance problem an incorrect command was sent causing this unexpected disruption. After this command was set, an unpredictable sequence of cascading events caused the big denial of service. Apache Ambari erroneously stored sensitive data on disk in temporary files on the Ambari server host.[210] These files were then readable by any authenticated users. The database server of Exactis was publicly accessible and resulted in the theft of millions user records.[74] [211]

- **Threat T4.2.1: Interception of information:** Attacks aiming to intercept data exchanged in internal or external communications involving the Big Data platform have been proposed in the past. Among them, we can consider hijacking and eavesdropping. Hijacking is an active attack and aims to take control of a communication and its content (this attack is considered in the network-centric domain in Section 3.4). Eavesdropping is a passive attack where the content of the communication is intercepted without interfering with the information flow. In 2017, the biggest data breach targeting Equifax[61] affected more than 100 million credit users worldwide and across the EU. Note that the General Data Protection Regulation (GDPR) that became applicable in May 2018 dictates the mandatory reporting of data breaches (both to affected individuals and Data Protection Authorities), provided that certain requirements are met. A vulnerability in Apache Hadoop Distributed File System (HDFS) permitted cyber criminals to remotely access sensitive information with no authentication. [212] Apache Ambari permitted cyber attackers to steal sensitive information, caused by the exposure of passwords for Hadoop credential. These passwords are stored in Ambari Agent informational log messages when the credential store feature is enabled for eligible services.[213] [214]
- **Threat T4.2.2: Unauthorised acquisition of information (data breach):** Massive privacy breaches (discussed in Section 3.8) have been reported,[215] [216] where administrative credentials have been used to regularly access private user information. As already mentioned, in 2017, the biggest data breach targeted Equifax[61] and affected more than 100 million credit users worldwide. Data breach at Yahoo is the biggest data breach ever and involved three billion

[208] Typo blamed for Amazon's internet-crippling outage https://www.theguardian.com/technology/2017/mar/03/typo-blamed-amazon-web-services-internet-outage

[209] Amazon knocked AWS sites offline because of typo https://www.zdnet.com/article/amazon-knocked-aws-sites-offline-because-of-typo/

[210] See https://www.cvedetails.com/cve/CVE-2017-5655/

[211]Cyber Risk Outlook 2018 https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf

[212] Common Vulnerabilities and Exposures https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1296

[213] Apache Ambari Hadoop credential stores information disclosure https://exchange.xforce.ibmcloud.com/vulnerabilities/146702

[214] See https://www.cvedetails.com/cve/CVE-2018-8042/

[215] "Google fires employees for breaching user privacy" in TechSpot news, (Sept 2010) in http://www.techspot.com/news/40280-google-fired-employees-for-breaching-user-privacy.html

[216] Armerding, T., The 17 biggest data breaches of the 21st century, https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, 2018.

customers.[61] [217] Abuse of Point of Sales (POS) terminals is another example of unauthorised acquisition of information.[61] The terminal is manipulated to access and distribute the data of the customers, or in other cases fake companies are created to steal these data. A weakness in the "Search" capability of the Facebook platform resulted in one of the biggest data breaches where about 2.000 million users' information was exposed (including Cambridge Analytica case[218]).[74] A problem in the Twitter procedure for password handling exposed passwords in plain text.[74]

- **Threat T4.3.1: Data poisoning:** Data poisoning is often seen as a preparation activity for launching attacks (e.g., Carbanak and Cobalt malware[219]). It is at the basis of the other threats in this deliverable, as a means for hiding malicious behavior and covering malicious traces (see Threat T4.4.5), and as a way to manipulate inferences and decisions. Specific to this threat, in 2015, attacks to drug infusion pump have been reported.[220] [221] Cyber criminals were able to modify the amount of drugs distributed to patients potentially causing an overdose, due to lack of authentication. Different attacks of this type are also reported in Section 3.3.
- **Threat T4.3.2: Model poisoning:** Adversarial machine learning is a technique developed in the field of machine learning that aims to fool model learning through data poisoning [140]. The goal is to provide model training with fake data that cause the trained model to make a mistake and malfunction. Zhao et al. [141] presented an overview of data poisoning attacks on multi-task relationship learning, and an approach to optimal data poisoning. Yi et al. [142] presented an adversarial machine learning approach that aims to spectrum data poisoning attack. The goal is to let an adversary falsify the spectrum sensing data in wireless communications. Li et al. [143] presented data poisoning attacks on collaborative filtering systems, where an attacker generates malicious data to avoid being detected. Zugner et al. [144] studied adversarial attacks on neural networks for graph data.
- **Threat T4.4.1: Identity fraud:** Some of the attacks based on identity fraud target the control infrastructure (and the user's system interface) where the Big Data systems is built, such as private or public clouds [145]. An attack permitting to take control over the console gives to the attacker the ability of managing the user's account including the access to stored data. Attacks of this type [222] are based on a mixture of signature wrapping and advanced XSS techniques, then privilege escalation leading to identity fraud. Last but not least, attacks often target social networks (see Section 3.8 for more details). For example, XSS vulnerabilities on Twitter have been used to push malicious and fake tweets, while Internet malware has emerged on Facebook as a means of

[217] Djurberg, J. A., Bekräftat: ddos-attack bakom tågförseningar [Confirmed: DDOS attack behind train delays], https://computersweden.idg.se/2.2683/1.690504/ddos-bakom-tagforseningar, 2017
[218] The Value of Personal Online Data https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data
[219] Carbank/Cobalt A global threat to financial institutions https://www.europol.europa.eu/sites/default/files/documents/carbanakcobalt.pdf
[220] A hacker can give you a fatal overdose https://money.cnn.com/2015/06/10/technology/drug-pump-hack/
[221] Hacker Can Spend Fatal Dose to Hospital Drug Pumps https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/
[222] US-CERT warns of guest-to-host VM escape vulnerability http://www.zdnet.com/article/us-cert-warns-of-guest-to-host-vm-escape-vulnerability/

promoting malicious profiles.[223] Social engineering attacks continue to grow with the goal of obtaining personal data, hijacking accounts, steal identities.[61] Identity fraud can also target companies. For instance, attackers can try to impersonate legitimate businesses to retrieve Point of Sales (POS) terminals that are then used to steal customer data.[61] This attack is possible since the information used to request a POS is non-confidential. The Card-not-present fraud is another example of attack that can be linked to the identify fraud.[61] Stolen credit cards are used for e-commerce shopping. These attacks are particularly relevant also for user-centric security in Section 3.8, since users (and their data) become the target of the attacks.

- **Threat T4.4.2: Denial of service:** A DoS attack targeted the Hadoop cluster, leading to a significant decrease of system performance and causing the loss of the targeted resource to other cloud users [146]. An attack to Amazon distributed storage was also reported, based on authenticated requests and account validation.[224] Also, attacks to social networks have been reported, such as the one exploiting some weaknesses of the Hadoop Distributed File system, to target Facebook.[205] Today, Distributed-Denial-of-Service (DDoS) attacks are distributed as a tool against private business as well as the public sector. The aims of these attacks are used financial gains, as well as ideological, political or purely malicious reasons. This type of attack is the most widespread second to malware attacks only (2017), and is increasingly becoming more accessible, low cost and low risk. Data wiping attacks target data availability by overwriting files/data with random data or by deleting them. Shamoon Malware infects a system and then wipes all its files, destroying the hard disk and making systems unusable. It was first introduced in 2012, and then reused in 2016, to attack oil and gas company Saudi Aramco in the Middle East. In 2018, the last version of the malware was used to attack the Italian oil and gas firm Saipem.[225] The new malware involves a new wiper that deletes files from infected computers before the Shamoon malware wipes the master boot record. Saipem stated that between 300 and 400 servers and up to 100 personal computers were compromised. DemBot malware [226] [227] targeted Hadoop server using a YARN exploit to take control of the system and launch a DDoS attack. A similar attack used Mirai malware to exploit the same Hadoop YARN exploit and launch a devastating DDoS.[228] [229]

[223] See Nine Threats Targeting Facebook Users in http://www.itbusinessedge.com/slideshows/show.aspx?c=90875
[224] ZDnet bog in http://www.zdnet.com/article/amazon-explains-its-s3-outage/
[225] Shamoon: Destructive Threat Re-Emerges with New Sting in its Tail https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
[226] DemonBot Malware Targets Apache Hadoop Servers Using Available Exploit Code https://www.tenable.com/blog/demonbot-malware-targets-apache-hadoop-servers-using-available-exploit-code
[227] New DDoS botnet goes after Hadoop enterprise servers https://www.zdnet.com/article/new-ddos-botnet-goes-after-hadoop-enterprise-servers/
[228] Mirai 'botmasters' now exploiting Hadoop flaw to target Linux servers https://www.itpro.co.uk/botnets/32427/mirai-botmasters-now-exploiting-hadoop-flaw-to-target-linux-servers
[229] Due to Misconfigured Component: DemonBot Malware Infects Multiple Apache Hadoop Servers https://hackercombat.com/due-to-misconfigured-component-demonbot-malware-infects-multiple-apache-hadoop-servers/

- **Threat T4.4.3: Malicious code/software/activity:** Service spoofing (e.g., ARP spoofing) aims to masquerades an attacker identity to take a competitive advantage. Web application attacks and code injection attacks (see Section 3.7) are traditional examples of attacks that often represent the starting point for more sophisticated attacks. In Big Data, malware can infect nodes to send malicious commands to other servers, worms can distribute themselves sending copies to other nodes. Backdoors or hidden functionality can simplify accesses to components and devices [147]. A malicious code attack is also reported in [147] as faulty results of the Hadoop logging data system. It uses a malicious script to let Flume streaming previously modified log data into Hcatalog [147]. MapReduce computational framework has been the target of malicious software. Untrusted mappers can in fact alter results, whose malicious activities could be difficult to identify with large amount of data.[73] Ransomware[61] is still a critical attack that aims to target availability of data; recently, we are moving from financial motivations to nation states actions. Meltdown [148] and Spectre [149] are new information disclosure vulnerabilities in most modern microprocessors.[197] They break the isolation between user applications and operating system, and different applications, respectively, to the aim of retrieving sensitive data in the memory of other running programs,[230] including passwords, personal photos, emails, instant messages and even business-critical documents. In 2013, the Carbanak and Cobalt malware[61] was launched targeting financial institutions. The malware took control of the servers and ATMs, impersonating customers for money transfers, inflating account balances and controlling ATMs. This attack also links to threat T4.4.1 identity fraud and threat T4.3.1 data poisoning. The gang managing this malware got arrested in 2018.
- **Threat T4.4.4: Generation and use of rogue certificates:** This threat is usually at the basis of more complex attacks as discussed in the previous threats, in particular, T4.2.1, T4.3.2, T4.4.1, T4.4.2. For instance, an increase in phishing sites using HTTPS has been observed.[74] Attackers used free certificate services like Let's Encrypt or Comodo to break the common assumption that HTTPS web sites are secure and safe.
- **Threat T4.4.5: Misuse of assurance tools:** The complexity of current data storage and databases makes poisoning of assurance tools critical to cover unauthorised access to large amounts of personally identifiable data. No recent attacks have been reported.
- **Threat T4.4.6: Failures of business process:** User re-identification is an example of weak anonymization. While data collection and aggregation use anonymization techniques, individual users can be re-identified by leveraging other Big Data data sets, often available in the public domain [150]. This scenario is put to the extreme by Big Data variety that permits to infer identity from anonymized data sets by correlating with apparently innocuous public information.[231] [232] [233]

[230] Meltdown and Spectre Vulnerabilities in modern computers leak passwords and sensitive data https://meltdownattack.com/
[231] AOL search data leak https://en.wikipedia.org/wiki/AOL_search_data_leak
[232] See NIST Big Data Interoperability Framework: Volume 4, Security and Privacy. Use case: Web traffic analytics in retail and marketing.
[233] ENISA's report "Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics "

- **Threat T4.4.7: Code execution and injection (unsecure APIs):** Data breaches due to unsecure APIs have been reported in the past and often targeted social networks (e.g., Facebook, Yahoo and Snapchat).[234] SPARQL code injection is an example of attacks to Semantic Web technologies [151]. Security flaws are rather common in Big Data languages like SPARQL, RDQL and SPARUL, mimicking the one affecting traditional and still dangerous query languages, like SQL, LDAP and XPath injection [152].[235] Hive, MongoDB and CouchDB also suffer from traditional threats such as code execution and remote SQL injection.[236] [237] A big data breach was reported on India's national ID database, "Aadhaar," affecting more than 1.2 billion Indian citizens.[197] The breach was due to an unsecured API used to check a customer's status and verify their identity.[238] Apache Hadoop YARN NodeManager Daemon has been found to be vulnerable to Zip Slip vulnerability.[239] This attack permits to inject malicious code in the jobs of other cluster users. In 2018, Alibaba Cloud Security Team discovered the first Remote Code Execution (RCE) exploit in Spark Rest API.[240] This weakness allowed to instruct the server to download and execute a remote jar file from the Darknet. A vulnerability in Apache Spark permitted an unauthenticated, remote attacker to execute arbitrary code on the master host of a targeted system.[241] This vulnerability exploits improper security restrictions and insufficient validation of user-supplied input. A vulnerability in Apache Ambari permitted to implement persistent cross-site scripting thanks to insufficient sanitization of user-supplied data.[242] A weakness in the British Airways web and mobile app caused the exposition of personal and payment data.[243]
- **Threat T4.5.1: Violation of laws or regulations:** See Chapter 4.
- **Threat T4.6.1: Skill shortage:** Data analysis and management are among the most important activities in a Big Data environment. Data science skill and data

[234] Jaime Ryan (CA, Sr. Director) and Tyson Whitten (CA, Director of API Management) in "Takeaways from API Security Breaches" presentation and webinar (2015) reported breaches, due to unsecure APIs, for Yahoo, Snapchat and other companies, see http://transform.ca.com/API-security-breaches.html?source=AAblog

[235] In October 2015, presumably, an SQL injection was used to attack the servers of British telecommunications company Talk Talk's, endangering the personal details of up to four million customers. See https://www.mobilenewscwp.co.uk/News/article/talktalk-hacking-scandal-expert-reaction

[236] 50 For example Hive version 2.0 suffers from cross site scripting, code execution, and remote SQL injection vulnerabilities, see https://packetstormsecurity.com/files/132136/Hive-2.0-RC2-XSS-Code-Execution-SQL-Injection.html.

[237] MongoDB suffers injection attacks, see https://www.idontplaydarts.com/2011/02/mongodb-null-byte-injection-attacks/

[238] A new data leak hits Aadhaar, India's national ID database https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/

[239] Apache Hadoop spins cracking code injection vulnerability YARN https://www.theregister.co.uk/2018/11/23/apache_hadoop_yarn_zip_slip_vulnerability/

[240] Alibaba Cloud Security Team Discovers Apache Spark Rest API Remote Code Execution (RCE) Exploit https://www.alibabacloud.com/blog/alibaba-cloud-security-team-discovers-apache-spark-rest-api-remote-code-execution-rce-exploit_593865

[241] Announcement Regarding Non-Cisco Product Security Alerts https://tools.cisco.com/security/center/viewAlert.x?alertId=59176

[242] Cross-site scripting in Apache Ambari https://www.cybersecurity-help.cz/vdb/SB2019052711

[243] Customer data theft https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information

scientist shortage introduce unprecedented risks.[244] Lack of skill can in fact result in wrong decisions and adaptations with catastrophic consequences on the target system (see also threat T4.1.1). The inability to properly analyse large data sets can then result in substantial loss of money, reducing productivity and innovation growth.

- **Threat T4.6.2: Malicious insider:** In the data domain, the risks introduced by insider threats are quite clear and often result in data leakage. The goal is to increase the cyber attacker revenue or to decrease the reputation of the attack target. Very famous are the cases of Edward Snowden or Chelsea Manning (the work in [153] provides the description of the most famous insider threat cases). Case studies of insider threats have been analysed in different domains and from different angles [28]. For instance, Randazzo et al. [154]presented 23 case studies in the finance sector, while Kowalski et al. [155] 36 case studies in the government sector, involving fraud, IP theft, and sabotage of the IS/network, and combination thereof. Other works [156] [157]described case studies including system administrators, programmers, and network professionals. Keeney et al. [158] also presented different cases of Sabotage using IT in critical infrastructures. Additional work has been done in [159] [160] [161] [162] aimed to data exfiltration, IP theft, or sabotage in financial and military sectors. Unintentional insider threat was considered by [162] (phishing attacks) and [163] (unintentional denial of service).

A.5 Attacks related to Application-Centric Security

In the following, the main attacks affecting Application domain are reported. We note that the threat description is available in Section 3.3.7.

- **Threat T5.1.1: Security Misconfiguration:** In addition to attacks presented in Threat T4.1.1 in Section 3.6.3 focusing on data breach, default configurations are usually at the basis of security breaches. For instance, Amazon AWS S3 poorly configured access control policy allows an attacker to read and write data from a bucket.[245] Mirai IoT malware targets the devices that are usually managed by not-expert people and come with default configurations. Being such devices often available through the network using an application (GUI) with default credentials, they are the perfect target for malware like Mirai.[246] Other attacks like WannaCry, one of the most known cryptolockers, used the EternalBlue exploit, spreading the ransomware to every other unpatched computer on the network using a single vulnerable and internet-exposed system.[247] The slow patching process of companies made the cryptolocker effective even if Microsoft already released a patch. Other attacks target insecure default configurations, incomplete or ad hoc configurations, open

[244] August LinkedIn Workforce Report: Data Science Skills are in High Demand Across Industries https://news.linkedin.com/2018/8/linkedin-workforce-report-august-2018

[245] AWS S3 Bucket Discovery
Build your own tools with the secapps Fuzzer https://blog.websecurify.com/2017/10/aws-s3-bucket-discovery.html

[246] I Can't Believe Mirais: Tracking the Infamous IoT Malware
https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/

[247] Two years after WannaCry, a million computers remain at risk
https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=G-KKo6amjJ2OCukY1Fh6-A

cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information in operating systems, frameworks, libraries, and applications.[88] Vulnerable XML processors can be used to attack XML-based web services:[88] *"Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks."* In this context, well-known attacks are Billion Laughs Attack and SAML Security XML External Entity Attack.

- **Threat T5.2.1: Interception of information:** In addition to attacks presented in other domains, many attacks resulting in information interception have been reported. Advanced Persistent Malware is increasingly designed to steal SSL/TLS keys and certificates.[248] For instance, the Heartbleed Bug vulnerability of OpenSSL cryptographic software library permitted to steal sensitive information (digital keys and certificates) normally protected by SSL/TLS encryption. [249] Man-in-the-Middle (MITM) Attacks are traditional attacks where an attacker impersonates a trusted website accessing all communications. Again, steal of SSL/TLS keys and certificates facilitates such attack, and unsecured or lightly protected wireless access points are often exploited for entry. Self-signed and wildcard certificates, as well as unknown, untrusted, and forged certificate authorities are other sources of attacks.[248] [250] The first is at the basis of fake web sites for phishing attacks; the second results, as proven by NetCraft in 2014, fake digital certificates impersonating banks, ecommerce sites, ISPs and social networks deployed across the Internet.
- **Threat T5.2.2: Sensitive data exposure:** Attacks in this threat mainly resembles to attacks described in T5.1.1 and T5.1.2 in this section, and T4.1.1, T4.2.1, T4.2.2, T4.4.4 in Section 3.6.3. Attacks such as the ones to ApplePay,[251] ATM,[252] banks,[253] are facilitated by cleartext, that is, either password stored in clear or cleartext communications.
- **Threat T5.3.1: Broken authentication and access control:** Automated brute force, dictionary, and session management attacks are spread. Several Member States have reported the exploitation of Remote Desktop Protocols (RDPs) for malware infection. Cyber attackers scan specific open ports and then attempt to brute force access to the victims RDP.61 254 For instance, in 2017, up to 90 email accounts of UK Parliament were compromised thanks to a brute force attack and weak passwords.255 Weak and default password are at the basis of many botnets, such as Mirai IoT malware, which compromised devices by

[248] Common SSL Attacks https://www.venafi.com/education-center/ssl/common-ssl-attacks
[249] The Hearthbleed Bug http://heartbleed.com/
[250] Why SSL/TLS attacks are on the rise https://www.csoonline.com/article/3212965/why-ssl-tls-attacks-are-on-the-rise.html
[251] Wallet-snatch hack: ApplePay 'vulnerable to attack', claim researchers https://www.theregister.co.uk/2017/07/28/applepay_vuln/
[252] ATM logic attacks: scenarios, 2018 https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/
[253] How hackers rob banks https://www.ptsecurity.com/ww-en/analytics/banks-attacks-2018/
[254] Panda Security, PandaLabs Annual Report 2017, 2017.
[255] 'Brute force' cyber attack on Parliament compromised up to 90 email accounts https://www.telegraph.co.uk/news/2017/06/25/brute-force-cyber-attack-parliament-compromised-90-email-accounts/

guessing weak passwords to access the management application (GUI) [164].[246]

- **Threat T5.3.2: Denial of service:** On one side, malware often targets components and services that result in an application DoS. For instance, Mirai malware targeted the availability of DNS to bring well-known applications down (e.g., Twitter, the Guardian, Netflix, Reddit, CNN).[246] On the other side, as already discussed in Threat T2.3.5 in Section 3.4.3 and T5.2.1 in this section, expired certificates can result in system outages or open a door to attacks, such as, in 2013, where Microsoft Azure experienced a worldwide outage or, in 2014, tens of thousands of payment terminals in U.S. made unavailable.
- **Threat T5.3.3: Code execution and injection (unsecure APIs):** Malware attacks have been extensively discussed in previous sections. As a summary, ransomware (e.g., WannaCry and NotPetya) attacks moved the malware attack to another level, difficult to challenge by national law enforcement agencies alone.[61] In addition, cyber attackers are turning security defences in weapons. SSL/TLS has been used to deliver malware undetected, to disrupt secured transactions, and to exfiltrate data over encrypted communication channels.[248] For example, Zeus botnet used SSL communication to upgrade the attack after the initial email infection. After the Boston Marathon bombing, a malware distributed through a spam message used SSL to report back to its command and control server.[248] Finally, mobile malware, specifically targeting mobile operating systems and mobile applications, is growing significantly since 2017, in particular mobile ransomware. [256] [257] Some reports indicate that this malware is active in Africa, Asia and USA, with the exception of mobile ransomware which heavily targets North America.[61] [257] More in detail, Ransomware, spyware, bots, Adware, Potentially Unwanted Applications (PUA), Trojans, and Trojan spyware are exponentially targeting smartphones and IoT devices [57], over which modern applications are installed. PUA is the topmost Android malware detected by Quick Heal, [258] where third-party application stores are used to spread malware and exfiltrate private information of the user. Gugi is an example of a banking Trojan exploiting the security policies of Android Marshmallow [57]. GooglePlay has dozen of malicious apps [57]; for instance, Judy, which affected around 36.5 million Android users,[259] was in about 40 applications. According to [57], runtime information gathering (RIG) [165], energy-based [166], remote code execution/injection,[260] [261] [167] hijacking,[262] privilege escalation attacks [168] [169] are the most critical targeting Android devices. They are most based on

[256] TrendLabs, 2017 Annual Security Roundup: the paradox of cyber threats, 2018.
[257] Symantec, 'Facts and figures', Internet Security Threat Report (ISTR), 2018
[258] Annual threat report. 2017. Quick Heal. https://www.seqrite.com/blog/quick-heal-annual-threat-report-2017-excerpts/
[259] Jason Murdock. Judy' could be the largest malware campaign ever found on google play. 2017. International Business Times. http://www.ibtimes.co.uk/judy-could-be-largest-malware-campaign-everfound-google-play-store-1623508
[260] Android Developers Blog. Android security bulletin, October. 2017. https://source.android.com/security/bulletin/2017-10-01
[261] Google ASI. Vungle support, security vulnerability in Android sdks prior to 3.3.0. 2016. https://support.google.com/faqs/answer/6313713
[262] Mohit Kumar. 2014. The hacker news. Facebook sdk vulnerability puts millions of smartphone users' accounts at risk. https://thehackernews.com/2014/07/facebook-sdk-vulnerability-puts.html

vulnerabilities in (third-party) libraries and over-permissioned applications, libraries, and ad libraries (more details can be found in Section 3.3) [57].

- **Threat T5.3.4: Insufficient logging and monitoring:** This class of threats is usually a pre-requisite for any large attack and major incident. It virtually exploits insufficient logging and monitoring to go undetected for a while, reducing timely response (191 days on average in 2016).[88]
- **Threat T5.3.5: Untrusted composition:** Attacks related to this threat mainly target single services/applications, trying to identify the weakest link in the composition. They then resemble to attacks described in this section. No recent attacks on the composition flow and orchestrators have been reported, while different assurance solutions (e.g., [27]) have been reported to verify (e.g., certify) the strength of a service composition by verifying the strength of the single component services.
- **Threat T5.4.1: Violation of laws or regulations:** See Chapter 4.
- **Threat T5.5.1: Malicious insider:** See Threat T4.6.2 in Appendix A.4.

A.6 Attacks related to User-Centric Security

In the following, the main attacks affecting User domain are reported. We note that the threat description is available in Section 3.3.8.

- **Threat T6.1.1: Mishandling of physical assets:** The problem of mishandling of physical assets is particularly evident with the case of stolen laptops. Laptops are systematically stolen from cars, offices, and public places, as witnessed by cybersecurity surveys like the Verizon DBIR or other studies [170]. More worrisome is the fact that there already is a history of severe data breaches caused by stolen laptops [171], and affecting critical and sensitive data.[263]
- **Threat T6.1.2: Misconfiguration of systems:** Attacks due to system misconfiguration have a long history. Incidents happened for misconfigurations of BGP [172] [173], DNS [174], firewalls [175], web applications [176], up to recent AWS S3 buckets [177], and many other systems. Beside the System and Application domains, the User domain is also involved because misconfigurations have often to do with situations leading users to make errors. This scenario should be accounted for and explicitly managed.
- **Threat T6.1.3: Loss of CIA on data assets:** This is a vast threat category, spanning over multiple domains and comprising almost countless attacks. Attacks on CIA regarding the User domain could be found in those cases where the human factor is key for the attack to succeed. For example, cases where a user has misused his/her access privileges [178], the case of fraudulent or mismanaged Certification Authority [179], or employees falling prey of impersonation attacks [180] or frauds, such as cases of so called CEO frauds, where CEOs (or other C-level managers) are either victims[264] or perpetrators of frauds [181].

[263] Jessica Davis, Data of 43,000 patients breached after theft of unencrypted laptop. Healthcare IT News, January 2018. https://www.healthcareitnews.com/news/data-43000-patients-breached-after-theft-unencrypted-laptop

[264] Jill McCabe, FBI Warns of Dramatic Increase in Business E-Mail Scams. FBI Phoenix, April 2016. https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams

- **Threat T6.1.4: Legal, reputational, and financial cost:** There are few examples of firms that were fined for a cybersecurity incident. For instance, in 2007, Heartland Payment Systems payed $150 million in fines and legal costs for a breach in which more than 100 million credit and debit card numbers were lost [182][265]. However, for the EU, things seem to have changed after the GDPR, which may impose severe fines, and organizations took notice [183] [184]. Cybersecurity incidents causing financial and reputational costs have been analysed, especially by scholars and analysts interested in the economics of cybersecurity [185] [186].
- **Threat T6.2.1: Profiling and discriminatory practices:** In 2012, the FTC published a document titled "Protecting Consumer Privacy in an Era of Rapid Change" [266] addressing the data broker sector and specifically those not regulated by the FCRA. Data brokers were categorized in those having an activity: (*i*) subject to the FCRA; (*ii*) not subject to FCRA and collecting data for marketing purpose; (*iii*) not subject to FCRA and collecting data for purposes other than marketing, for instance to detect frauds or locate people. Then, in 2014, a new report titled "Data Brokers - A Call for Transparency and Accountability" was published [267]. To date, it represents one of the most comprehensive analysis of the data broker industry. The characteristics of nine data brokers are described. Their names are unknown for almost everybody (i.e., Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, and Recorded Future), but their activity has involved nearly every US consumer and many others internationally. These companies manage consumers' data - usually bought from other data brokers or from companies directly collecting them from individuals – and produce derived data for satisfying their clients business needs in terms of marketing, risk mitigation, and people search. Citizens are normally unaware and never specifically informed of their personal data being used for these purposes. Data may include bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other from everyday online and offline activity. Data sources are heterogeneous; from publicly available blogs and social media to commercial sources, for example about the purchasing history of customers or online service registrations. Data updates are commanded by data brokers according to their cost-benefit assessment: The more frequent the update, the higher the classification accuracy and costs. For this reason, some personal data might be inaccurate even for a long time, without the individual able to know about that and about possible consequences of misalignment. Typically, data brokers compile commercial categories and group customers with similar behaviors. Such categories may look fancy to those not accustomed with advertising practices. Example of

[265] Danny Yadron, "Companies Wrestle With the Cost of Cybersecurity," Wall Street Journal, https://www.wsj.com/articles/no-headline-available-1393371844

[266] US Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. March 2012. https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

[267] US Federal Trade Commission, Data Brokers - A Call for Transparency and Accountability, Washington, DC: US Federal Trade Commission, May 2014, available at: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

categories could be: Soccer Moms, Urban Scramble, Rural Everlastings or Thrifty Elders. Bizarre as they may sound, categories like these are useful for targeting *quality buyers*, as profiled citizens are dubbed by a very active online advertising company[268]. Another data broker activity is to develop models to predict behaviors. In this case, a subset of customers is specifically analysed for its purchase behavior and that knowledge is applied to predict future purchases of other customers with similar characteristics. This may also involve sensitive information like those related to health, pregnancy and medicine consumption. In particular, privacy abuses of health data have been the subject of several journalistic investigations[269][270] and scientific research [187] [188], which unveiled some commercial practices that most citizens completely ignore but strongly oppose when informed. For instance, the severity of medical privacy invasion came shockingly to light in 2013 with the Congressional testimony of Pam Dixon of World Privacy Forum[271]. In that occasion, Dixon presented evidences that lists of patients suffering from mental illness to sexual dysfunctions, cancer and HIV/AIDS to name just a few examples were commonly traded. Even more outrageously, lists of rape victims were publicly advertised and sold. Opting out of data broker profiling is often impractical, at least. Since data broker typically do not interact directly with consumers, even those offering clear opt-out procedures are unlikely to be known by consumers willing to exercise their choice. Many data broker instead provide murky opt-out procedures or simply do not care of providing any. In Dixon Congressional testimony, it was mentioned that in a sample of 352 data broker, just 128 provided an opt-out procedure. In some cases, for example when consumers are profiled to calculate a credit score, it is practically impossible to be deleted from a score list. In other situations, the opt-out choice is made difficult to exercise due to clauses such as the request of a motivation to be approved or of a fee. Therefore, opting-out of data broker profiling, when permitted, is likely to be incomplete, does not imply deletion of personal data and does not involve third parties, it may be costly, hard to find and there is no guarantee that it is not just temporary.

- **Threat T6.2.2: Illegal acquisition of information:** Data has always been the target of attacks[272]. Now they are often reported at great length by the press and might represent a major incident for a company, Cambridge Analytica[273] and Equifax [189] are just two of the most noticeable examples. With respect to the User domain, the illegal acquisition of information may have unforeseen

[268] Rubicon Project. The Advertising Automation Cloud, 2016, available at: https://rubiconproject.com/

[269] L. Beckett. Everything We Know About What Data Brokers Know About You, *Pro Publica*, 2014, available at: https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you

[270] A. Tanner. How Data Brokers Make Money Off Your Medical Records, *Scientific American*, 2016, available at: http://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/

[271] P. Dixon. Congressional Testimony: What Information Do Data Brokers Have on Consumers?, *World Privacy Forum*, 2013, available at: https://www.worldprivacyforum.org/2013/12/testimony-what-information-do-data-brokers-have-on-consumers/

[272] Juliana De Groot, The History of Data Breaches. Digital Guardian's Blog, October 2019. https://digitalguardian.com/blog/history-data-breaches

[273] Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, *17*, 22.

consequences on a company's operations. From damaging the brand reputation to costs for litigations and liabilities, the loss of trustworthiness, scapegoating and career damages, and so forth. A data breach is not only a threat for data and data owners, but it might trigger a cascade of consequences on the organization's processes and personnel.

- **Threat T6.3.1: Organized criminal groups' activity:** Attacks perpetrated by organized criminals are almost countless. From petty crimes to large frauds. Europol publishes one of the leading reports providing with plenty of information[61]. In the current issue, one of the key messages is that still criminals mostly target data. Europol, too, insists on the need to counteract criminal groups by considering the big picture and adopting a holistic approach consisting in analysing single vulnerabilities but also the system perspective, technologies and organizational processes, tools and people.
- **Threat T6.3.2: State-sponsored organizations' activity:** Political, geostrategic, and business tensions arose in recent years among several countries worldwide leading to a wave of state-sponsored attacks. It has become common to talk about state-sponsored organizations engaged in hostile activities against organizations in other countries. *Stuxnet*, often dubiously dubbed as "the first act of cyberwar", was one of the first episodes of clear state-sponsored attack [190]. After that episode, state-sponsored attacks seem to have escalated, becoming common and motivated by vary different reasons [42] [191] [192] [193].
- **Threat T6.3.3: Malicious employees or partners' activity:** As we reminded, it is way too easy to overhype the dangers posed by disloyal insiders and oversell stereotypes like the "disgruntled employee" or the "treacherous sysadmin". On the other side, it is true that cases of cybercrimes made by employees are countless. For example, the US Department of Homeland Security has published a long list of references to insider threats analyses, showing the many ways an employee may become the responsible of a cybercrime [194].[274]
- **Threat T6.4.1: Misinformation/disinformation campaigns:** A misinformation or disinformation campaign (the difference laying in the intentionality of the campaign) targeting a company might inflict not negligible damages on brand reputation and trustfulness, which would require public relation efforts to be mitigated. Evidences of this are still murky and opinionated, but at least we can observe that the problem is growing and has already put pressure on some companies.[275] [276] With regard to software tools developed to assists in misinformation campaigns [195], the massive surge of social bots (i.e., software bots employed in social media and mimicking legitimate journalists or just common social media users) is one of the most relevant phenomena and has attracted a great deal of interest and analyses [196] [197]. According to some estimates, on Twitter, social bots represent

[274] Department of Homeland Security, Insider Threat - Cyber. DHS National Cybersecurity and Communications Integration Center, 2019. https://www.dhs.gov/cisa/insider-threat-cyber

[275] Mike Isaac, Facebook Finds New Disinformation Campaigns and Braces for 2020 Torrent. The New York Times, October 21, 2019. https://www.nytimes.com/2019/10/21/technology/facebook-disinformation-russia-iran.html

[276] Shelly Banjo, Facebook, Twitter and the Digital Disinformation Mess. The Washington Post, October 2, 2019. https://www.washingtonpost.com/business/facebook-twitter-and-the-digital-disinformation-mess/2019/10/01/53334c08-e4b4-11e9-b0a6-3d03721b85ef_story.html

between 5 to 15% of users and are responsible for misinformation campaigns, phishing attacks, election and market manipulation[277] and, in most cases, are organized in social bot networks centrally coordinated, an approach that closely mirrors the command&control scheme of botnets exploited for electronic crime [198, 199]. Many research efforts are ongoing with the goal of detecting social bots from legitimate human users, with the subject of social bot detection as one of the most active in the area of social media security [200] [201] [202] [203].

- **Threat T6.4.2: Smear campaigns/market manipulation:** This is still more a theoretical case than a real threat, but nevertheless the growing influence of online media and social networks provide the means for new forms of classical pump-and-dump schemes. Example of politically motivated smear campaign abound [204]. The shift to a business threat is certainly possible in the future [205]. With respect to software tool employed in smear campaigns and market manipulation operations, we forward to the previous discussion regarding social bots, because they represent a general family of software tools and coordination mechanisms largely employed in malicious activity on social media.
- **Threat T6.4.3: Social responsibility/ethics-related incidents:** IT companies accused of unethical behavior [206] and that have suffered for the consequences of having behaved (or the perception of) unethical are not rare in history [207]. Interestingly, cases of modern Internet-based, technology intensive companies that are reported to engage in unethical behavior seem rampant. Sometimes, the bad reputation gained has triggered boycotts by customers. Uber, for example, has been recently often accused of unethical activities and its reputation has clearly suffered for that [208]. The sharing economy as a whole has been studied as possibly facilitating unethical activities [209].
- **Threat T6.5.1: Skill shortage/undefined cybersecurity curricula:** No recent attacks have been reported.
- **Threat T6.5.2: Business misalignment/shift of priorities:** Many companies still struggle with deciding the right position in the organigram of the responsible of cybersecurity, being either the CSO (Chief Security Officer) or the CISO (Chief Information Security Officer), or even the more recent CRO (Chief Risk Officer)[278] [279]. The organizational weakness of the cybersecurity function in many companies is also one of the reasons for the common shift of priority of cybersecurity, that sees drastic budget reduction as soon as the company is in need of review budgets [210].

[277] Cloudflare Inc. What is a Social Media Bot?, Cloudflare, 2020., available at: https://www.cloudflare.com/learning/bots/what-is-a-social-media-bot/
[278] Westby JR. Governance of enterprise security: CyLab 2012 report. Pittsburgh, PA. 2012. http://www.fbiic.gov/public/2010/jul/cylab-governance-2010.pdf
[279] Data Security Council of India. "Developing a Framework to Improve Critical Infrastructure Cybersecurity." https://www.nist.gov/document/040813dscipdf