D2.2 Analysis NIS directive Cross domain threats and proof of concepts

Work Package	2
Task	T2.2 Cross-domain threat analysis
Authors	Kostas Maliatsos, Costas Lambrinoudakis, Andreas Menegatos, Christos Lyvas, Athanasios Kanatas, Christos Kalloniatis (UPRC), Rosella Omana Mancilla (ENG), Pietro De Vito (STAM), Alkiviadis Giannakoulias (ED)
Dissemination Level	PU
Status	Final
Due Date	31/07/2021(initial) 31/05/2022 (review changes)
Document Date	31/07/2021 (initial) 31/05/2022 (review changes)
Version Number	1.0

Quality Control

	Name	Organisation	Date
Editor	Kostas Maliatsos	UPRC	26/07/2021 (initial) 31/05/2022 (review changes)
Peer review 1	Daniele Marenco	AMT	29/07/2021
Peer review 2	Luca Bianconi	SIGLA	29/07/2021
Authorised by	Jason Sioutis	ICCS	28/07/2021 (initial) 30/05/2022 (review changes)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

(Technical Coordinator)			
Authorised by (Quality Manager)	Panagiotis Lytrivis	ICCS	28/07/2021 (initial) 30/05/2022 (review changes)
Submitted by (Project Coordinator)	Angelos Amditis	ICCS	31/07/2021 (initial) 31/05/2022 (review changes)

Contributors

Name	Organisation	Date
Kostas Maliatsos	UPRC	26/06/2021
Andreas Menegatos	UPRC	26/06/2021
Christos Lyvas	UPRC	01/07/2021
Rosella Omana Mancilla	ENG	06/07/2021
Pietro De Vito	STAM	16/07/2021
Costas Lambrinoudakis	UPRC	21/07/2021
Andreas Menegatos	UPRC	23/07/2021
Alkiviadis Giannakoulias	ED	26/07/2021
Kostas Maliatsos	UPRC	26/07/2021
Kostas Maliatsos	UPRC	28/05/2022

Document Revision History

Version	Date	Modification	Partner
Table of Contents released	04/06/2021	Creation	UPRC
First Draft	16/06/2021	Creation	UPRC
First Draft released	26/06/2021	New content added	UPRC
Second draft released	16/07/2021	New content from ENG and STAM added	ENG, STAM, UPRC
Third draft released	23/07/2021	Integration of all contributions, editing, and additional content	UPRC
Fourth draft released	26/07/2021	New content from ED and review	ED, UPRC
Quality Control review	28/07/2021	Final quality control	ICCS

Final version	31/07/2021	Resolution of issues and reviewer comments	UPRC
2nd round of quality control	22/05/2022	Suggestions and comments from project interim review	URPC, ICCS
Revised version	28/05/2022	Integration of minor corrections due to project officer and reviewer comments	UPRC
Final quality and technical quality control	30/05/2022	Final Quality Control	ICCS

Legal Disclaimer

CitySCAPE is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No. 883321. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The CitySCAPE Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

Abbreviation	Meaning
CCP	Central Clearing Counterparty
DoS	Denial of Service
DNS	Domain Name Server
DSP	Digital Service Providers
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
HW	Hardware
I/O	Input-Output
ITS	Intelligent Transportation System
IXP	Internet Exchange Point
LNG	Liquefied natural gas
NIS	The EU Network and Information Security directive
OES	Operator of Essential Services
TLD	Top Level Domain
SW	Software

VTS	Vessel Traffic Services

Executive Summary

The initial objectives of the work carried out during Task 2.2 “Cross-domain threat analysis” include a detailed investigation of the current threat landscape against the major Operators of Essential Services (OES) and the Digital Service Providers (DSP) as defined by the EU Network and Information Security (NIS) directive. More specifically, six domains operating critical infrastructure of extreme importance for the prosperity of EU citizens have been identified:

- Energy,
- Transportation,
- Health,
- Finance,
- Banking,
- Water Supply/Facilities.

CitySCAPE targets the Transportation domain offering enhanced security functionalities for the modern, urban, multimodal public transportation ecosystem. Nevertheless, the integration of digital services for the administration, control, management and operation of the critical infrastructure has created a common field of risks and threats related to cybersecurity incidents and attacks. Moreover, all domains are interconnected and interdependent with each other and, if no security measures are applied, are vulnerable to cascading risks and threats.

This deliverable includes threat analysis on the aforementioned NIS directive domains, including also DSPs that are offering cross-domain support over all essential services. This analysis, makes clear that a large set of common generic threats for the OESs/DSPs in different domains is identified.

Additionally, the deliverable describes a methodology and criteria to be applied for the identification of OES and DSPs as well as the identification of serious incidents. Thus, in order to facilitate the estimation of the criticality of potential incidents, a detailed set of evaluation criteria is proposed. For each criterion, estimates on threshold values/metrics are also provided.

1 INTRODUCTION

1.1 Project Introduction

The traditional security controls and security assurance arguments are becoming increasingly inefficient in supporting the emerging needs and applications of the interconnecting transport systems, allowing threats and security incidents to disturb all dimensions of transportation. CitySCAPE is a project funded by the EU's Horizon 2020 research and innovation program, which consists of 15 partners from 6 European countries, united in their vision to cover the cybersecurity needs of multimodal transportation. More specifically, the CitySCAPE software toolkit will:

- Detect suspicious traffic-data values and identify persistent threats.
- Evaluate an attack's impact in both technical and financial terms.
- Combine external knowledge and internally observed activities to enhance the predictability of zero-day attacks.
- Instantiate a networked overlay to circulate informative notifications to CERT/CSIRT authorities and support their interplay.

The project duration extends from September 2020 to August 2023.

WP2 unfolds activities related to the use-cases, risk analysis and threats in the multimodal transport domain. Initial use-cases will be further detailed and updated, while an exhaustive threat analysis taking into high consideration GDPR will be developed. WP2 outcomes will set the basis for the articulation of the two CitySCAPE pilots planned, as well as a major contributor to the development objectives of the CitySCAPE toolkit.

1.2 Deliverable Purpose

The purpose of this document is to present the current threat landscape against all domains of the NIS directive major OESs and DSPs and define a methodology for criticality/impact estimation of potential incidents.

The document is provided in M11 of the project so that the main objectives of Task 2.2 (Cross-domain threat analysis) and its final deliverable that contains the complete risk analysis for the CitySCAPE reference use cases can be executed. Furthermore, it aims to facilitate the efforts in user/system requirements elicitation of WP3 (User/system requirements & architecture) and the initial development tasks of WP5 (CitySCAPE security layer implementation).

1.3 Intended Audience

Besides the internal project reviewers, the project reviewers and the project partners, this deliverable is addressed to any interested reader (i.e., public dissemination level). This deliverable is intended for reading by all transport and cybersecurity experts in the field, especially those in the public sector - nevertheless, due to the fact that the documents include analysis of threats and impact classifications for all NIS directive OES/DSP domains, the document is expected to be a reference for related work across all types of critical infrastructures.

The deliverables outcomes have direct relevance to the following CitySCAPE tasks:

Table 1: Tasks related to the deliverable

Task	Relationship
T2.2 Cross-domain threat analysis	The deliverable treats the initial objectives of T2.2 and act as a reference for the main risk and threat analysis tasks that will be documented by the following task deliverable (D2.3).
T2.3 Mechanisms of cascading threats (across multimodal ecosystem)	The deliverable provides a reference list of generic threats for the initiation of the cascading threat analysis, as well as facilitates the investigations of interconnections of multi-domain threats.
T3.2 System requirements elicitation	The deliverable provides a reference list of generic threats, as well as their association with basic types of system assets that may be affected/attacked. This information will assist the efforts for system requirement elicitation and system architecture definition.
T3.3 Secure multi-modal transport architectures	
T5.5 Risk analysis and impact assessment engine	The deliverable sets the basis for the risk analysis that is implemented in T5.5 and the common threat basis that can cause multi-domain cascading effects.
T5.6 Financial impact assessment engine	

	Additionally, both tasks 5.5 and 5.6 are assisted by the impact/criticality assessment methodology.

1.4 Outline of the Document

The document is structured as follows:

- Chapter 2:
  - A description of the NIS directive, the Operators of Essential Services and Digital Service Providers is defined, as well as a methodology for the definition and identification of an OES is provided.
- Chapter 3:
  - The current threat landscape for the OESs and the DSPs is documented. More specifically, the analysis covers the following domains:
    - Energy sector,
    - Transportation sector,
    - Health sector,
    - Finance sector,
    - Banking sector,
    - Water utilities,
    - Digital Service Providers (in general),
- Chapter 4:
  - A methodology for the impact and criticality of an incident per OES for all identified domains is presented, as well as determination of the severity of incidents of DSPs is provided.
- Chapter 5:
  - The derived conclusions are presented.

2 NIS AND OPERATORS OF ESSENTIAL SERVICES AND DIGITAL SERVICE PROVIDERS

2.1 The NIS Directive's purpose and scope

Directive 2016/1148 on the security of network and information systems (the NIS Directive)[1] is the first horizontal legislation undertaken at the European Union (EU) level for the protection of network and information systems across the Union. This legislative tool aims to address the constantly increasing threats and deliberate actions that intend to cause disruption to IT services and critical infrastructures. Therefore, the security of network and security systems is a high priority across the EU and as such, it needs to be addressed in a common way by all Member States. This need is evident in the Directive's text where in its first article it is stated that: "*The Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market*".

The NIS Directive was published in July 2016; however, the EU has been addressing cyber security issues in a comprehensive manner since 2004, when ENISA (European Union Agency for Network and Information Security), a new specialised EU agency, was founded. The NIS Directive itself has its roots in the Commission's Communication of 2009, which focuses on prevention and awareness and defines a plan of immediate action to strengthen the security and trust in the information society. This was followed, in 2013, by a joint Communication released by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy on the Cybersecurity Strategy of the European Union. From 2013 to 2015, the Commission, the Council and the Parliament discussed the draft put forward by the Commission intensely and these discussions resulted in the NIS Directive. It finally entered into force in August 2016. The deadline for national transposition by the EU Member States was the 9th of May 2018.

2.2 Basic definitions

Some of the main definitions included in the NIS Directive's text, as of relevance to the CITYSCAPE project, may be seen below:

- **network and information system** mean:
  (a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC (transmission systems and, where applicable, switching or routing equipment and other

[1] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

(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.

- **security of network and information systems** means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;
- **digital service** means service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services). For the purposes of this definition:
  (i) "**at a distance**" means that the service is provided without the parties being simultaneously present;

  (ii**) "by electronic means**" means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

  (iii) "**at the individual request of a recipient of services**" means that the service is provided through the transmission of data on individual request.
- **digital service provider** means any legal person that provides a digital service.
- **operator of essential services** means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2), that is:
  (a) an entity that 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.

- **incident** means any event having an actual adverse effect on the security of NIS.

2.3 The NIS Directive's application to operators of essential services and digital service providers

2.3.1 General

The NIS Directive applies to both operators of essential services and digital services providers. Their definitions are included in articles 4 and 5 of the Directive but should be examined in combination with the Directive's annexes, as well as Directive EU 2015/1535[2]. It should be mentioned that undertakings providing public communication networks or publicly available communications services[3] and trust services providers[4] are excluded from the scope of the NIS Directive.

2.3.2 Operators of essential services

It has to be noted that this analysis focuses more on the digital services providers rather than on the operators of essential services since the CITYSCAPE project focuses on the protection of the digital infrastructures from various types of cyberattacks. **The term operator of essential services** includes a public or private entity that activates in specific sectors such as the sector of energy, health, transport and any other sector of the ones listed of a type referred to in Annex II of the NIS Directive.

Article 5 of the NIS Directive specifies the criteria for the identification of the operators of essential services. For an entity to be characterised as "operator of essential services", the following criteria should be met:

(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

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535

[3] Framework Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services

[4] Regulation 910/2014 on electronic identification and trust services for electronic transactions in the Internal market and repealing Directive 1999/93/EC

(c) an incident would have significant disruptive effects on the provision of that service. The definition of “significant disruptive effect” is given under Article 6 of the Directive.

Article 5 states that all Member States shall, by 9 November 2018, for each sector and subsector referred to in the Annex, identify the operators of essential services with an establishment on their territory. Such a list will be updated by the Member States at least every two years after 9 May 2018.

Consequently, not all operators of essential services fall within the scope of the NIS Directive. Member States are tasked with the process of their categorisation and identification in order to determine which individual companies meet the criteria of the definition of operators of essential services.

2.3.3 Digital Service Providers

a. Definition of digital service providers

The NIS Directive also applies to digital services providers. The reason behind the decision of their inclusion in the Directive’s scope is given in Recital 48 of the NIS Directive, which reads as follows: “*Many businesses in the Union rely on digital service providers for the provision of their services. As some digital services could be an important resource for their users, including operators of essential services, and as such users might not always have alternatives available, this Directive should also apply to providers of such services*”.

The definition of a digital service provider is given under Article 4(6) and includes any legal person that provides a digital service. Digital service means service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535, which is of a type listed in Annex III of the NIS Directive, namely **online marketplace**, **online search engine** and **cloud computing service**. These three types of services were chosen to be regulated due to the increasing number of businesses that fundamentally rely on them for the provision of their own services.

b. Definition of an online marketplace

The NIS Directive defines **“online marketplace”** as a digital service that allows consumers and/or traders (as respectively defined in points (a) and (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council[5] to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace.

[5] on attacks against information systems and replacing Council framework Decision 2005/222/JHA

According to points (a) and (b) of Article 4(1) of Directive 2013/11/EU,

(a) "**Consumer**" means any natural person who is acting for purposes which are outside his trade, business, craft or profession;

(b) "**Trader"** means any natural persons, or any legal person irrespective of whether privately or publicly owned, who is acting, including through any person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession;

Recital 15 of the NIS Directive gives **an additional definition for an online marketplace** which could prove very useful when defining the boundaries of the Directive's implementation. "*An online marketplace allows consumers and traders to conclude online sales or service contracts with traders and is the final destination for the conclusion of those contracts. It should not cover online services that serve only as an intermediary to third-party services through which a contract can ultimately be concluded. It should therefore not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product*". **Application stores, which operate as online stores enabling the digital distribution of applications or software programs from third parties, are to be understood as being a type of online marketplace.**

Finally, ENISA has contributed to further clarifying what a marketplace is by stating in its guidelines released in February 2017[6] that "*There are no special provisions as to what can be sold through online market places, so it applies to all types of contracts (products and services). Although from a technical perspective most online marketplaces use an Incident notification for DSPs in the context of the NIS Directive website or web related technologies for delivering their services, it should not be a restriction in this sense, as mobile application stores make use of other technologies also*".

2.4 Security and notification requirements for Digital Service Providers

2.4.1 How are digital service providers treated in the context of the NIS Directive

The NIS Directive provides a lighter regime for digital service providers compared to operators of essential services. The softer approach towards digital service providers is mainly based on the different nature of the infrastructures they use as well as of the services they provide. In this

[6] https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

context, recital 57 of the Directive states that "*Given the fundamental differences between operators of essential services, in particular their direct link with physical infrastructure, and digital service providers, in particular their cross-border nature, this Directive should take a differentiated approach with respect to the level of harmonisation in relation to those two groups of entities. For operators of essential services, Member States should be able to identify the relevant operators and impose stricter requirements than those laid down in this Directive. Member States should not identify digital service providers, as this Directive should apply to all digital service providers within its scope*". In addition, recital 49 of the NIS Directive mentions that " [...] *the security requirements for digital service providers should be lighter. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems*".

2.4.2 Security requirements for digital service providers under article 16 of the NIS Directive

The NIS Directive describes, in its article 16, the security measures that digital service providers should take to mitigate the risks that threaten the security of the network and information systems they use for the provision of their service. The same article regulates the incident notification process digital service providers should follow to comply with the provisions of the Directive.

Article 16 (1) lists the elements that need to be taken into account by the Member States when they consider what measures they should adopt in order to manage the risks posed to the security of their network and information systems. These are:

a. The security of the systems and facilities;

b. Incident handling;

c. Business continuity management;

d. Monitoring, auditing and testing;

e. Compliance with international standards.

It is noted that the Commission, by virtue of article 16(8) of the NIS Directive,[7] issued an Implementing Regulation[8] that specifies further these elements,

[7] The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in article 22(2) by 9 August 2017.

[8] Commission Implementing Regulation (EU) 2018/151, of 30 January 2018, laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

as well as the parameters to be taken into account in order to determine whether an incident has a substantial impact on the provision of those services.

According to the Implementing Regulation, the elements of article 16 (1) are further described as follows:

a) Security of systems and facilities shall include the following elements:

- the systematic management of network and information systems, which means mapping of information systems and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, security of operations, security architecture, secure data and system life cycle management and where applicable, encryption and its management;
- physical and environmental security, which means the availability of a set of measures to protect the security of digital service providers' network and information systems from damage using an all-hazards risk-based approach, addressing, for instance, system failure, human error, malicious action or natural phenomena;
- the security of supplies, which means the establishment and maintenance of appropriate policies in order to ensure the accessibility and, where applicable, the traceability of critical supplies used in the provision of the services;
- the access controls to network and information systems, which means the availability of a set of measures to ensure that the physical and logical access to network and information systems, including administrative security of network and information systems, is authorized and restricted based on business and security requirements.

b) Incident handling: measures to be taken by the digital service provider

- detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events;
- processes and policies on reporting information security incidents and identified weaknesses and vulnerabilities in their information systems;
- a response in accordance with documented procedures and reporting the results of the measure taken;
- an assessment of the incident's severity, documenting knowledge from incident analysis and collection of relevant information which may serve as evidence and support a continuous improvement process.

c) Business continuity management shall include:

- the establishment and the use of contingency plans based on a business impact analysis for ensuring the continuity of the services provided by digital service providers, which shall be assessed and tested on a regular basis for example, through exercises;
- disaster recovery capabilities shall be assessed and tested on a regular basis, for example, through exercises.

d) The monitoring, auditing, and testing shall include the establishment and maintenance of policies on:

- the conducting of a planned sequence of observations or measurements to assess whether network and information systems are operating as intended;
- inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met;
- a process intended to reveal flaws in the security mechanisms of a network and information system that protect data and maintain functionality as intended. Such a process shall include technical processes and personnel involved in the operation flow.

e) Compliance with i**nternational standards** means standards that are adopted by an international standardization body as referred to in point (a) of Article 2(1) of Regulation (EU) No 1025/2012. Pursuant to Article 19 of Directive (EU) 2016/1148, European or internationally accepted standards and specifications relevant to the security of network and information systems, including existing national standards, may also be used.

2.4.3 Notification requirements for digital service providers under Article 16 of the NIS Directive

a) General

Except for the security requirements mentioned above, in order for a digital service provider to safeguard the security of its network and information system, an incident notification procedure should be followed. The obligation of DSPs to notify any incidents with a substantial impact on the provision of their service is regulated under Article 16 par 3 and 4 of the Directive. In particular, digital service providers shall **take measures to prevent and minimise the impact of incidents affecting the security of their systems and at the same time notify the competent authority or the CSIRT of any incident with a substantial impact on the provision of their service**.

It is pointed out that, according to article 16 (4), digital service providers are burdened with the obligation to notify an incident only in those cases where they have access to the information needed to assess the impact of an incident. As with security requirements, notification requirements for digital service providers are also lighter. ENISA comments on this lighter approach towards DSPs in its 2017 incident notifications for DSPs in the context of the NIS Directive paper where it states that "*In this respect, the light-touch approach aims at avoiding overburdening the DSPs while not hampering the capacity of the EU to react to cybersecurity incidents in a swift and efficient manner. Therefore, there are reasons to be concerned that a significant lowering in the requirements of incident notification (types of incidents, parameters to be used) could result in hindering the capacity (at EU or national level) to follow up on specific incidents threatening the functioning of the internal market at various levels*".

b) Substantial impact

The obligation of digital service providers to notify an incident is limited to incidents having a substantial impact on the provision of their services. In other words, not all incidents need to be notified to the competent authorities. According to par. 4 of article 16, the impact of an incident is substantially based on the following criteria:

(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident;

(d) the extent of the disruption of the functioning of the service;

(e) the extent of the impact on economic and societal activities.

c) Substantial impact according to the Implementing Regulation

According to the Implementing Regulation (article 4), an incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

- the service provided by a digital service provider was unavailable for more than 5 000 000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes;
- the incident has resulted in a loss of integrity, authenticity, or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100.000 users in the Union;
- the incident has created a risk to public safety, public security or of loss of life;
- the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

The Implementing Regulation also lists in its article 3 the parameters that determine the substantial impact of an incident. In particular and with regard to each criterion of article 16 (4) of the NIS Directive, the following should be taken into consideration:

The number of users: the digital service provider shall be in a position to estimate either of the following:

- the number of affected natural and legal persons with whom a contract for the provision of the service has been concluded; or
- the number of affected users having used the service based in particular on previous traffic data.

The duration of an incident, meaning the time period from the disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality until the time of recovery.

The geographical spread with regard to the area affected by the incident: the digital service provider shall be in a position to identify whether the incident affects the provision of its services in the specific Member States.

The extent of disruption of the functioning of the service: this shall be measured as regards one or more of the following characteristics impaired by an incident: the availability, authenticity, integrity or confidentiality of data or related services.

The extent of the impact on economic and societal activities: the digital service provider shall be able to conclude, based on indications such as the nature of his contractual relations with the customer or, where appropriate, the potential number of affected users, whether the incident has caused significant material or non-material losses for the users such as in relation to health, safety, or damage to property.

d) Substantial impact according to ENISA's guidelines

The notion of substantial impact is also examined under ENISA's guidelines[9]. To this end, ENISA provides a further elaboration of the parameters that must be taken into account when determining the impact of an incident, as these are provided under article 16 (4) of the NIS Directive. In more detail:

- **The number of users affected by the incident.** ENISA's analysis is led by the methodologies used by DSPs when assessing the number of users affected. In this context, the following measurement units were identified: corporate subscribers, non-subscribers (visitors), reliant services and individual subscribers/accounts. DSPs have visibility only

[9] https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive

at the first layer of users, namely the ones that have directly accessed the initial services and are considered users by the initial DSP.

- **Duration of the incident.** ENISA's report provides for a definition of duration of an incident as following "*NIS downtime= the period of time when a digital service provided by a DSP is unavailable or unsecured (confidentiality, integrity or authenticity affected)*".
- **Geographical spread.** According to ENISA's guidelines, the term geographical spread as referred to in the NIS Directive could be defined as follows: "*Member States or regions within the EU where users were affected by impairments (NIS downtime) of the digital service provided by the DSP*". The report points out that this parameter is difficult to be evaluated. In practice f*or a DSP that offers online web access to its services, the identification of the exact countries or geographical areas affected might be impossible without the use of estimations based on previous data*.
- **The extent of the disruption of the functioning of the service.** The extent of the disruption should be evaluated by considering the availability factor, as well as confidentiality, integrity and authenticity. The report concludes to the following definition of "extent of disruption": *extent of the disruption of the functioning of the service= the number of protection goals affected due to an incident disturbing a digital service offered by a DSP*".
- **The extent of the impact on economic and societal activities.** This parameter is the least utilised by the industry. The report defines the impact on economic and societal activities as follows "*by impact on economic and societal activities reference is made to possible damages brought to the functioning of the EU internal market, meaning the encompassing markets in the EU's 28 member states*". The extent of the impact on economic and societal activities is consequently defined as: "*the effects produced by a cybersecurity incident at DSP level that, as a result, affected the overall community, disrupting its normal functioning, generating either economic or social negative consequences*".
- **Other issues related to parameters.** The guidelines also raise the issue of the lack of distinction between the three types of DSPs in the Directive's text. In this context, it is pointed out that there should be a distinction given the different factors that differentiate the providers of digital services, such as technical particularities, criticality etc. It is on this basis that cloud services are considered the most critical out of the three, the online marketplaces follow and when it comes to search engines, the situation is considered even less critical (in the sense that one can always turn to another provider in case of failure of one's favourite engine).

In view of the above, the NISD does not restrict the adoption of subsequent policies that distinguish between the types of DSPs. However, it is pointed out in this report that the technical particularities for each of the three types of DSPs should be addressed early on, since not addressing them might eventually prove to be a mistake (as already mentioned, some parameters required by the NIS Directive cannot be measured in the same way for the different providers).

2.5 National Strategies and national authorities on the security of network and information systems

2.5.1 General

Each Member State must adopt a national framework to comply with the provisions of the NIS Directive. The national framework includes the national strategy on the security of network and information systems and the designation of the authorities that shall be responsible for monitoring the implementation of the NIS Directive. According to article 7 of the NIS Directive, this national strategy shall address a list of issues such as a risk assessment plan, a governance framework to achieve the objectives of the national strategy, the objectives and priorities of the national strategy on the security of network and information systems etc.). Member States are obligated to communicate their national strategies to the Commission within three months from their adoption (article 7 (3)).

The authorities and other bodies that shall be tasked with the role of monitoring the application of the NIS Directive at a national and EU level are specified in articles 8, 9, 11 and 12 of the Directive.

2.5.2 National authorities

The Directive sets the obligation of Member States to designate one or more national competent authorities on the security of network and information systems, as well as a single national point of contact to the same effect (article 8). The competent authorities shall monitor the application of the Directive at national level. The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.

Each Member State shall notify to the Commission, without delay, the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. The Commission shall publish the list of designated single points of contacts.

Additionally, to the designation of the competent authority and the single point of contact, each Member State shall designate one or more computer security incident response teams, the so-called CSIRTs (Article 9). A CSIRT may be established within a competent authority. Their requirements and tasks are described in Annex 1 of the Directive. The CSIRTs role, as per Annex I of the Directive, is to monitor incidents at a national level, provide early warning, alerts and information to relevant stakeholders about risks and incidents, respond to incidents, provide dynamic risk and incident analysis and increase situational awareness, as well as, to participate in a network of the CSIRTs across Europe.

2.5.3 The Cooperation Group and the CSIRTs Network

As far as cooperation at EU level is concerned, a Cooperation Group is established under the Directive (Article 11). The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA (European Union Agency for Network and Information Security). Its tasks are described in Article 11 par. 3 (it shall provide strategic guidance for the activities of the CSIRT network, exchange best practices between Member States, as well as information on research and development relating to the security of network and information systems etc.). The Group's functioning is further clarified by the Implementing Decision issued by the Commission by virtue of article 11(5) of the Directive.

Finally, Article 12 establishes the creation of a network of the national CSIRT's. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. Among the tasks that fall within the CSIRTs Network's competencies are: exchanging information on CSIRTs' services, operations and cooperation capabilities, exchanging and discussing information related to incidents and associated risks (on request, on a voluntary basis), identifying a coordinated response to an incident (on request), providing MS support in addressing cross–border incidents (on a voluntary basis), etc.

2.6 ENISA: The EU Agency for Cybersecurity

2.6.1 General

ENISA is the European Union Agency for Cybersecurity. It is located in Greece (Heraclion, Crete) and it has an operational office in Athens. ENISA was founded by Regulation (EC) No 460/2004 whereas its current regulatory framework consists of Regulation (EU) No 2019/881 of the European Parliament and of the Council (the EU Cybersecurity Act), that only recently came into effect (on 27 June 2019).

ENISA was set up in 2004 and since then is actively contributing to a high level of network and information security (NIS) within the Union. ENISA's mandate is to achieve “a high common level of cybersecurity across the Union” (Article 3.1 of the EU Cybersecurity Act). In particular it shall do so by being a “center of expertise”, and also by acting as a reference point for advice and expertise on cybersecurity for EU stakeholders (Articles 4.1 and 3.1 of the EU Cybersecurity Act respectively).

2.6.2 ENISA’s contribution to Network and Information Security

ENISA’s contribution to network and information security includes:

- Issuing Recommendations;
- Carrying out activities that support policy making and implementation;
- “Hands-On” work, whereby ENISA collaborates directly with operational teams throughout the EU.

A summary of ENISA’s strategy for the years 2016-2020 is being published and can be reached at https://www.enisa.europa.eu/publications/corporate/enisa-strategy. The strategy incorporates the following priorities:

a. Anticipate and support Europe in facing emerging network and information security challenges;

b. Promote network and information security as an EU policy priority;

c. Support Europe in maintaining state of the art NIS capacities;

d. Foster the emerging European NIS Community;

e. Reinforce ENISA’s impact.

2.6.3 ENISA’s contribution to implementation of the NIS Directive

ENISA’s role in implementing the provisions of the NIS Directive is embedded in its text. More particularly, Recital 36 of the NIS Directive states that “ENISA should assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practice. In particular, in the application of this Directive, the Commission should, and Member States should be able to, consult ENISA.” Recital 38 states that “*In general, ENISA should assist the Cooperation Group in the execution of its tasks, in line with the objective of ENISA set out in Regulation (EU) No 526/2013 of the European Parliament and the Council (1), namely to assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information system security under existing and future legal acts of the Union. In particular,* *ENISA should provide assistance in those areas that correspond to its own tasks, as set out in Regulation (EU) No 526/2013, namely analysing network and information system security strategies, supporting the organisation and running of Union exercises relating to the security of network and information systems, and exchanging information and best practice on awareness-raising and training. ENISA should also be involved in the development of guidelines for sector-specific criteria for determining the significance of the impact of an incident*". Finally, Recital 69 states that "*When adopting implementing acts on the security requirements for digital service providers, the Commission should take the utmost account of the opinion of ENISA*".

In practice and with regard to digital service providers, ENISA has issued a report concerning the minimum-security measures for digital service providers[10], as well as another set of guidelines to further describe the incident notification process imposed on DSPs as per article 16 of the NIS Directive[11].

The objectives of the report on the security requirements are summarised to the following:

- Define common baseline security objectives for Digital Service Providers (DSPs);
- Describe different levels of sophistication in the implementation of security objectives;
- Map the security objectives against well-known industry standards, national frameworks and certification schemes.

With regard to the guidelines on the incident notification, they significantly contribute to further elaborating and clarifying notions that are included in the Directive's text, such as the "incidents" that fall within the notification obligation, the term "substantial impact", as well as the "parameters" that must be taken into account when determining the impact of an incident, as these are included in article 16 (4) of the NIS Directive.

Regarding the term 'incident', the guidelines provide the following definition "Any incident affecting the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed by a digital service provider (DSP) through network and information systems, which has a substantial impact on the provision of the digital service offered".

[10] https://www.ENISA.europa.eu/publications/minimum-security-measures-for-digital-service-providers

[11] https://www.ENISA.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive

3 THREAT LANDSCAPE AGAINST OES AND DSP

3.1 OES Identification methodology

After studying the NIS Directive, the ENISA documents [1][2][3] and EU commission recommendations [4][5][6] and the member state actions [7] with particular emphasis on the approaches by Greece, Cyprus [8], Spain [9] and UK[10], a methodology for the identification of an OES was concluded. The criteria are generally based on the size and importance of the organization and critical infrastructure, which subsequently depends on the society and market needs of the member states.

In the energy domain, three main sub-domains are generally identified: electricity, oil and gas. For each sub-domain, the figures regarding production, processing, refining, supply, distributions and/or storage of an operator should be quantified for the identification of an OES.

For the transportation sector, the relevant information/figures for both passenger and goods transportation have to be investigated. The domain includes air, sea, rail and road transportations. From the aforementioned sub-domains, only operators that use digital technologies to provide critical services may be identified as OESs according to the NIS directive. Then, a quantitative analysis of the operator data has to be analyzed (including e.g., number of customers, number of itineraries offered by the operator, kilometers/miles, possible offered alternatives, etc.).

For the banking and finance domains, the reports from the EU central bank, the member state central banks, the market and insurance commissions/authorities and the market chambers have to be investigated in order to identify the OESs of each domain.

For the health sector, general hospitals are investigated through quantitative analysis (e.g., number of beds, medical staff/services, internal and external patients). Respectively, for the water supply sector, the thresholds for the OES identification among providers depend on the number of people served.

Finally, for the digital infrastructure, the DSPs can be classified depending on the total traffic managed/served, the different active domain names, the ICANN certified records, the service rate (queries / day), the uptime, the latency, etc.

After defining the exact quantities/metrics for a member state and for the identification of an OES for each domain, the steps of the methodology depicted in Figure 1.

In the following subsections, the threat landscape per domain is presented in the respective tables. As an introduction for each section, the quantitative criteria for the OES definition per sector are provided (the presented metrics are mainly the result of the policy analysis in Greece, Cyprus, Spain, and UK).

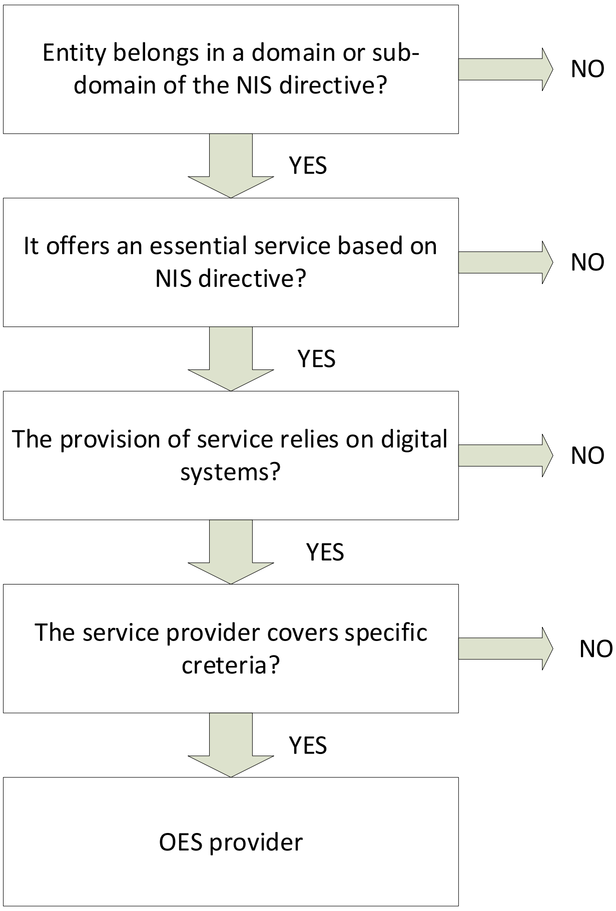
Entity belongs in a domain or sub-domain of the NIS directive?
NO
YES
It offers an essential service based on NIS directive?
NO
YES
The provision of service relies on digital systems?
NO
YES
The service provider covers specific creteria?
NO
YES
OES provider

Figure 1: Steps for the identification of an OES

The determination of the thresholds of the criteria should be based on the state population and its distribution, the existence of alternative agencies or solutions and the needs of the state/market/society in each sector.

The involved quantities and metrics are also taken into account in the assessment of incidents that are presented in Sec. 4. For example, the number of affected people and their distribution but also the incident impact on the economy, the state/government/public operations, the public safety and order, the public opinion, the environment, the international relations, the threat of human life, and the recovery time after the event are metrics that are used to quantify the impact of an attack or failure.

3.2 Basic Asset Categories

As part of the risk analysis, a set/number of basic generic assets were defined. The main concept behind the definition of the basic asset was that all assets involved in a cyber-physical system can be decomposed into basic assets – thus, sharing a large number of common features, threats and vulnerabilities.

In the following subsections, the threats are correlated with basic assets to form common threat patterns that are identified at several or all domains. The scope behind the definition of the basic assets is analyzed in the Risk Analysis deliverables of the project (D2.4 and D2.3). However, the adopted asset taxonomy is also presented in Table 2 for the sake of completeness.

Table 2: Asset groups and basic asset types

Asset Group ID	Asset Group	Asset ID	Basic Asset Type	Reference
AS-HW	Hardware	AS-HW-01	Sensors/Actuators Hardware	[11]
		AS-HW-02	Power supply	[11]
		AS-HW-03	Computational Device	[14]
		AS-HW-04	HW Interface	–
		AS-HW-05	I/O Devices	–
		AS-HW-06	Storage	[14]
AS-DA	Data	AS-DA-01	Backup Data	[11]
		AS-DA-02	Configuration Data	[14]
		AS-DA-03	Operation Data / Application Data	[14]
		AS-DA-04	System Data	[14]
		AS-DA-05	Test Data	[14]
		AS-DA-06	Audit Data	[14]
AS-OS	System Software	AS-OS-01	Embedded Systems Firmware	[11]
		AS-OS-02	Native API	–
		AS-OS-03	Hypervisor	[13]
		AS-OS-04	Operating System	[14]
		AS-OS-05	Containers / VMs	[14]
AS-SO	Application Software	AS-SO-01	Web-Based Services	[11,14]
		AS-SO-02	Application Software	[14]

		AS-SO-03	Database Management Systems	[14]
AS-US	Users	AS-US-01	System Users	[14]
		AS-US-02	End Users	[14]
		AS-US-03	Contractors/Sub-contractors	[14]
AS-NE	Communication Network	AS-NE-01	Communication Protocol	[11]
		AS-NE-02	Network Interfaces	–
		AS-NE-03	Network Controller (HW)	–
		AS-NE-04	Network Stack (SW)	–

3.3 Common threats under a common structure

The identification of generic threats per domain presented in subsections. 3.4 to 0 indicated that a large number of identified threats is shared among the various domains despite the fact that the scope of operation of the OESs and DSPs may be vastly different. This was due to the fact that:

- The functional areas of the Operators remain the same regardless of the domain/sector of the OES.
- All functional areas of the Operators rely on an information and communication platform – a digital infrastructure possibly provided, operated or implemented by a DSP.
- All essential services are interconnected with each other in modern society, and therefore cascading risks and threats are highly possible.

For all Operators, regardless of the domain, the key tasks of their operation are the following:

- Administrative task,
- Production task,
- Distribution task,
- Sales task,
- Customer service task,
- Financing task,
- Marketing task,
- Human resources task,
- R&D task,
- And Information and Communication platform operation.

The last point manages, monitors, controls all the aforementioned tasks, which means that it has become the heart of the system (Figure 2).

Depending on the domain, the scope and type of each task may vary – especially for tasks like Production, Distribution, and R&D, where the majority of the performed functions are domain-specific. However, regardless of the functional procedures, all tasks are monitored, controlled of carried out through a network of computing devices. Maintaining the resources (physical or virtual), installing new software and/or additional hardware, updating all components are crucial ICT functions that ensure the smooth and reliable OES operation. On the other hand, a failure or an attack on the ICT system may be catastrophic since it may affect all possible functional areas of the OES.

This practically means that:

- All OES components -from data to sensors-actuators, web-sites and mobile applications- controlling all aspects - from production to marketing – of the OES operation constitute the ICT platform.
- All conventional cyber-threats that concern an ICT platform or a digital infrastructure are relevant for all OESs regardless of the sector.
- The main differences per sector are located in the impact and criticality of an attack depending on the functionality of the compromised asset.

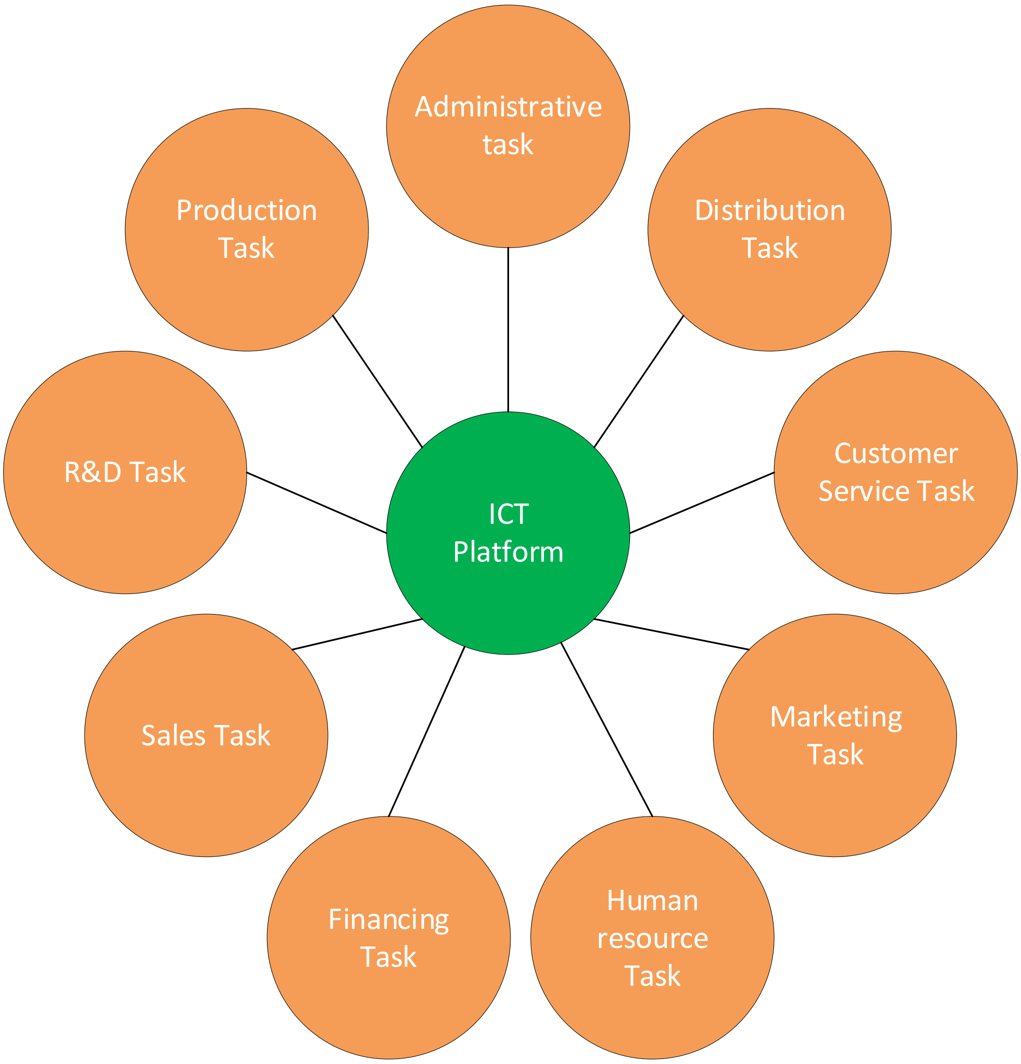

Figure 2: Key tasks of operator functionalities

In [15], ENISA emphasizes the fact that the threat landscape reveals a number of emerging interdependencies between OESs and DSPs at system and service levels. In fact, there is an increasing number of cybersecurity incidents that, due to these interdependencies, either propagated across organizations, often across borders or had a cascading effect at the level of essential services.

Generally, interdependencies and cascading effects propagate through the following modes:

- *Physical:* if the state of a service depends on the material/physical output of another service/infrastructure.
- *Cyber*: if the state of a service depends on information and data exchanged through the information service and communication links. CitySCAPE focuses on cyber interdependencies.
- *Geographic*: The spatial proximity between services/infrastructures makes them geographically dependent in case of a local (e.g. environmental) event/incident.
- *Logical*: Logical interdependency is a connection between states of operations between services/infrastructures that are not physical, cyber or geographic and are the result of human decisions and actions (e.g., failure of infrastructure will increase demand for substitute services).

3.3.1 Interdependencies per sector

Energy: Energy operations are possible thanks to a combination of goods and services that include digital services, finance, digital infrastructure and transport. The energy sector also has dependencies on financial market infrastructures.

Transportation: The increasing digitalization of the transport sector makes it highly dependent on digital infrastructure and DSPs. The transport sector is highly reliant on digital services such as online marketplaces, online search engines and cloud computing services for their daily operations. For instance, the unavailability of such services would severely impact automated airport processes such as online check-in, self-service luggage, ticketing, etc., resulting in flight delays, financial and reputational losses.

The cyber (inter)dependencies of the transport sector are likely to increase due to the digitalisation and integration of transport services (multimodal transport).

Another dependency is on the energy sector since energy disruptions will cause transport service disruption (oil/gas outage). There is also dependence on the banking sector since transactions through DSPs are performed via e-banking platforms.

Banking and Finance: The sectors of banking and financial market infrastructures show a high level of dependency on digital infrastructure and DSPs. This is because the activities of these sectors involve electronic transactions that rely on digital infrastructures and services. Additionally, disruptions to energy supplies could potentially trigger a cascade effect on the normal functioning of digital infrastructures and then consequently to banking and financial market infrastructures.

Health: The dependency on the electricity sector is essentially the most critical for health services. The case of a power outage is just a practical example that highlights the dependency of health operators on the energy sector for maintaining their services – conventional and/or electronic. Moreover, the sector is becoming more and more dependent on digital infrastructure. The dependency on the drinking water supply and distribution sector is another critical dependency for the health sector. Healthcare also depends on banking sector services in order to perform several financial transactions.

Water utilities: Services of drinking water supply and distribution depend on different automation systems, which need to operate constantly to provide the necessary operational information creating a dependency on the energy sector. Growth in the variety of data processed by the water supply and distribution operators, particularly unstructured data, is changing the landscape of water data and the manner the use, storage and protection of this data is more and more dependent on the DSPs.

3.3.2 Interdependencies examples

Concerning software and its dangers in Critical Infrastructure information systems, one should look no further than the incident with the security worm, Stuxnet. The Stuxnet incident was a typical example of software being able to misuse functionality in machinery and manifest catastrophic failures across multiple infrastructures. Many Critical Infrastructures use Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) as control locations in order to handle the machinery and functionality of an infrastructure (e.g. valves, sensors, breakers, etc.). Thus, a failure on any one of them may affect the operation of the entire infrastructure and start a cascading event, where multiple CIs fail due to their dependencies.

As far as the dangers of interdepended infrastructures are concerned, Rinaldi, Peerenboom and Kelly in [16] provide a visual presentation of the well-known electric failure scenario of California, which is a characteristic, real-case example of a multi-order dependency between CIs. The electric power disruptions in California caused cross-sectoral cascading effects, as power disruptions affected natural gas production, operation of petroleum product pipelines transporting gasoline and jet fuel, along with the operation of massive water pumps for crop irrigation.

3.4 Threat Landscape for the Health Sector

Type of entities: Healthcare providers

The term "Health care" refers to health services provided to patients by health professionals to assess, maintain or restore their state of health, including the prescribing, administration and supply of medicines and medical devices and the execution of surgeries and invasive therapies.

Criteria

For the health domain and, in particular, for the basic health care services, the criteria are:

- The institution/organization should be considered a General Hospital,
- Threshold 1: It should have the capacity to treat at least T_1 patients annually,
- Threshold 2: As a General Hospital, it should have at least T_2 hospital beds

As an example, in Greece, $T_1 = 40{,}000$ patients and $T_2 = 500$ beds

Following the threat taxonomy of ENISA's procurement guide [17][18], this section also shows how the specific cybersecurity issues in healthcare can have implications for Cloud services [18].

Table 3:Threat Landscape for the Health Sector

High-level threat	Threat	Description	Affected assets
Natural phenomena	Fire, floods, earthquakes	Fire, floods or earthquakes are infrequent but possible threats to the infrastructure and overall equipment (devices, network components etc.). Habitually, computerized tomography scan machines, Magnetic Resonance Imaging (MRI) equipment, **radiotherapy equipment and other highly expensive devices are usually located on the ground floor or at the basement of the hospitals** -either by regulatory laws or just because of their weight and dimensions- **and are especially affected by this type of phenomena**. It should be noted that **failures due to floods or fires** i.e., broken pipe flooding the basement of a patient room, **can have a different impact than a disaster due to natural phenomena** (wildfire, storm, tsunami etc.)	All assets

High-level threat	Threat	Description	Affected assets
		and **eventually could affect the whole hospital** and **its surrounding or supply chain provider**. Concerning the Cloud infrastructure, natural forces could eventually **destroy relevant systems**, **network components**, or **devices**. Although the threat probability is low, the impact might be huge.	
Supply chain failure	Cloud Service Provider (CSP) failure *** if cloud environment is used; otherwise, the threat applies to the hospital servers***	**Not all services are hosted on hospital servers**. Accounting, salaries, stock control may be outsourced and depend on third-party cloud services. Nearly all personal IoT medical devices work in the cloud. In fact, some hospitals -especially regional or small associated centers- can have their entire electronic health record system located in other sites. If not adequately backed up to work off-line, these services may cause severe disruptions in the provision of medical services. **The Cloud services' availability is highly dependent on the Cloud service provider**. The bankruptcy of the Cloud service provider, for instance, may threaten the continuous availability of the Cloud service, which may cause operational outages of healthcare organizations due to service failure. In the case of the Cloud provider's failure, a lack of data export and portability may result in loss of data. For all supply chain threats, redundancy and resiliency are critical topics healthcare organizations should consider and inquire about.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-OS-03 Hypervisor AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-03 DBMS AS-US-01 System users AS-US-02 End users AS-US-03 Contractors AS-NE-03 Network HW AS-NE-04 Network SW
	Network provider failure	A network failure can have devastating effects. Most of the main hospital centers form a hub between the main building and its associated centers -mostly radiology or ambulatory or day-care centers. **Redundancy and topology design are crucial** when mitigating this type of threat. Network connection is also crucial to access Cloud healthcare services. **A network failure may impact Cloud-based healthcare service provision** and affect the collaboration between different internal and external partners.	AS-OS-03 Hypervisor AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-NE-03 Network H/W AS-NE-04 Network S/W

High-level threat	Threat	Description	Affected assets
	Power supply failure	Loss of electricity can be of importance depending on the equipment affected. **Intensive care units, operative rooms, servers and clients are usually protected by uninterruptible power sources or batteries but other equipment such as MRI or CT machines can be compromised**. Power supply **can also affect the Cloud service's availability, which may be critical when a pacemaker's data cannot be observed.**	AS-HW-02 Power supply AS-HW-03 Computational device AS-HW-04 H/W interface AS-HW-06 Storage AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-US-01 System users AS-US-02 End users AS-NE-03 Network controller
	H/W failure	**Failure of IT hardware** at a customer's (or maybe a Cloud service provider's) site limits the service's availability which may severely impact patients' health in emergency cases. A medical device failure **affects real-time data availability in the service, possibly harming the patient's health**.	AS-HW-04 H/W interface AS-NE-03 Network H/W AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data

High-level threat	Threat	Description	Affected assets
Human errors	Unauthorised access control	**Due to the variety of roles** in a hospital (i.e. physicians, caregivers, administration), **access control procedures should be in place**. As the priority to all hospital staff is care, workarounds are often the case when it comes to access control (including all types of access control from buildings to systems and accounts). This poses great threats to the hospital interconnected environment.	AS-HW-02 Power supply AS-HW-03 Computational device AS-HW-05 I/O devices AS-SO-02 Application software AS-SO-03 DBMS AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Unauthorized data access	**Cloud users may gain unauthorized access to data due to insufficient access management** or **lack of awareness**, which causes unintentional data disclosure. For example, a Cloud-based electronic health record has more users than a telemedicine solution.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Non-compliance (BYOD)	Today's employees want the freedom to work from any location and any device at any time of day. These individuals are increasingly using their personal mobile devices to undertake work tasks. From a business perspective, enabling BYOD is an advantageous strategy. However, bring-your-own-device (BYOD) can also represent a significant risk for organisations. For the IT department, **there is massive pressure to find a way to securely enable BYOD. Failure to do so can lead to malware outbreaks**, **noncompliance with regulatory requirements** and **corporate exposure in the wake of personal device theft**. The BYOD policy is widely applied in the healthcare sector, which causes variation in endpoint security. Measures to secure endpoints need to be adopted, and impacts on compliance, especially for accessing electronic health records, should be analysed.	Potentially most of the assets

High-level threat	Threat	Description	Affected assets
	Unintentional change of data	**Entering incorrect data** into a healthcare system **can result in loss of integrity and data disclosure to unauthorised users**, such as uploading medical documents to the wrong electronic health record.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Errors by Cloud service administrators/support staff	**If data is not appropriately deleted from a Cloud storage or the backup media, the data may be accessed later by another Cloud customer** of the same Cloud provider, and eventually result in a data breach. Configuration errors by Cloud service support staff may also leave vulnerabilities unpatched and leave entry points open for malicious attackers.	AS-HW-06 Storage AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-US-01 System Users
	Malware injection attacks (i.e. virus, ransomware, worms)	In healthcare organisations, IT systems are strongly interconnected and difficult to isolate without generating service disruption, creating a comfortable ecosystem for malware. Enterprises with a very large number of devices may have difficulties updating their licenses because of the elevated costs. Adware is one of the easiest ways to distribute malware and more often ignored by users. **Ransomware is perhaps the most known threat for healthcare organisations**, due mainly to the Wannacry case. Ransomware usually makes indiscriminate low-cost attacks. **It's very easy to infect healthcare infrastructure** because of two factors; (i) **software infrastructure is hard to keep updated because it's very difficult to get a downtime slot**, (ii) **machines that run legacy software** that only works on specific OS or drivers' version turns out to be an easy target for these attacks. Many of these legacy devices that cannot be updated act as reservoirs for the malware helping it spread through the network.	H/W asset group DATA asset group SYSTEM S/W asset group USERS asset group COMMUNICATION NETWORK asset group

High-level threat	Threat	Description	Affected assets
		Cloud environments are susceptible to malware injection attacks, which are a subcategory of web-based attacks. Attackers exploit vulnerabilities of a web application and embed malicious code into the normal action course. **All Cloud service models are equally vulnerable to this kind of malicious action**. Once the malicious code is executed, **the attacker may eavesdrop, manipulate or steal data and instigate further attacks**.	
Malicious actions	Web application attacks	**SQL Injection and Denial of Service represent the 68,8% of web application attacks**, while government institutions represent only the 26% or 27,7% globally. SQL injection alone represents the 46% in the case of healthcare, similar percentage to energy and manufacturing companies, another environment where industrial equipment is very frequent.	AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-DA-01 Backup data AS-DA-03 Application data AS-DA-04 System data (Logs) AS-US-01 System users AS-US-02 End users
	Mobile application attacks	**Vulnerability in mobile apps** running in the Cloud **may also leave entry points open to be exploited by malicious attackers** and result in data disclosure to unauthorised persons or even data loss.	AS-HW-03 Computational device AS-HW-04 H/W interface AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-OS-01 Embedded System's firmware AS-OS-02 Native API AS-SO-02 Application S/W

High-level threat	Threat	Description	Affected assets
			AS-NE-01 Communication protocol AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W
	Hijacking (Cryptojacking, medjacking)	Medical equipment usually needs real time communications, and clinicians need also a quick response from the system when they look for patient data or test information. **Dedicating processor time or communication capacity to mining cryptocurrency impacts performance and** of course, **the health care provision**. The **difference between cryptojacking and medjacking** is basically the kind of hardware involved. **In the first case we are talking about general-purpose IT infrastructure** and **in the second we are referring to IT-based medical equipment**. Hijacking infrastructure of the Cloud service provider to mine cryptocurrency (crypto-jacking) or a medical device (med-jacking) affects the patient's safety or the performance of the Cloud service healthcare provision. **Hyper-jacking refers to hijacking the hypervisor using a virtual machine-based rootkit.** Successful compromise of the hypervisor grants access to the entire machine and allows the compromise of the virtual machine.	AS-HW-03 Computational device AS-HW-04 H/W interface AS-DA-01 Backup data AS-DA-03 Operation data AS-DA-04 Log data AS-DA-06 Audit data AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-US-01 System users AS-US-02 End users
	Social Engineering attacks (Phishing, baiting, device cloning)	Compromised email (phishing, spam and spear-phishing) is the dominating attack vector for malware infections. According to Verizon DBIR334, **email compromise was the attack vector for 92,4% of detected malware.** Most organizations still allow access to private mail web accounts in most of the computers of the hospital. Mail addresses from clinicians are easy to collect through hospital public directories, existing	AS-DA-01 Backup data AS-DA-03 Operation data AS-DA-04 System data AS-DA-06 Audit data

High-level threat	Threat	Description	Affected assets
		presentations on the web, etc. Using professional e-mail accounts for personal matters and vice versa should be considered a bad policy. **Device cloning (ID cards) requires a high level of specialization and the necessity to get closer to the victim to clone his/her ID**. Two-factor identification (2FA) has made this type of threat very unlikely. **In cloud environments, social engineering attacks to steal user credentials for SaaS solutions** through phishing, spam, or spear-phishing emails are always targeted at the weakest link in the security chain, the human factor. Overall, the healthcare sector is commonly known as less IT savvy, and this raises the exposure to cyberattacks. Strong authentication provided by the Cloud service provider helps to prevent these kinds of attacks. **Successful attacks could result in data breaches, data leakage, or data theft**.	AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-US-01 System users AS-US-02 End users
	Account hijacking/Identity Theft	There are 2 cases: employees' identity or patients' identity. The first case can be dangerous because impersonating a doctor or nurse allows, for example, to do wrong prescriptions or diagnose a patient of a certain disease, and the second case could be used to fraud the healthcare system and introduce wrong diagnoses as well.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Theft: - Device - Data	The cost of medical devices is very high. **Stealing of medical equipment is a very common crime**. Devices are usually sold in the second-hand market of underdeveloped countries or for veterinary uses for a fraction of their price. Small to medium-sized portable devices as ultrasound equipment, EKG, defibrillators, infusion pumps or vital signs monitors are among the most robbed pieces. Devices should not expose medical data unless adequately logged in. Unfortunately, most of them use the factory default credentials. The lack of involvement of IT security department in setting up and managing medical equipment, the lack of risk-awareness of the staff can generate information leaks that could impact reputation, patient privacy, penalties, or even patient safety.	AS-HW-03 Computational devices AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Medical device tampering	Unprotected communications between medical devices and servers can result in tampering with the information. **Sophisticated man-in-the-middle (MITM) attacks can change the data coming from vital signs monitors**, laboratory, pathology reports or even DICOM	AS-HW-03 Computational device AS-HW-04 H/W interface

High-level threat	Threat	Description	Affected assets
		images coming from CT scans, MRI or ultrasound systems in their way to the PACS server.	AS-HW-05 I/O devices AS-HW-06 Storage AS-NE-02 Network Interface
	Insecure interfaces and APIs	A possibly existing Cloud computing environment in healthcare systems provides **user interfaces** and **APIs to interconnect devices** and interact with the Cloud service. **These interfaces offer an entry point for malicious attackers** if they are poorly designed and lack security measures such as encryption and access control. Broken or hacked API's **may result in data breaches**.	AS-HW-04 H/W interface AS-OS-02 Native API AS-NE-02 Network interfaces
	Insider threat	Insiders **can be current or former employees** of healthcare organizations, **contractors** or **other trusted partners** who gain access from the inside of an organization. These parties have had authorized access and may negatively affect a possibly existing Cloud service, ultimately resulting in a data breach.	AS-US-01 System users AS-US-02 End users AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Denial of Service (DoS)	**Denial of service attacks** against the Cloud service **overload its resources due to a flood of requests** originating from many sources and **cause its unavailability** and inability to process requests.	AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-OS-03 Hypervisor AS-OS-05 Containers/VMs AS-NE-01 Communication protocol AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W

High-level threat	Threat	Description	Affected assets
	Intercepting data in transit (Man-in-the middle attack)	In a possibly existing Cloud architecture model, **data** is **transferred from the Cloud customer to the Cloud service provider**. During transition, it **may be intercepted** and eventually result in a data breach.	AS-DA-01 Backup data AS-DA-03 Operation data AS-DA-04 System data
	Network-related technical failures or attacks	**Technical failures of network-related components influence the availability** of Cloud service. Examples include the **loss of Internet connectivity due to failures at the Cloud customer's or service provider's site**, a temporary reduction of network bandwidth at the Cloud customer's internet service provider, which affects the data transfer from and to the Cloud service provider, and disruptions in the global Internet routing infrastructure capping the connection between the Cloud customer and Cloud service provider.	AS-HW-03 Computational devices AS-OS-01 Embedded firmware AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W

High-level threat	Threat	Description	Affected assets
System Failure	S/W failure	**Any piece of software can have errors**. Special security measures are taken in devices such as infusion pumps, electrosurgical units, ventilators, medical use lasers, or devices that use ionizing radiation to work - radiology and radiotherapy equipment- that could generate physical damage if an error occurred. Lessons have been learned from severe incidents that occurred in the past. **The general rule is: all measures have to be taken so no overdose can be administered under any circumstance**. **Servers are more prone to failure**, not only because of failures in the design of their dedicated software but because they rely in other software platforms (operating systems, programming frameworks, databases) that can fail as well. If fact, experience has shown us that many errors occur after a software update. **Failures in medical servers normally occur as latent errors and, in some occasions, can stop the service**. They habitually disappear after a server reboot. Analysis of the generated logs is crucial to find what the cause of the error was. **Failures that do not cause server breakdowns or service disruption** (loss of patients' appointments or patient's clinical information, for example) **are usually detected several months after the system has been running**. **Several specially prepared tests should be run to ensure that the system does what it is expected to do**. As these systems run 24-7, if there is no testing environment, finding downtime slots to run the tests can be very difficult if not impossible. **Frequent server failures deteriorate medical care and degrade confidence in the institution**. Due to errors, **software failure can affect the Cloud services or medical device data availability and eventually endanger patient safety**.	AS-HW-03 Computational device AS-OS-01 Embedded firmware AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS
	Outdated firmware	**Lack of procedures** in place **to update the firmware in all devices** (medical or not) in the hospital **is a top threat for healthcare organisations and namely hospitals. Legacy systems and software offer backdoors** to malicious actors that can access sensitive healthcare data.	AS-OS-01 Embedded system's firmware

3.5 Threat Landscape for the Banking Sector

Type of entities: Credit institutions

Credit institutions are defined as undertaking whose business is the acceptance of deposits or other repayable funds by the public and the provision of credits for their own account.

Criteria

For the basic Financial Transactions service, the criterion is that the banking institution has been licensed to operate in the member state and has been designated by the central bank of the member state as a systematically important credit institution (Other Systemically Important Institutions (O-SII)). In general, the central bank of each member state is responsible for the identification of other systemically important credit institutions among the institutions that have received an operating license in the member state.

In the following table, the threat landscape for the banking sector is presented [19][20][21].

Table 4: Threat landscape for the banking sector

High-level threat	Threat	Description	Affected assets
	H/W failure	**Failure of IT hardware** at a Cloud service provider's site, limits the service's availability which may severely impact **real-time data availability of e-banking services**.	AS-HW-04 H/W interface AS-NE-03 Network H/W AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data

Human errors	Unauthorized access control	**Due to the variety of roles** in a bank (i.e., manager, client advisers, investment analyst etc.) multiple **access control procedures should be applied.**	AS-HW-02 Power supply AS-HW-03 Computational device AS-HW-05 I/O devices AS-SO-02 Application software AS-SO-03 DBMS AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Unauthorized data access	**Cloud users may gain unauthorized access to data due to insufficient access management** or **lack of awareness**, which causes unintentional data disclosure.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Non-compliance (BYOD)	Banks have allowed a record number of employees to work from home in response to the COVID-19 pandemic. For many of these organizations, a remote workforce will become the new normal despite data security concerns prohibiting them in the past. However, bank employees are not the only stakeholders driving the demand for mobile access. Customers are also looking for fully remote solutions, and it seems highly unlikely that they will return to bank lobbies once they become accustomed to mobile banking. This remote user influx means a larger attack surface consisting of less secure devices connecting to a cloud-based network. As a result, cybersecurity teams face a perfect storm of issues leading to some notable breaches. Traditional Mobile Device Management (MDM) solutions for BYOD devices are heavy-handed and raise several privacy issues (Horne, 2020). Finding the best bank data security solution can be a daunting task as a failure to do so can lead to malware	

		outbreaks, noncompliance with regulatory requirements (such as GDPR) and corporate exposure in the wake of personal device theft.	
	Unintentional change of data	**Entering incorrect data** into a banking system **can result in loss of integrity and data disclosure to unauthorized users**, such as altering transactions or revealing customers' personal financial data.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Malware injection attacks (e.g. ransomware)	Malware has long been a threat to the banking sector. By infecting vulnerable end-user devices with malware, cybercriminals are able to gain access to entire banking networks and steal critical user data. With malware becoming easier than ever to obtain, this threat has grown in recent years, as in 2019, it was responsible for 75% of all data breaches in the banking sector (Bitglass, 2019). The growth of the malware-as-a-service model, as well as fileless malware attacks, highlights the need for comprehensive security policies in the banking industry. Malware attacks are becoming easier and cheaper to carry out so it is essential that banks work with their security teams to ensure that both customer and employee devices cannot be compromised (Hewit, 2020).	H/W asset group DATA asset group SYSTEM S/W asset group USERS asset group COMMUNICATION NETWORK asset group
Malicious actions	Web application attacks	An annual security report issued by (Akamai, 2021) observed nearly 6.3 billion web application attacks in 2020, with more than 736 million targeting financial services -- which represents an increase of 62% from 2019. SQL Injection (SQLi) attacks remained in the top spot across all business types globally, making up 68% of all web application attacks in 2020, with Local File Inclusion (LFI) attacks coming in second at 22%. However, in the financial services industry, LFI attacks were the number one web application attack type in 2020 at 52%, with SQLi at 33% and Cross-Site Scripting at 9%.	AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-DA-01 Backup data AS-DA-03 Application data AS-DA-04 System data (Logs) AS-US-01 System users AS-US-02 End users
	Mobile application attacks		AS-HW-03 Computational device AS-HW-04 H/W interface

		Vulnerability in mobile apps running in the Cloud **may also leave entry points open to be exploited by malicious attackers** and result in data disclosure to unauthorized persons or even data loss.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-OS-01 Embedded System’s firmware AS-OS-02 Native API AS-SO-02 Application S/W AS-NE-01 Communication protocol AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W
	Social Engineering attacks (Phishing, baiting, device cloning)	Unlike traditional hacking methods, social engineering attacks exploit human behavior to gain access to company servers. Social Engineers manipulate employees into sharing login credentials or other sensitive information which is then used to compromise the network. As it was stated in an annual report issued by (Akamai, 2021) 50% of all unique organizations impacted by observed phishing domains were from the financial services sector. **Phishing attacks** are methods of communication, such as emails, calls, or texts, that impersonate company officials to trick employees into divulging personal information (e.g., their credentials). Phishing attacks can also use misleading links to guide employees to websites that are infected with malware. Customers are also frequently targeted in phishing attacks, so it is essential to educate them about cybersecurity best practices as well. This can be done through a security awareness newsletter or email (Hewit, 2020).	AS-DA-01 Backup data AS-DA-03 Operation data AS-DA-04 System data AS-DA-06 Audit data AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS

			AS-US-01 System users AS-US-02 End users
	Account hijacking/Identity Theft	Identity theft is the practice of taking someone else's financial or personal data without their knowledge with the motive of conducting concealed, illegal activities. When there is a privacy breach in a bank, the stolen information of the bank's customers is usually sold and purchased on the dark web by illegal organizations and other cybercriminals.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Data Manipulation	A common misconception about cyber-attacks is that they are only concerned with data theft. That is not always the case, however, as data manipulation attacks have become an increasingly popular means of attack for cybercriminals. Data manipulation attacks occur when a threat actor gains access to a target system and makes undetected changes to data for their own personal gain. An example of this is if an employee modifies customer transactional data. This will likely go unnoticed as the transactions will appear legitimate, leading to mistakes in how future data is recorded. The longer the manipulation goes undetected, the more damage it will cause. Because manipulated data does not look any different than normal data, these attacks are extremely difficult to detect and prevent. In the banking sector, this is especially dangerous as manipulated data can result in non-compliance with data standards and lead to substantial fines (Hewit, 2020).	AS-HW-03 Computational devices AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Insecure interfaces and APIs	A possibly existing Cloud computing environment that hosts e-banking services provides **user interfaces** and **APIs to interconnect devices** and interact with the Cloud service. **These interfaces offer an entry point for malicious attackers** if they are poorly designed and lack security measures such as encryption and access control. Broken or hacked API's **may result in data breaches**.	AS-HW-04 H/W interface AS-OS-02 Native API AS-NE-02 Network interfaces

	Insider threat	Insiders **can be current or former employees** of bank organizations, **contractors** or **other trusted partners** who gain access from the inside of an organization. These parties have had authorized access and may negatively affect a possibly existing Cloud service, ultimately resulting in a data breach.	AS-US-01 System users AS-US-02 End users AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Denial of Service (DoS)	**Denial of service attacks** against a Cloud-based banking service **overload its resources due to a flood of requests** originating from many sources and **cause its unavailability** and inability to process requests. Over the past three years, 2018-2020 (Akamai, 2021) observed DDoS attacks against the financial services sector grow by 93%, indicating that systemic disruption remains an objective for criminals, who target services and applications required for daily business.	AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-OS-03 Hypervisor AS-OS-05 Containers/VMs AS-NE-01 Communication protocol AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W
	Intercepting data in transit (Man-in-the middle attack)	In a possibly existing Cloud architecture model, financial and other types of personal **data** is **transferred from the Cloud customer (a bank organization) to the Cloud service provider**. During transition, it **may be intercepted** and eventually result in a data breach.	AS-DA-01 Backup data AS-DA-03 Operation data AS-DA-04 System data
		Technical failures of network-related components influence the availability of Cloud service. Examples include the **loss of Internet connectivity due to**	AS-HW-03 Computational devices

	Network-related technical failures or attacks	**failures at the Cloud customer's or service provider's site**, a temporary reduction of network bandwidth at the Cloud customer's internet service provider, which affects the financial and other types of personal data transferred from and to the Cloud service provider, and disruptions in the global Internet routing infrastructure capping the connection between the Cloud customer and Cloud service provider.	AS-OS-01 Embedded firmware AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W
System Failure	S/W failure	By software failure we refer to malicious code and intruders exploiting flaws in the software code of either a mobile banking application or a banking system. A direct threat to the data exists when software failure causes information to be inaccurate or simply corrupts or impedes availability.	AS-HW-03 Computational device AS-OS-01 Embedded firmware AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS

3.6 Threat Landscape for the Finance Sector

Type of entities: financial product market trading operators and CCPs

A financial product market is a facility where financial products are bought or sold, or where offers or invitations to buy or sell financial products are made.

A central clearing counterparty (CCP), also referred to as a central counterparty, is a financial institution that takes on counterparty credit risk between parties to a transaction and provides clearing and settlement services for trades in foreign exchange, securities, options, and derivative contracts.

Criteria

For the basic service of financial market trading operator venues, the criterion is that the operator makes at least 10% of the transactions made on an annual basis.

For CCPs, the criterion is for the entity to make at least 10% of the total transactions of an annual basis.

In the following table, the threat landscape for the finance sector is presented [20][21][22][23].

Table 5: Threat landscape for the finance sector

High-level threat	Threat	Description	Affected assets
Natural phenomena	Fire, floods, earthquakes	Large scale and large effects of natural disasters and social phenomena can have a different probability. Large scale natural disasters and rare social phenomena are infrequent but could impact the systems supporting critical business functions.	All assets
Supply chain failure	Cloud Service Provider (CSP) failure	Cloud services are an on-demand service model for IT provision often based on virtualization and distributed computing technologies. More and more financial institutions are moving their systems into the cloud. The benefits of the cloud are very clear to the institutions – cost savings, flexibility and resilience, are just some of the key advantages. With cloud services, the security model changes. Although the liability stays with the financial institution, some of the security controls are with the cloud provider and this brings additional security challenges. One of the key challenges that we have seen in cloud adoption is isolation failure, which means that there is no proper access to the resources. Another challenge is the customer management interfaces of public cloud providers, which are Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-OS-03 Hypervisor AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-03 DBMS AS-US-01 System users AS-US-02 End users AS-US-03 Contractors

High-level threat	Threat	Description	Affected assets
			AS-NE-03 Network HW AS-NE-04 Network SW
	Network provider failure	Network failures (electricity, telecommunications) can often disrupt the reactivity of operational actors, particularly the establishment of connections. Therefore, more flexible solutions must be found, solutions that do not depend on telecommunications or Internet networks	AS-OS-03 Hypervisor AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-NE-03 Network H/W AS-NE-04 Network S/W
	Power supply failure	Loss of electricity can be of economic importance depending on the equipment affected.	AS-HW-02 Power supply AS-HW-03 Computational device AS-HW-04 H/W interface AS-HW-06 Storage AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-US-01 System users AS-US-02 End users AS-NE-03 Network controller

High-level threat	Threat	Description	Affected assets
Human errors	Unauthorized access control	Attackers might seek to compromise software vulnerabilities, the payment gateways hosted at the payment service providers for instance, by exploiting unauthorized access to payment gateways and weaknesses in enforcement of internal payment service providers' security controls and measures. An example of this type of attack is the one which was carried out against British Airways in August 2018 (6), when credit card data was stolen by injecting code directly onto the company's website, which is also used by the mobile app. Through the injected code, credit card data was transmitted to a website controlled by the criminals.	Payment systems compromise AS-HW-03 Computational device AS-HW-05 I/O devices AS-SO-02 Application software AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Unauthorized data access	Stolen or compromised data usually is found in the Dark Web where it is usually offered for sale in Dark Web marketplaces alongside other illegal content. Latest exploits, drugs and stolen sensitive data (credit cards, identities) are some of the most common items that can be found there.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Non-compliance (BYOD)	Today's employees want the freedom to work from any location and any device at any time of day. These individuals are increasingly using their personal mobile devices to undertake work tasks. From a business perspective, enabling BYOD is an advantageous strategy. However, bring-your-own-device (BYOD) can also represent a significant risk for organisations. For the IT department, there is massive pressure to find a way to securely enable BYOD. Failure to do so can lead to malware outbreaks, noncompliance with regulatory requirements and corporate exposure in the wake of personal device theft.	
	Unintentional change of data	Entering incorrect data can result in loss of integrity and data disclosure to unauthorised users, such as	AS-DA-01 Backup data

High-level threat	Threat	Description	Affected assets
		uploading documents to the wrong electronic record. It causes economic damage to the company	AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Errors by Cloud service administrators/support staff	If data is not appropriately deleted from a Cloud storage or the backup media, the data may be accessed later by another Cloud customer of the same Cloud provider, and eventually result in a data breach. Configuration errors by Cloud service support staff may also leave vulnerabilities unpatched and leave entry points open for malicious attackers.	AS-HW-06 Storage AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-US-01 System Users
	Configuration errors Operator/user error	Configuration errors or operator/user errors also have a negative impact. The impact could also introduce major security weaknesses, or at worst could potentially cause severe incidents involving users, e.g. self-driving vehicles. Lost hardware, such as laptops containing sensitive data or authentication details (passwords, or VPN certificates) can introduce vulnerability and lead to subsequent attacks.	AS-OS-01 Enbedded Systems Firmware AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-US-01 System Users AS-US-02 End users AS-US-03 cont/sub-contractors
	Malware injection attacks (i.e. virus, ransomware, worms)	Malware potentially causes a huge impact on the whole infrastructure, as it acts maliciously in the machine where it runs and often propagates through other connected systems. Usually, the cause is vulnerabilities not patched in time. Mobile devices have become the norm today for making online payments. Most of the threats affecting these devices are very similar to a	H/W asset group DATA asset group SYSTEM S/W asset group USERS asset group

High-level threat	Threat	Description	Affected assets
		desktop computer or a laptop, but due to its size, mobile devices offer additional opportunities for an attacker. Mobile devices usually do not offer the same protection as desktop PCs as they rarely run an antivirus software, a firewall, etc. With the introduction of new mobile payment services, they will be a more interesting target for attackers. Abusing a lost or stolen device to make online transactions is a very common threat. Another could be, installing malware on the device to tamper with or gain access to mobile application for online transactions. Payment Service Providers (PSPs) offer terminals for payments as well as aggregated payment services for merchants by processing data from different channels, including face-to-face (card present) payments, online payments and mobile/contactless payments. PSP payment gateways represent an interesting target for attackers that seek to compromise the payment data in transit from the merchants to the different acquiring banks. Attackers might seek to compromise software vulnerabilities, the payment gateways hosted at the payment service providers for instance by exploiting unauthorized access to payment gateways and weaknesses in enforcement of internal payment service providers' security controls and measures.	IT communications Mobile payments Payment systems
	Man-In-The-middle	Man-In-The-Middle (MiTM) attacks against the POS and ATM terminals are enabled by weaknesses regarding the end-to-end encryption between the terminal and the server. If encryption is not properly configured or non-existent, information could be stolen and used for abuse later. Attackers can also attempt to exploit network security weaknesses such as a lack of firewalls to protect the internal network or vulnerabilities in POS/ ATM software and misconfigurations (e.g. not enforcing minimum privileges to access terminals and servers).	All the assets Especially: AS-DA-01 Backup data AS-DA-03 Operation data AS-DA-04 System data
	Social engineering (Pretexting, Untrusted links (fake websites / CSRF / XSS), Baiting, Reverse social engineering, Impersonation, Identity Theft)	Social engineering is the manipulation of people to divulging information or performing actions on behalf of the attacker. Social attacks are effective as they can	AS-DA-03 Operation data AS-DA-04 System data AS-DA-06 Audit data

High-level threat	Threat	Description	Affected assets
		bypass technical and physical controls. Successful attacks could result in data breaches, data leakage, or data theft	AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-US-01 System users AS-US-02 End users IT and Communication
Malicious actions	Web application attacks	SQL Injection and Denial of Service represent the 68,8% of web application attacks. SQL Injection (SQLi) attacks remained in the top spot across all business types globally, making up 68% of all web application attacks in 2020, with Local File Inclusion (LFI) attacks coming in second at 22%. However, in the financial services industry, LFI attacks were the number one web application attack type in 2020 at 52%, with SQLi at 33% and Cross-Site Scripting at 9%.	AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-DA-01 Backup data AS-DA-03 Application data AS-DA-04 System data (Logs) AS-US-01 System users AS-US-02 End users
	Mobile application attacks	Vulnerability in mobile apps running in the Cloud may also leave entry points open to be exploited by malicious attackers and result in data disclosure to unauthorised persons or even data loss.	AS-HW-03 Computational device AS-HW-04 H/W interface AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data

High-level threat	Threat	Description	Affected assets
			AS-DA-04 Log data AS-OS-01 Embedded System's firmware AS-OS-02 Native API AS-SO-02 Application S/W AS-NE-01 Communication protocol AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W
	Cryptojacking	Cryptojacking (also known as cryptomining) is the unauthorized use of a device's resources to mine cryptocurrencies. Targets include any connected device, such as computers,tablets and mobile phones; however, cybercriminals have been increasingly targeting cloud infrastructures. This type of attack has not attracted much attention from law enforcement agencies and its abuse is rarely reported, mainly because of its relatively few negative consequences. Nevertheless, organisations may notice higher IT costs, degraded computer components, increased electricity consumption and reduced employee productivity caused by slower workstations	AS-HW-03 Computational device AS-HW-04 H/W interface AS-DA-01 Backup data AS-DA-03 Operation data AS-DA-04 Log data AS-DA-06 Audit data AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-US-01 System users

High-level threat	Threat	Description	Affected assets
			AS-US-02 End users
	Social Engineering attacks (Phishing, baiting, device cloning)	Compromised email (phishing, spam and spear-phishing) is the dominating attack vector for malware infections. According to Verizon DBIR334, email compromise was the attack vector for 92,4% of detected malware. Device cloning (ID cards) requires a high level of specialization and the necessity to get closer to the victim to clone his/her ID. Two-factor identification has made this type of threat very unlikely.	AS-DA-01 Backup data AS-DA-03 Operation data AS-DA-04 System data AS-DA-06 Audit data AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-US-01 System users

High-level threat	Threat	Description	Affected assets
			AS-US-02 End users
	Insecure interfaces and APIs	A possibly existing Cloud computing environment provides user interfaces and APIs to interconnect devices and interact with the Cloud service. These interfaces offer an entry point for malicious attackers if they are poorly designed and lack security measures such as encryption and access control. Broken or hacked API's may result in data breaches.	AS-HW-04 H/W interface AS-OS-02 Native API AS-NE-02 Network interfaces
	Insider threat	Insiders can be current or former employees, contractors or other trusted partners who gain access from the inside of an organization. These parties have had authorized access and may negatively affect a possibly existing Cloud service, ultimately resulting in a data breach.	AS-US-01 System users AS-US-02 End users AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Denial of Service (DoS)	Denial of Service and/or Distributed Denial of Service (DoS/DDoS) attacks targeting the availability of any internet-exposed services hosted by payment network organization (banks, payment service providers, etc…) can affect online payment services. These attacks might affect transactions that require real-time access by payment applications to the payment services. They may also block the legitimate access for the consumers to their bank accounts and thwart online payments.	AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-OS-03 Hypervisor AS-OS-05 Containers/VMs

High-level threat	Threat	Description	Affected assets
		Payment Service Providers (PSPs) offer terminals for payments as well as aggregated payment services for merchants by processing data from different channels, including face-to-face (card present) payments, online payments and mobile/contactless payments. PSP payment gateways represent an interesting target for attackers that seek to compromise the payment data in transit from the merchants to the different acquiring banks. Attackers might seek to compromise software vulnerabilities, the payment gateways hosted at the payment service providers for instance, by exploiting unauthorized access to payment gateways and weaknesses in enforcement of internal payment service providers' security controls and measures.	AS-NE-01 Communication protocol AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W Payment systems
	Network-related technical failures or attacks	Technical failures of network-related components influence the availability of Cloud service. Examples include the loss of Internet connectivity due to failures at the Cloud customer's or service provider's site, a temporary reduction of network bandwidth at the Cloud customer's internet service provider, which affects the data transfer from and to the Cloud service provider, and disruptions in the global Internet routing infrastructure capping the connection between the Cloud customer and Cloud service provider.	AS-HW-03 Computational devices AS-OS-01 Embedded firmware AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W
System Failure	S/W failure	Any piece of software can have errors. The general rule is: all measures have to be taken so no overdose can be administered under any circumstance.	AS-HW-03 Computational device AS-OS-01 Embedded firmware AS-OS-02 Native API AS-OS-03 Hypervisor

High-level threat	Threat	Description	Affected assets
			AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS
	Outdated firmware	Firmware is a basic type of software that is embedded into every piece of hardware. It cannot be uninstalled or removed and is only compatible with the make and model of the hardware it is installed on.	AS-OS-01 Embedded system’s firmware AS-HW-03 Computational devices
	H/W failure	Failure of IT hardware at a customer's (or maybe a Cloud service provider's) site, limits the service's availability.	AS-HW-04 H/W interface AS-NE-03 Network H/W AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data

3.7 Threat Landscape for the Water Utilities’ Sector

Type of entities: Suppliers and distributors of water for human consumption

Suppliers and distributors of water for human consumption, i.e., water, whether in its natural state or after processing, intended for drinking, cooking, food preparation or other household use, regardless of its origin and whether supplied by a distribution network, by tank, or in bottles or container - but excluding the distributors for whom the distribution of water for human consumption is only part of their general activity of distributing other products and goods that are not considered basic services

Criteria:

For the water utilities and distribution sector and in particular for the respective basic drinking water supply and distribution service, the threshold is for the water company to supply drinking water to a population of more than T_3consumers per year or to distribute more than T_4cubic meters of water per year through its network (for Greece, $T_3 = 0.5\,million$ and $T_4 = 50million$)

In this section we are going to list only the cyber threats that pertain to the Industrial Control Systems (ICS) of the water and wastewater utilities [24][25][26][27][28].

Table 6: Threat landscape for the Water utilities sector

High-level threat	Threat	Description	Affected assets
Malicious actions	Malware injection attacks (e.g., ransomware)	Ransomware (victimizing 22.9 companies per minute) along with the phishing attacks (which victimize 1.5 companies per minute) top the list of the cyber threats that target the water supplies' control systems[12]. In this context, several attacks[13,14] have been performed with	

[12] Hermano, J. (2019). "Cybersecurity Risk & Responsibility in the Water Sector". Retrieved from: https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance

[13] New York Times (2018, May 27). "*A Cyberattack Hobbles Atlanta, and Security Experts Shudder*". Retrieved from: **https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html**

[14] Kumar, M. (2016, April 29). "*Ransomware virus shuts down Electric and Water Utility*". Retrieved from: https://thehackernews.com/2016/04/power-ransomware-attack.html

		detrimental effects especially concerning the environmental remediation costs[15,16].	Affects **NETWORK - H/W assets** (ICS) depending on the configuration
	Social Engineering (e.g. Spear Phishing)	Unlike traditional hacking methods, social engineering attacks exploit human behavior to gain access to company servers. *Spear Phishing* are attacks targeting specific individuals, in this case by sending emails personalized to the recipient that are (or appear to be) from a legitimate account and usually entice the recipient to click on a link that injects malware onto their systems. Spear phishing emails currently are the most prevalent method for delivering advanced persistent threat (APT) attacks. 84% of organizations have stated that a spear-phishing attack successfully penetrated their organization with an average impact of $1,6M per attack with those numbers constantly growing[17,18].	
	Denial of Service (DoS)	Denial of service attacks against the ICS overload its resources due to a flood of requests originating from many sources and cause its unavailability and inability to process requests.	
	Insider threat	Insiders can be current or former employees of water organizations, contractors, or other trusted partners, who gain access from the inside of an organization. These parties have or used to have authorized access and may negatively affect the functionality of the ICS if they want to.	

[15] See https://www.ajc.com/news/local/atlanta-network-almost-recovered-from-cyber-attack-cost-still-unkown/k6srGim85Q8dKwUFPbcDhN/

[16] Freed, B. (2018, April 10). "*Colorado has spent more than $1 million bailing out from ransomware attack*". Retrieved from: https://statescoop.com/colorado-has-spent-more-than-1-million-bailing-out-from-ransomware-attack/

[17] FireEye. "*Spear-Phishing Attacks: Why They Are Successful and How to Stop Them*". Retrieved from: https://www.fireeye. com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf

[18] See "*Why 2017's Phishing Attacks Teach Us All to Beware*," InfoSecurity Magazine, September 20, 2017, https://www.infosecurity-magazine.com/opinions/why-2017-phishing-attacks-teach/

System Failure	Outdated firmware	Lack of procedures in place to update firmware along with legacy systems and software offer backdoors which can be exploited by malicious actors to harm the ICS' functionality. In one water utility attack, cybercriminals exploited antiquated computer systems to gain access to the valve and flow operations and were able to manipulate the water flow and the amount of chemicals used to treat the water. Cybercriminals also accessed customer data via the company's online payment system, through which the attackers gained administrator credentials and maneuvered laterally through the network[19].	

3.8 Threat Landscape for the Transportation Sector

The transport domain is generally considered consisted of three sub-domains. Each sub-domains includes transportation of both people and goods.

3.8.1 Air transportation

Type of entities: Air transportation carrier and Airline and Airport management
Air carrier means an air transport undertaking which holds a valid license or equivalent. Airline and airport management companies and operators of ancillary facilities located within airports.

Criteria:
For the basic air transport service, the threshold is for the operator to have an annual passenger traffic of at least T_5 passengers or to handle more than T_6% of the annual total number of passengers at the airports of a member state.
For the basic service of Airport management and auxiliary facilities operations within the airport, the threshold is for the operator to manage an airport with an annual passenger traffic of at least T_7 passengers or to manage T_8% of the annual total flights of a member state.
For the basic air traffic management service, the threshold is for the administrator to operate an airport with a minimum annual number of passengers greater than T_9 passengers or T_{10}% of the total annual flights of a member state.

[19] *See: Verizon's Data Breach Digest (2016) p. 39-42.*

3.8.2 Railways

Type of entities: Railway infrastructure operators or railway operators

A railway infrastructure operator is any organization or company responsible for the operation, maintenance, upgrade and renovation of railway infrastructure on a network, as well as the responsibility for participating in its development, in accordance with the rules laid down by the member state.
A railway operator is any public or private licensed undertaking whose principal activity is the carriage of goods and/or passengers by rail, provided that such undertaking also provides traction.

Criteria:
For the basic railway infrastructure management service, the threshold is that the operator should manage infrastructure that serves more than T_{11} million passenger-kilometers or T_{12}million tonne-kilometers or to manage more than T_{13}% of the railway network infrastructure for a member state.
For the basic railway transportation services, the threshold is for the operator to manage a transport project of more than T_{14} million-passenger kilometers or T_{15} million tonne-kilometers or more than T_{16}% of the annual passenger-kilometers or more than T_{17}% of the tonne-kilometers of the railway network of a member state.

3.8.3 Water-sea transportation

Type of entities: Maritime transport companies, Port management, VTS operators

Inland waterway, sea and coastal passenger and freight transport companies as defined by the EU regulation for maritime transport, excluding individual ships used by these companies.
Port management bodies and companies that exploit port facilities or perform works/projects within ports, or use equipment located within ports.
Vessel Traffic Services operators.

Criteria:
For basic inland waterway, sea and coastal passenger and freight transport service, the threshold is for the carrier to carry at least T_{18} passengers per year or to carry at least T_{19} containers (TEUS) per year or to transport at least T_{20} trucks per year.

For the basic port management and operation service, including port facilities as well as the operation of works and equipment located within ports, the threshold is for the operator to operate a port carrying at least T_{21} passengers per year or transport at least T_{22}containers (TEUS) per year or transport at least T_{23} trucks per year.
For the basic Vessel Traffic Management (VTS) service, the threshold is for the operator to have supervised port(s) carrying at least T_{24} passengers per year or transporting at least or transporting at least T_{25} containers (TEUS) per year or transport at least T_{26} trucks per year.

3.8.4 Road transport

Type of entities: Road authorities or bodies that use ITS technologies

A road authority is any public authority responsible for the design, control or management of the road network which falls within its territorial jurisdiction.
A road operator is any public or private entity responsible for maintaining and managing the road network.
Operators of intelligent transport systems (ITS)

Criteria:
For the basic traffic management control service, the threshold is for the body (road authority) to be responsible for managing the traffic of motorways of at least T_{27} million kilometers per year or at least T_{28} average daily vehicle traffic per year or T_{29} kilometers of a national highway.
For the basic intelligent transport systems (ITS) service, the threshold is for the operator to be responsible for managing intelligent transport (ITS) systems of vehicles with traffic of at least T_{30} million kilometers per year or at least T_{31} average daily vehicle traffic per year.

In the following table, the threat landscape for the transport sector is presented [29][30][31].

Table 7: Threat landscape for the Transportation sector

High-level threat	Threat	Description	Affected assets
Natural and social phenomena	Earthquakes Fires Extreme weather Solar flare Volcano explosion Nuclear incidents Dangerous chemical incidents Pandemic Social disruptions	Large scale and large effects of natural disasters and social phenomena can have a different probability. Large scale natural disasters and rare social phenomena are infrequent but could impact the systems supporting critical business functions (e.g., destruction of an airport). Also, other sectors could be affected if transport infrastructure is not working properly due to calamities: (e.g., goods are not delivered in time or quality is altered)	All assets

	Shortage of fuel Space debris & meteorites	threat probability is low, but the impact might be huge.	
Supply chain failure	Internet service provider Cloud service provider (SaaS / PaaS / SaaS/Iaas/SecaaS) Utilities (power / gas / water) Remote maintenance provider Security testing companies	Third-party failure in the transport sector has a huge impact on the provisioning of services. This dependency is guided by safety reasons, operational and financial responsibilities, compliance with safety reasons, cybersecurity and technical standards, cost, and contractual obligations. Collaboration is vital; this means that a failure of a third party will surely impact negatively. e.g. in July 2016 the third-party failure, internet service provider failure at Rome's Fiumicino airport caused two hours of delay for the passenger checking operation[20] In the railway sector cloud services are now used to increase the capability of rail signaling: due to a growing volume of users, railways operators have to assess in the best way possible where to invest in enhancing their services. If no adequate measures, like access controls, redundancy and fallback computers in the datacenters, the security is compromised, also for users: e.g. self-driving vehicles that are not able to run close to each other in a safe manner can harm passengers and pedestrians.	AS-HW-02 Power supply AS-HW-03 Computational device AS-HW-04 H/W interface AS-HW-06 Storage AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-OS-03 Hypervisor AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-03 DBMS AS-US-01 System users AS-US-02 End users AS-US-03 Contractors AS-NE-03 Network HW AS-NE-04 Network SW AS-NE-03 Network controller Safety and security assets Facilities and maintenance assets

[20] Aeroporto di Fiumicino, ore di stop e code al check in per un guasto alla connessione, http://roma.repubblica.it/cronaca/2016/07/18/news/fiumicino_problema_tecnico_al_t3_code_per_i_controlli_arrivano_in_strada-144357812/?ref=HREC1-6.

Human errors	Unauthorized access control Unauthorized data access	**To ensure availability, integrity and confidentiality, access control procedures should be in place**: e.g., there is a high need for protection of the radio block centers (RBC) (railway sector) which in case of unauthorized access and also manipulation, can lead to the inoperability of trains or worst could produce consequence to the operational safety.	Potentially all the assets
	Non-compliance (BYOD)	The lack of control on BYOD makes these devices potentially dangerous for the infrastructure. These appliances should be kept off the perimeter of relevant servers and services. The access to the infrastructure's network should be regulated/secured by individual credentials associated with the device (for example, using digital certificates). Wherever possible, these devices should operate under a policy-based infrastructure while joining the airport IT domain or stations IT domain, giving a more restricted environment (i.e., restriction of peripherals usage via group policy).	AS-HW-03 Computational device AS-HW-05 I/O devices AS-SO-02 Application software AS-SO-03 DBMS AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data
	Configuration errors Operator/user error	Configuration errors or operator/user errors also have a negative impact: for example, system downtime, cancelled flights on smart airports could be caused by a failure or a missing secure setting of password on devices before they are deployed. The impact could also introduce major security weaknesses, or at worst, could potentially cause severe incidents involving users, e.g., self-driving vehicles. Lost hardware, such as laptops containing sensitive data or authentication details (passwords, or VPN certificates) can introduce vulnerability and lead to subsequent attacks.	Traffic and vehicle management, transportation safety and security, Sustainable urban mobility, Passenger safety and security Data protection and privacy Sales, fees and charges, Resilient management structures, Energy and environment
	Malware injection attacks (i.e. virus, ransomware, worms)	Malware potentially causes a huge impact on the whole infrastructure, as it acts maliciously in the	Safety and Security

		machine where it runs and often propagates through other connected systems. It can be spread in different ways, like SE, direct exploitation of software vulnerabilities or device tampering. The lately popular ransomware has already hit many stakeholders of the transport sector: in 2020 Adif, the Spanish Administrator of Railway Infrastructures, has been hit by a ransomware attack and personal and business data were exposed; Airbus Group is hit by up to twelve cyber-attacks each year and most of them are ransomware. Usually, the cause is vulnerabilities not patched in time	Airline/Airside Operations IT and Communications Passenger Management
Malicious actions	Denial of Service (DoS), Amplification / Reflection Flooding Jamming	The consequence of DOS is the outage of service, in a distributed environment, this threat (DDOS) can cause the outage of some cloud-based services: security check slow down, passenger delays, cancelled flights, loss of confidence, damages to company reputation, and/or financial damage. A DDOS attack on DSB ticketing systems in 2018 (Denmark), has affected approximately 15000 customers who were not able to buy tickets from ticket machines.	AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-OS-03 Hypervisor AS-OS-05 Containers/VMs AS-NE-01 Communication protocol AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W Traffic and vehicle management, transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment
	Social engineering attacks (Phishing Pretexting Untrusted links (fake websites / CSRF / XSS) Baiting Reverse social engineering Impersonation, Identity Theft)	Social engineering is the manipulation of people to divulging information or performing actions on behalf of the attacker. Social attacks are effective as they can bypass technical and physical controls. In general, employees who are not adequate security-aware and trained on these issues or do not follow procedures can pose a significant risk to the infrastructure cybersecurity; since the attackers may earn full access to the victims' accounts, identity, and authorization.	AS-DA-01 Backup data AS-DA-03 Operation data AS-DA-04 System data AS-DA-06 Audit data

		Successful attacks could result in data breaches, data leakage, or data theft.	AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-US-01 System users AS-US-02 End users IT and Communication
	Exploitation of software vulnerabilities	Vulnerabilities may exist in Smart airport systems or railway systems (in general in every type/sector system), as well as unknown security issues of the IT/smart assets, or issues for which patches have been created but not applied yet. Assets' vendors and transport infrastructure managers have to check if their systems are running with all the latest security patches, otherwise, they may be targets of sophisticated attacks. Also, the outdated firmware is part of this classification (see the section below).	AS-HW-03 Computational devices AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment
	Transport device tampering	Tampering of self-serving e-ticketing systems is an easy task since they are usually located in public spaces. Successful attacks can then result in the attacker having unauthorized access to the machine and	AS-HW-03 Computational device AS-HW-04 H/W interface

		potentially change expected behavior and also steal users' personal information.	AS-HW-05 I/O devices AS-HW-06 Storage AS-NE-02 Network Interface Passengers Management
	Insecure interfaces and APIs	A possibly existing Cloud computing environment in systems, of any sector, provides **user interfaces** and **APIs to interconnect devices** and interact with the Cloud service. **These interfaces offer an entry point for malicious attackers** if they are poorly designed and lack security measures such as encryption and access control. Broken or hacked API's **may result in data breaches**.	AS-HW-04 H/W interface AS-OS-02 Native API AS-NE-02 Network interfaces
	Insider threat (Stealing information or manipulation of data, Sales of important data to competitors, Leaking information)	Insiders **can be current or former employees**, **contractors** or **other trusted partners** who gain access from the inside of an organization. These parties have had authorized access and may negatively affect a possibly existing Cloud service, ultimately resulting in a data breach.	AS-US-01 System users AS-US-02 End users AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data Traffic and vehicle management, Transportation safety and security, Resilient management structures
	Intercepting data in transit (Man-in-the-middle attack)	In a possibly existing Cloud architecture model, **data** is **transferred from the Cloud customer to the Cloud service provider**. During the transition, it **may be intercepted** and eventually result in a data breach.	AS-DA-01 Backup data AS-DA-03 Operation data AS-DA-04 System data
	Network-related technical failures or attacks	Poorly configured filtering devices such as firewalls or generally weak network security can often allow attackers to open backdoors and exploit vulnerabilities. An attacker can then have access to unauthorized data and functions or may upload malicious software or launch malicious commands.	AS-HW-03 Computational devices

			AS-OS-01 Embedded firmware AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-NE-02 Network interface AS-NE-03 Network H/W AS-NE-04 Network S/W
System Failure	S/W failure (Failure on parts of devices, failure of devices or systems, disruptions of communication links, disruptions of main supply, disruptions of service providers, disruptions of the power supply, failures of hardware, and software bugs)	Impact on the security posture and operational capacity of the infrastructure are the outcomes of system failure. Infrastructure systems' managers should have to ensure certain critical functions at a minimum level or at least they have to define a recovery protocol.	AS-HW-03 Computational device AS-OS-01 Embedded firmware AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment
		In particular subsectors, such as railways, some components/systems were developed according to state-of-the-art security measures but it is difficult to	

	Outdated firmware	keep them up-to-date and they eventually become obsolete and potentially vulnerable. Furthermore, these systems are usually spread across the network (stations, track, etc.), making it difficult to comprehensively control cybersecurity.	AS-OS-01 Embedded system's firmware AS-HW-03 Computational devices AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data Traffic and vehicle management, Transportation safety and security, Sales, fees and charges, Resilient management structures, Energy and environment

3.9 Threat Landscape for the Energy Sector

The energy domain is generally considered consisted of three sub-domains: electricity, oil and gas.

3.9.1 Electricity

Type of entities: Electricity companies, distribution network operators, transmission system operators

Electricity company: entity (private or public) that carries out at least one of the following activities: generation, transmission, distribution, supply, or purchase of electricity and it is responsible for commercial and technical tasks and/or maintenance tasks related to these activities.

Distribution network operator: entity (private or public) that is responsible for the operation, maintenance, provision of access to end-users and power plant companies and, if necessary, the
development of the distribution network in a given area and, its interconnections with other distribution networks and transmission

systems, as well as the long-term capacity of the network to meet the reasonable demand for electricity distribution services.

Transmission system operator: entity (private or public) that is responsible for the operation, maintenance and, if necessary, development of the transmission system in a given area and, when necessary its interfaces and interconnections with other systems, as well as the long-term ability of the system to meet the reasonable demand for electricity transmission services.

Criteria:

For the basic electricity supply service, the criterion is for the operator to supply electricity to more than T_{32}% of the total number of customers of the electricity distribution network or to have more than T_{33} customers or to supply the national electricity transmission system with power units of at least T_{34} GW.

For the basic electricity distribution service, the criterion is for the operator to supply electricity to more than T_{35} % of the total distribution network customers or to have more than T_{36} customers connected to the electricity distribution network.

For the basic electricity transmission service, the criterion is for the operator to manage at least T_{37} % of the GWh that are moved annually from the national electricity transmission system, or to manage more than T_{38} GWh that are moved annually from the national electricity transmission system,

3.9.2 Oil

Type of entities: Oil pipeline operators, operators of oil production

Oil pipeline operators: entities (public or private) that are responsible for the management, operation, maintenance and, if necessary, development of oil pipelines.
Operators of oil production: entities (public or private) involved in the production, refining, maintining refining facilities, storage and transportation of oil.

Criteria:

For the basic oil pipeline service, the criterion is for the operator to operate a pipeline or pipelines with capacity of more than T_{39} million cubic meters of oil per year.

For the basic service of production, refining, processing, storage and transportation of oil, the criterion for the operator is per case:

- To manage the production of more than T_{40}% of the country's annual oil needs or at least T_{41} million cubic meters of oil;
- To operate refining and processing facilities with a refining capacity of more than T_{42}% of the country's annual oil needs or at least T_{43} million cubic meters of oil;

- To manage the transportation of more than T_{44}% of the annual oil needs of the country or at least T_{45} million cubic meters of oil.

3.9.3 Gas

Type of entities: gas companies, distribution system operators, transmission system operators, operators of storage facilities, operators of gas refining and processing facilities:

Gas company: entity (public or private) that carries out at least one of the following activities: production, transport, distribution, supply, purchase, temporary storage and regasification of Liquid Natural Gas (LNG) and is responsible for commercial and technical taks and/or maintenance tasks related to these activities. This definition does not include Customers who purchase natural gas for their own use.

Gas distribution operators: entity (public or private) responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long term ability of the system to meet reasonable demands for the distribution of natural gas.

- Gas Transmission System Operator: entity (public or private) who carries out the work of gas transmission and is responsible for the operation, maintenance and, if necessary, the development of the gas transmission system in a given area and, where applicable, its interconnections with other systems, and to ensure the long-term ability of the system to meet the reasonable demands for natural gas transmission.
- Gas storage operators: entity (public or private) responsible for operating an installation used for gas storage. Storage Facilities are also considered the installation of Liquid Natural GAS (LNG) storage with with the exception of those used for temporary storage, regasification of the LNG and its injection into a natural gas transmission system
- Operators of gas refining and processing facilities.

Criteria:

For the basic gas supply service towards a national gas transmission system, the criterion is for the operator to inject into the national gas transmission system more than T_{46} billion cubic meters of natural gas or to inject more than T_{47}% of gas in the national gas transmission system.

For the basic gas distribution service, the criterion is for the operator to distribute gas to more than T_{48}% of the total number of customers or to have more than T_{49} customers connected to its gas distribution network or its jurisdiction to cover the boundaries of a geographical region (defined by the authorities of a country).

For the basic gas transmission service, the criterion is for the operator to manage at least T_{50}% or T_{51} million cubic meters of natural gas moved through the national gas transmission system.

For the basic gas storage service, the criterion is for the operator to have storage facilities with a capacity of more than T_{52} cubic meters of liquefied natural gas (LNG).

For the basic LNG systems management service, the criterion is for the operator to have the technological capacity to provide more than T_{53}% of the annual movement or T_{54} million cubic meters of natural gas per year into the national gas transmission system.

For the basic gas supply service to consumers, the criterion is for the operator to have more than T_{55}% of the total gas distribution network customers or to have at least T_{56} customers connected to the gas distribution network.

For the basic gas refining and processing service, the criterion is for the operator to have the capacity to refine and process at least T_{57} billion cubic meters of natural gas.

In the following table, the threat landscape for the energy sector is presented

Table 8: Threat landscape for the Energy sector

High-level threat	Threat	Description	Affected assets
Damage/Loss	Loss of devices, media and documents Information leakage	Loss of devices, media and documents involves rummaging through disposed magnetic media for retrieving sensitive data that is left behind on it. (etc. unauthorized people might get access to data related to Advanced Metering Infrastructure (AMI) communication.) Attacks of Information leakage target various smart grid components with the aim to acquire private sensitive information. (energy consumption, credit cards, session data, access control data)	All assets
Eavesdropping /Interception /Hijacking	Interfering radiation	This threat aims at performing unauthorized interception of private communication, thus enabling the possession of data related to AMI from unauthorized people.	AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW) AS-OS-04 Operating System

High-level threat	Threat	Description	Affected assets
			AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-05 Test Data AS-DA-06 Audit Data AS-HW-03 Computational Device AS-HW-04 HW Interface AS-HW-05 I/O Devices AS-SO-03 Database Management Systems
	Session hijacking	Interactions between AMI components and infrastructure might be jeopardized in smart grid systems. This might eventually lead to unauthorized access to AMI communication information, AMI data alteration, denial of service to authorized users, and repudiation of actions.	AS-US-01 System Users AS-US-02 End Users AS-NE-01 Communication Protocol AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-SO-03 Database Management Systems AS-SO-02 Application Software AS-OS-04 Operating System

High-level threat	Threat	Description	Affected assets
	MITM-Attack	In this type of threat an attacker performs a Man-in-the-Middle (MITM) attack on communication between any of the processes, data stores, or external interactors in the grid.	AS-US-01 System Users AS-US-02 End Users AS-NE-01 Communication Protocol AS-DA-01Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-SO-03 Database Management Systems AS-SO-02 Application Software AS-OS-04 Operating System
	Network reconnaissance and information gathering	Information gathering attacks of mobile communication (in particular 802.16e) may target the Advanced Encryption Standard (AES) cipher.	AS-DA-01 Backup Data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW) AS-US-01 System Users AS-US-02 End Users AS-NE-01 Communication Protocol
	Replay of messages		AS-US-01 System Users

High-level threat	Threat	Description	Affected assets
		This threat assumes that an attacker knows the DNS value and can send a false acknowledgement messages to mislead the sender claiming that the receiver has received the message when, in fact, it hasn't.	AS-US-02 End Users AS-NE-01 Communication Protocol AS-SO-01 Web-Based Services AS-DA-06 Audit Data
	Interception of information	Interception of information could affect several networks, such as WiFi, Zigbee and fixed networks, by: ▪ Hijacking the meter connection. ▪ Intercepting the information by side-channel attacks. ▪ Intercepting and examining messages in order to deduce information from patterns in communication. ▪ Capturing and analysing the messages transmitted over the network.	AS-US-01 System Users AS-US-02 End Users AS-HW-01 Sensors /Actuators Hardware AS-HW-03 Computational Device AS-HW-06 Storage AS-HW-04 HW Interface AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-SO-01 Web-Based Services AS-SO-03 Database Management Systems AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW)

High-level threat	Threat	Description	Affected assets
Failures/ Malfunction	Failure of devices and systems	ENISA has confirmed that a significant amount of incidents will be attributed to failures, misconfiguration and errors due to the complexity of smart grids and the multiplicity of devices and systems.	AS-HW-01 Sensors/Hardware AS-HW-02 Power supply AS-HW-03 Computational Device AS-HW-04 HW Interface AS-HW-05 I/O Devices AS-HW-06 Storage AS-OS-01 Embedded Systems Firmware AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating System AS-US-01 System Users
	Failure or disruption of communication links (communication networks)	Attacks abusing implementations of standards are based on missing or weak implementations of security mechanisms.	AS-NE-01 Communication Protocol AS-NE-03 Network Controller (HW) AS-SO-02 Application Software AS-OS-03 Hypervisor AS-OS-04 Operating System AS-DA-01Backup Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data
	Spear Phishing	Spear phishing is an email scam targeting a specific individual, organization or business. It aims at stealing	

High-level threat	Threat	Description	Affected assets
Nefarious Activity/Abuse		data for malicious reasons and install malware on the computer of a targeted person.	AS-SO-01 Web-based services AS-SO-02 Application S/W AS-SO-03 DBMS AS-DA-03 Application data AS-DA-04 System data (Logs) AS-US-01 System users AS-US-02 End users
	Brute force	Brute force attacks are used to steal a company's intellectual property for the purpose of industrial espionage.	AS-US-01 System Users AS-US-02 End Users AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW) AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-01 Backup Data AS-DA-06 Audit Data AS-SO-03 Database Management Systems
	IoT Botnet	An IoT botnet targeting high-wattage devices could enable cybercriminals to launch a large-scale, coordinated attack on the power grid.	AS-HW-02 Power supply AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW)

High-level threat	Threat	Description	Affected assets
			AS-NE-04 Network Stack (SW) AS-OS-04 Operating System AS-SO-01 Web-Based Services AS-US-01 System Users AS-US-02 End Users
	Botnets	Botnets are malicious networks computers, connected to the Internet. The basic function of botnets consists of the following: Try to infect as many unsuspecting users as possible, taking advantage of possible vulnerabilities in their system, with the aim of stealing personal data, the money laundering and large-scale attacks.	AS-US-01 System Users AS-US-02 End Users AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data AS-SO-01 Web-Based Services AS-SO-02 Application Software AS-SO-03 Database Management Systems AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces AS-NE-04 Network Stack (SW) AS-OS-05 Containers / VMs

High-level threat	Threat	Description	Affected assets
	Ransomware	Ransomware is a type of malware that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid.	AS-OS-04 Operating System AS-OS-01 Embedded Systems Firmware AS-OS-02 Native API AS-OS-05 Containers / VMs AS-US-01 System Users AS-US-02 End Users AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data AS-SO-01 Web-Based Services AS-SO-02 Application Software AS-SO-03 Database Management Systems AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces AS-NE-04 Network Stack (SW)
	Malicious code /Activity/ Malware	These threats affect smart grid as the operation of all involved IT components depends on the installed software. In detail, this threat consists of the following attacks: ▪ Exploit kits ▪ Worms	All assets

High-level threat	Threat	Description	Affected assets
		▪ Trojans ▪ Backdoors/trapdoors ▪ Service Spoofing ▪ ICMP-flooding	
	Unauthorized access to information system / network, Social Engineering, Password Pilfering	▪ Disclosure of information is an attack whereby information is being disclosed to unauthorized entities. ▪ Password guessing, password sniffing, dictionary attacks, and social engineering are common methods used for password attacks. ▪ Social engineering is a method to penetrate a system using social skills, rather than technical attacks. ▪ Unauthorized access to systems/network, can be obtained/gained from different locations of the smart grid (etc. Customer endpoint, Remote access, Remote access or physical access to the network, Compromise RTU and send commands directly to controller).	Potentially all the assets
	Manipulation of information	This threat includes all kinds of manipulative activity regarding smart grid information, in particular AMI data and repudiation related information (e.g. AMI data, pricing information, invoicing information, etc.). This threat relates to information of all software used, but also certificates.	AS-DA-01 Backup data AS-DA-02 Configuration data AS-DA-03 Operation data AS-DA-04 Log data AS-DA-06 Audit Data AS-OS-01 Embedded Systems Firmware AS-OS-02 Native API AS-OS-04 Operating System AS-OS-05 Containers / VMs AS-SO-01 Web-Based Services AS-SO-02 Application Software AS-SO-03 Database Management Systems AS-HW-01 Sensors/

High-level threat	Threat	Description	Affected assets
			Actuators Hardware AS-HW-02 Power supply AS-HW-03 Computational Device AS-HW-04 HW Interface AS-OS-04 Operating System AS-NE-01 Communication Protocol AS-US-01 System Users AS-US-02 End Users
	Misuse of information/Information Systems	In the absence of end-to-end encryption, a compromised data concentrator can be misused to monitor data of other customers.	AS-US-02 End Users AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-SO-03 Database Management Systems AS-DA-01 Backup Data AS-DA-06 Audit Data
Physical attack	Fraud	In a reverse engineering attack, a customer can achieve reduction of energy bills by using information freely available from the AMI meter vendor or the standard used within AMI meters to reset the meter and reprogram it to report false information. If such information is not freely available, an attacker could reverse-engineer a meter to develop a way to modify it.	AS-HW-01 Sensors/Actuators Hardware AS-HW-03 Computational Device AS-HW-04 HW Interface AS-HW-05 I/O Devices AS-US-01 System Users

High-level threat	Threat	Description	Affected assets
			AS-US-02 End Users AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces AS-SO-03 Database Management Systems AS-OS-02 Native API AS-OS-04 Operating System AS-OS-05 Containers / VMs AS-OS-01 Embedded Systems Firmware
Spoofing	Control input spoofing	In this type of threat an attacker sends control input to a process, pretending it originates from a legitimate source (such as Windmill Process, Substation Process, IED Process, Automatic Voltage Regulator Process, Circuit breaker Process, Onload Tap Changer Process, Remote Terminal Unit (RTU) Process, and virtual RTU Process). As a result the attacker can cause a process responsible for controlling the grid to behave in a malicious way.	AS-OS-01 Embedded Systems Firmware AS-OS-02 Native API AS-OS-04 Operating System AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-HW-01 Sensors/ Actuators Hardware AS-HW-02 Power Supply AS-HW-03 Computational Device AS-HW-04 HW Interface

High-level threat	Threat	Description	Affected assets
	Spoofing the source	In this type of threat an attacker pretends to be a legitimate process, data store, or external interactor. This could lead to unauthorized access to a process or to incorrect data being sent to a process.	AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data AS-OS-04 Operating System AS-US-01 System Users AS-OS-05 Containers / VMs AS-NE-01 Communication Protocol
	Spoofing the target	In this type of treat an attacker pretends to be a legitimate process, data store, or external interactor. This could lead to information being sent to the attacker instead of the legitimate process.	AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-05 Test Data AS-DA-06 Audit Data AS-OS-04 Operating System AS-US-02 End Users
	Spoofing of data store source	In this type of treat an attacker sends malicious data to a process by pretending to be a legitimate data store. This could cause the process to behave in a malicious way by tricking it into basing decisions on false data.	AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data

High-level threat	Threat	Description	Affected assets
			AS-OS-04 Operating System
	Reuse of authentication tokens	In this type of treat an attacker acquires cryptographic keys from a legitimate IoT Device Process or an IoT Field Gateway Process in order to use them to communicate with an IoT Field Gateway Process or an IoT Cloud Gateway Process. This enables the attacker to send false data to the process or receive data meant for someone else.	AS-OS-04 Operating System AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data AS-DA-01 Backup Data AS-NE-01 Communication Protocol AS-SO-03 Database Management Systems AS-SO-02 Application Software
	GPS spoofing	In this type of treat an attacker sends false GPS signals to a PMU Process. PMUs generally rely on GPS to timestamp their measurements. These measurements may later be used for state estimation, and a successful GPS spoofing attack may cause the grid operators to estimate a wrong state.	AS-US-01 System Users AS-OS-04 Operating System AS-SO-03 Database Management Systems AS-DA-06 Audit Data
	Replay attack	In this type of treat an attacker captures a message from the network and resends it at a later time. This attack is possible if the data flow does not provide replay protection.	AS-US-01 System Users AS-US-02 End Users AS-NE-01 Communication Protocol AS-SO-01 Web-Based Services AS-DA-06 Audit Data AS-NE-02 Network Interfaces

High-level threat	Threat	Description	Affected assets
Tampering	Tampering of communication	In this type of treat an attacker interferes with a data flow and as a result the target stores false values in its database or otherwise behaves in a malicious manner. The threat is not manifested if the communication provides integrity.	AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data AS-OS-04 Operating System AS-SO-03 Database Management Systems AS-NE-01 Communication Protocol
	Injection of data in optical fiber	In this type of treat an attacker injects data into communication over optical fiber. The threat is related to communication with DERs via fiber optical cables.	AS-HW-01 Sensors/ Actuators Hardware AS-HW-02 Power supply AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data AS-OS-04 Operating System AS-SO-03 Database Management Systems AS-NE-01 Communication Protocol
	SQL injection attack	In this type of treat an attacker performs an SQL attack on an SQL relational database that does not sanitize	AS-SO-03 Database

High-level threat	Threat	Description	Affected assets
		input. An SQL injection attack may corrupt the database content or reveal the content to the attacker.	Management Systems AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-05 Test Data AS-DA-06 Audit Data
	Corruption of data store by tampering of data flow	In this type of treat an attacker interferes with a data flow going to a data store. The consequence of such an attack is that false data is stored in the data store.	AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data AS-SO-03 Database Management Systems AS-HW-06 Storage
Repudiation	Repudiation of sent/received data	This is the threat of not identifying if a process or data storage sent or received a message. Due to a lack of such proof, it may be difficult to investigate attacks or deny false claims motivated by financial gain. If the activities on the database or data storage are logged, the threat is not manifested.	AS-SO-03 Database Management Systems AS-NE-01 Communication Protocol AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data

High-level threat	Threat	Description	Affected assets
			AS-DA-04 System Data AS-DA-05 Test Data AS-DA-06 Audit Data AS-HW-06 Storage
	Repudiation of actions on smart grid process	This is the threat of not being able to prove whether an action was committed on a process or not. This can lead to repudiation claims after an attack and make it harder to attribute an attack to an actor.	AS-OS-04 Operating System AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-US-01 System Users AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces
Information Disclosure	Data flow sniffing	In this type of treat an attacker learns the contents of a data flow in the grid. If the flow does not offer confidentiality, this could lead to theft of confidential information or be used to reverse engineer commands in preparation for a later attack.	AS-SO-03 Database Management Systems AS-NE-01 Communication Protocol AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-05 Test Data AS-DA-06 Audit Data AS-OS-01 Embedded Systems Firmware

High-level threat	Threat	Description	Affected assets
			AS-OS-04 Operating System
	Wiretapping of fiber optic cables	In this type of treat an attacker wiretaps optical fiber cables to obtain the content of the communication. If the flow does not offer confidentiality, the consequences are the same as for the data flow sniffing threat.	AS-HW-01 Sensors/ Actuators Hardware AS-HW-02 Power supply AS-HW-03 Computational Device AS-HW-04 HW Interface AS-DA-04 System Data AS-SO-03 Database Management Systems AS-NE-01 Communication Protocol AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data
	Exploitation of weak credential transit	In this type of treat an attacker snifs credentials as they are transmitted to processes or data stores. If transmitted credentials are not encrypted, they may be sniffed and used to obtain elevated privileges.	AS-HW-06 Storage AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data

High-level threat	Threat	Description	Affected assets
			AS-NE-01 Communication Protocol AS-SO-03 Database Management Systems
	Exploitation of weak credential storage	In this type of treat an attacker obtains credentials from a data store. Such credentials may be used to obtain elevated privileges.	AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data AS-SO-03 Database Management Systems AS-OS-03 Hypervisor AS-OS-04 Operating System
Denial of Service	Denial of Service	These attacks attempt to make smart grid resources unavailable to its intended users.	AS-HW-01 Sensors/ Actuators Hardware AS-HW-02 Power supply AS-HW-04 HW Interface AS-HW-05 I/O Devices AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-OS-04 Operating System AS-NE-02 Network Interfaces

High-level threat	Threat	Description	Affected assets
			AS-NE-03 Network Controller (HW) AS-NE-04 Network Stack (SW)
	Distributed denial of service	This is the threat of distributed attack from an external network on the availability of a process. Such an attack may cause the target to become momentarily inaccessible to legitimate communication from other sources. This threat deals with generating large amounts of traffic, possibly from distributed hosts.	AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW) AS-NE-04 Network Stack (SW) AS-OS-04 Operating System AS-US-01 System Users AS-US-02 End Users AS-HW-01 Sensors/Actuators Hardware AS-HW-02 Power supply AS-HW-03 Computational Device AS-HW-04 HW Interface AS-HW-06 Storage
	Smart meter-based DDoS attack on AMI server	In this type of treat an attacker compromises many smart meters and subsequently uses them for a DDoS attack on an AMI Server. Such an attack could cause the AMI server to become unavailable.	AS-HW-01 Sensors/ Actuators Hardware AS-HW-02 Power supply AS-HW-03 Computational Device AS-HW-04 HW Interface AS-OS-01 Embedded

High-level threat	Threat	Description	Affected assets
			Systems Firmware AS-OS-04 Operating System
	Denial of service through specially crafted message	In this type of treat an attacker targets the functional availability of a circuit breaker using a specially crafted package. (According to Slowik[36], an attempt was made in the 2016 Ukraine attack to place a safety breaker in a firmware update mode, leaving it in a state unable to perform its normal function. The attack attempted this by exploiting a vulnerability in the device by sending it a specially crafted UPD packet.)	AS-SO-01 Web-Based Services AS-SO-03 Database Management Systems AS-HW-02 Power supply AS-HW-03 Computational Device AS-HW-04 HW Interface AS-HW-01 Sensors /Actuators Hardware AS-OS-01 Embedded Systems Firmware
	Signal jamming	In this type of treat an attacker jams the wireless communication between processes, data stores or external interactors in the grid. The threat concerns communication with a DER.	AS-SO-03 Database Management Systems AS-US-01 System Users AS-US-02 End Users AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces AS-HW-06 Storage AS-DA-01 Backup Data AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data

High-level threat	Threat	Description	Affected assets
			AS-DA-04 System Data AS-DA-06 Audit Data
	Protocol-specific flooding	In this type of treat an attacker targets the network availability of components using a specific protocol (e.g., TCP or UDP) and can cause the components to become unresponsive for a period.	AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW) AS-NE-04 Network Stack (SW) AS-NE-01 Communication Protocol AS-OS-01 Embedded Systems Firmware AS-OS-04 Operating System AS-SO-01Web-Based Services AS-SO-02 Application Software AS-SO-03 Database Management Systems
	Interruption of data flow	In this type of treat an attacker disrupts the data flow, attacking the network availability of the target.	AS-SO-03 Database Management Systems AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW) AS-NE-04 Network Stack (SW)
	Denial of service of data store	In this type of treat an attacker makes the data store inaccessible.	

High-level threat	Threat	Description	Affected assets
			AS-SO-03 Database Management Systems AS-HW-06 Storage AS-DA-01 Backup Data AS-DA-06 Audit Data
Elevation of Privilege	Elevation of privilege in database due to poor configurations	In this type of treat an attacker obtains greater privileges than intended in a database. This threat is generated if access to a database is not configured based on least privilege. Least privilege implies that a user does not have more permissions than what is needed.	AS-SO-03 Database Management Systems AS-DA-06 Audit Data
	Execution of malware	In this type of treat an attacker executes malware in a process (execution of malware has been observed in the Triton[37], Crashoverride[36], and Stuxnet[39] attacks on Industrial Control Systems).	Probably will affect all assets.
	Exploitation of publicly disclosed vulnerabilities	In this type of treat an attacker exploits a publicly disclosed vulnerability in a process or a data store in order to obtain elevated privileges. Vulnerabilities are continuously discovered and disclosed. Failure to update systems after such vulnerabilities have been made publicly known lowers the effort for conducting an attack (According to Slowik[38], an example of this can be found in the 2016 Ukrainian attack). The threat is generated for IoT Devices or IoT Gateways.	AS-SO-03 Database Management Systems All Assets
	Exploitation of unused services or features	In this type of treat an attacker exploits unnecessary functionality in order to access and obtain elevated privileges on a process or data store. The threat is adapted from the Azure Cloud Service template, where it is included for IoT devices and IoT gateways. An example of such services may be open ports, as identified in threat ICS-CERT[40] recommends that	AS-SO-03 Database Management Systems

High-level threat	Threat	Description	Affected assets
		ports are closed and unused services turned off. Staggs et al.[41] argue that system hardening can be used as a mitigation technique which include disabling unnecessary remote interfaces, removing unused interfaces and functionality, and adjusting default configurations to fit the operating environment.	AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-05 Test Data AS-DA-06 Audit Data AS-OS-01 Embedded Systems Firmware AS-OS-04 Operating System
	Exploitation of lack of input validation	In this type of treat an attacker gives malicious input to a process or data store in order to obtain elevated privileges. A well-known form of such a threat is a buffer overflow attack.	AS-SO-03 Database Management Systems AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-DA-06 Audit Data AS-OS-01 Embedded Systems Firmware AS-OS-04 Operating System
	Unauthorized access through vendor VPN	In this type of treat an attacker obtains access to a process through a vendor VPN. This threat is related to DERs and on the Crashoverride attack.(ICSCERT[40] reports that a VPN connection may have been used by attackers to open circuit breakers in the 2015 Ukraine attack.)	AS-SO-03 Database Management Systems AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data

High-level threat	Threat	Description	Affected assets
			AS-DA-05 Test Data AS-DA-06 Audit Data AS-OS-01 Embedded Systems Firmware AS-OS-04 Operating System AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW)
	Unauthorized execution of commands	In this type of treat an attacker executes unauthorized commands on a process or data store. The threat is included for IoT related communication.	AS-US-01 System Users AS-SO-03 Database Management Systems AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-OS-01 Embedded Systems Firmware AS-OS-04 Operating System AS-NE-01 communication Protocol AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW)

High-level threat	Threat	Description	Affected assets
	Exploitation of weak authentication	In this type of treat an attacker obtains elevated privileges on a process or data store due to weak authentication mechanisms. This can be the case if the authentication mechanism consists of easily guessable credentials or factory default credentials.	AS-SO-03 Database Management Systems AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-OS-01 Embedded Systems Firmware AS-OS-04 Operating System AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces AS-NE-03 Network Controller (HW)
	Remote control of circuit breakers	In this type of treat an attacker obtains control of a remote circuit breaker in the grid. (This threat is inspired by the 2015 Ukraine attack where ICS-CERT[40] reports that the attackers opened circuit breakers in the grid. Malware containing this functionality was also identified in the 2016 Crashoverride attack[36]).	AS-SO-03 Database Management Systems AS-DA-02 Configuration Data AS-DA-03 Operation Data / Application Data AS-DA-04 System Data AS-OS-01 Embedded Systems Firmware AS-OS-04 Operating System AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces

High-level threat	Threat	Description	Affected assets
			AS-HW-01 Sensors/ Actuators Hardware AS-HW-02 Power supply AS-HW-03 Computational Device AS-HW-04 HW Interface AS-NE-03 Network Controller (HW)

3.10 Threat Landscape for the Digital Infrastructures

In this section, the threat landscape for the Digital Infrastructures is provided. With the term digital infrastructure, a more generic set of entities is described besides the DSPs. Thus, our analysis extends beyond the DSP context (i.e. the online marketplace, online search engine and cloud computing service). More specifically, the following entities are considered:

- Internet Exchange Points (IXP)
- Domain Name System (DNS) Servers
- Top-Level Domains (TLD)
- Internet Service Providers
- Mobile operators
- Content delivery networks
- Cloud service providers
- Marketplaces,
- Search engines.

As reference to the investigation of the threat landscape, a plethora of reports from ENISA was used, namely: [12],[13], [14], [15], [50], [51], [52], [53], [54], [55]. However, it must be noted that most of the content of Table 9 has been influenced by the analysis in [50]. This is due to the fact that the 5G networks are currently the technology edge in digital infrastructure, since they include:

- Cloud computing,
- Virtualization,
- Multi-site deployment,
- Multiple access networks,
- Variaty of server and services,
- They constitute Internet infrastructure,
- Supports IoT and provides services to OESs.

and more.
In the following table, the threat landscape for the digital infrastructures is presented.

Table 9: Threat landscape for Digital Infrastructure

High-level threat	Threat	Description	Affected assets
Disasters	Natural disasters	Large scale and large effects of natural disasters and social phenomena can have a different probability. Large scale natural disasters and rare social	All assets

		phenomena are infrequent but could impact the systems supporting critical business function	
	Environmental disasters	Large scale and large effect catastrophic event regarding the natural environment that is due to human activity.	All assets
	Terrorist attack against infrastructure	Act of terrorism in the physical resources of the digital infrastructure.	All assets
Physical Attacks	Sabotage/vandalism of network infrastructure	Threats related to actions taken by actors aimed at destroying, disabling or stealing physical assets supporting the digital infrastructure. A physical attack to critical assets may disrupt, interfere and ultimately cause unavailability of the provided service.	AS-HW-03 Computational Device AS-HW-02 Power supply AS-HW-05 I/O devices AS-NE-03 Network controller
	Sabotage/vandalism of computational infrastructure		AS-HW-01 Sensors/Actuator s AS-HW-03 Computational Device AS-HW-02 Power supply AS-HW-05 I/O devices AS-HW-06 Storage AS-NE-03 Network controller
	Theft of physical assets	Self-explanatory	AS-HW-01 Sensors/Actuator s AS-HW-02 Power Supply AS-HW-03 Computational device AS-HW-05 I/O Devices AS-HW-06 Storage AS-NE-03
	Unauthorized physical access to based stations in shared locations	Modern digital infrastructure may include functional nodes and stations installed in remote locations that cannot be monitored continuously or protected by means of physical security. These stations are prone to physical attacks.	AS-HW-01 Sensors/Actuator s AS-HW-02 Power Supply AS-HW-03 Computational device AS-HW-05 I/O Devices

			AS-HW-06 Storage AS-NE-03
	Fraud by digital infrastructure employees	Malicious insiders exploit their access rights to cause service/network unavailability, intentional data/information destruction, or data/software tampering.	All assets
Unintentional damages	Misconfigured or poorly configured systems/networks	The exploitation of a misconfigured system that in essence is from an unintentional nature, creates the opportunity for a threat actor to reach critical assets in the infrastructure or stage an attack. Configuration flaws may happen at different stages of the solution implementation life-cycle such as product installation and maintenance. Examples include poorly configured APIs, network functions, access control rules, network slices, administration rights, virtualized environments, orchestration software, firewalls, etc.	AS-OS All System Software AS-NE All Network assets AS-SO All software assets
	Inadequate designs and planning or lack of adaption	Threats related to issues arising from the multiple options and features that a service or technology has to offer. The level of complexity and the difficulty to reach an optimal architecture, adequate security and operating procedures may lead to poor design and implementation.	All assets
Failures or malfunctions	Erroneous use or administration of the network, systems and devices	Failure in software operation, service and application functionalities or HW/device operation due to erroneous configuration, or admin commands.	AS-OS all system software assets All-SO all software assets AS-NE-02 Network Interfaces AS-NE-03 Network Controller AS-HW-01 Sensors/Actuators AS-HW-03 Computational device AS-HW-04 HW interface AS-HW-05 I/O device
	Information leakage/sharing due to human error	Unintentional data leakage from mis-configuration or unintentional provision of access rights.	AS-DA all data assets
	Data loss from unintentional deletion	Self-explanatory.	AS-DA all data assets
	Failure of the network, devices or systems	Malfunction in the operation of networks and system nodes.	AS-HW all hardware assets AS-OS all system software assets AS-NE-02 Network Interfaces

			AS-NE-03 Network controller
	Failure or disruption of communication link	Malfunction in the communication link or used network service.	AS-NE all network assets
	Failure or disruption of main power supply	Loss of electricity can be of importance since it can disable all physical equipment in a given area. Power supply can also affect cloud service availability.	AS-HW all hardware assets
	Failure or disruption from service providers	Failure of a vendor to deliver a hardware/software/network product as intended Disruption of operation due to erroneous update or failed configuration by the service provider.	All assets
	Malfunction of equipment (devices or systems)	Malfunction-failure in the equipment	AS-HW all hardware assets AS-OS all system software assets
Outages	Loss of resources	The threat refers to outage of human resources or physical resources to support and operated the digital infrastructure.	AS-HW all hardware assets AS-US-01 system users AS-US-03 Contractors
	Support services	The threat is realized when there is no availability of support services necessary for the proper operation of the system. The threat refers to lack of human assets, management processes, polices, legal support and more.	AS-US-01 system users AS-US-03 Contractors
	Data network	The resources made available by the data network, the core network, the access network, or the local or virtual networks used to access the infrastructure services are not sufficient to serve the requested traffic load.	AS-NE-01 Communication Protocol AS-NE-02 Network Interfaces AS-NE-03 Network Controller AS-NE-04 Network Stack AS-OS-0t Containers/VMs
	Communication link outages		
Various Nefarious Activity/ Abuse of assets	Traffic Tampering	Modifying (destroying, manipulating, or editing) data through unauthorized channels, when data are in transit.	AS-NE all network assets AS-OS-02 Native API AS-OS-04 Operating system AS-SO all software assets
	Abuse of authentication	Unauthorized access to an application, service, device, or data either through knowledge of the inherent weaknesses of an authentication mechanism, or by exploiting a flaw in the authentication scheme's implementation.	AS-OS all system software assets AS-SO all software assets

	Abuse of remote access to the network	Taking advantage of remote working technologies like remote desktop software, video conferencing tools, enterprise VPNs, and other remote access solutions to gain access to a physical or virtual system and consequently data, services and applications. Especially popular during the COVID-19 crisis.	AS-OS all system software assets AS-SO all software assets AS-US-02 end users
	Remote access exploitation		AS-OS all system software assets AS-SO all software assets AS-US-02 end users
Eavesdropping/ Interception / Hijacking	Traffic sniffing	Sniffing is a popular method used by malicious actors to capture and analyze network communication information. With sniffing, an attacker is able to eavesdrop data from network elements or links and steal valuable information. Sniffing can happen anywhere where there is constant traffic.	AS-NE all network assets AS-S0 all software assets AS-OS-02 Native API AS-DA-03 Application Data
	Manipulation of network traffic, network reconnaissance and information gathering	The threat includes the modification or falsification of data in transit (messages), injection of illegitimate data into the network, whether by replaying previous messages or by forging new messages, the use of traffic spikes and rerouting, modification of flow priorities	AS-NE all network assets AS-S0 all software assets AS-OS-02 Native API AS-DA-02 Coniguration Data AS-DA-03 Application Data AS-DA-04 System data
	Man in the middle/ Session hijacking	Man-In-The-Middle attacks against any communication link or communication session are enabled by weaknesses regarding the end-to-end encryption between the terminal and the server. If encryption is not properly configured or non-existent, information could be stolen and used for abuse later. Attackers can also attempt to exploit network security weaknesses such as a lack of firewalls to protect the internal network or vulnerabilities at an application level, data access, and misconfigurations.	AS-DA all data assets AS-NE all network assets AS-SO all software assets AS-OS-02 native API
	Interception of information	By gaining access to a resource with data in motion or in rest, unencrypted information may be intercepted and device or identity tracking is possible.	AS-DA all data assets AS-US-01 system users AS-US-02 end users
Denial of Service (DoS)	Distributed denial of service (DDoS)	Malicious attempts to disrupt the normal traffic of a targeted server, service or network (physical or virtual) by overwhelming the target or its surrounding infrastructure with a flood of traffic, or requests.	AS-OS all system software assets AS-SO all software assets AS-NE all network assets

	Flooding of network components	In DoS attacks achieve effectiveness by utilizing multiple attack agents or compromised systems as sources of attack traffic.	AS-NE all network assets
	Flooding of stations/terminals/servers		AS-OS all system software assets AS-SO all software assets
	Amplification attacks	Amplification attacks exploit a disparity in bandwidth consumption between an attacker and the targeted web resource. When the disparity in cost is magnified across many requests, the resulting volume of traffic can disrupt network infrastructure	AS-OS all system software assets AS-SO all software assets AS-NE-01 communication protocol
	MAC layer attacks	MAC layer attacks typically focus on disrupting channel access for regular nodes in a computer network (physical or virtual), thus disrupting the information flow both to and from the sensor node; this leads to a DoS condition at the MAC layer	AS-NE all network assets
	Jamming attacks	Denial of Service through noise injection and interference in a communication/network link.	AS-NE-01 Communication Protocol AS-NE-02 Network interface AS-NE-03 Network controller
	Edge node overload	This threat relates to attacks against edge networks disrupting the vicinity of the affected networks, at a local or service-specific level. The overload may take place by flooding the edge node with request or traffic directed to this component, initiated by a specific application or device.	AS-NE-01 Communication Protocol AS-NE-02 Network interface AS-NE-03 Network controller AS-SO all software assets
	Authentication traffic spikes	This threat relates to a massive number of authentication requests sent by a malicious actor in a short time. A malicious actor initiates traffic spikes or emphasizes the effects of natural traffic spikes with devices aiming to connect. Consequently, the service or the network will experience more signalling and authentication requests that is capable of handling.	AS-OS all system software assets AS-SO all software assets
Exploitation of hardware, software vulnerabilities	Zero-day exploit	A zero-day exploit is a software security flaw that does not have a patch to fix the flaw and can be exploited by attackers if discovered.	AS-OS all system software assets AS-SO all software assets
	Abuse of edge open application programming interfaces	This threat involves exploiting application programming interfaces (APIs) to launch different types of attacks. Open and customizable frameworks expand the use of APIs. A poorly designed or configured API with inaccurate access control rules may expose digital infrastructure sensitive data and parameters. The threat of having one small	AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating system AS-OS-05 Containers/VMs
	Application programming interface (API) exploitation		

		compromised API in a service may place the entire infrastructure are risk.	AS-SO all software assets
	Software tampering	An intentional but unauthorized act resulting in the modification of a software component – its intended behavior, produced results or produced/consumed data.	AS-OS all system software assets AS-SO all software assets
	System execution hijack		AS-OS all system software assets
Malicious code/software	Ransomware	Ransomware is a type of malware that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. Relevant to any kind of data and computational system.	AS-DA all data AS-OS all system software assets AS-SO all software assets AS-US all users
	Injection attacks	The threat includes the installation and distribution of malicious software or the implant of specific code or software inside a product or updates. Examples of malicious software include malware, ransomware, virus, worms, trojans, SQL injections, rogue security software, rogueware and careware. Malware may be installed in various virtual and physical components of the digital infrastructure	
	Rootkits/Rogueware/Worms/Trojan		
	Malware attacks on computational units		
	Malware attacks on network products		AS-OS all system software assets AS-NE-02 Network interface AS-NE-04 Network stack
	Malware attacks on business applications		AS-DA all data AS-SO all software assets AS-US all users
	Botnets	Botnets are malicious networks computers, connected to the Internet. The basic function of botnets consists of the following: Try to infect as many unsuspecting users as possible, taking advantage of possible vulnerabilities in their system, with the aim of stealing personal data, the money laundering and large-scale attacks.	AS-DA all data AS-OS all system software assets AS-SO all software assets AS-US all users
Identity fraud/account or service	Identity theft	This threat may materialize when a malicious actor successfully determines the identity of a legitimate entity and then masquerades to launch further attacks. Identity spoofing is a threat that can affect any software component or human agent. In this attack, the attacker spoofs the identity of a legitimate controller and interacts with the infrastructure functions controlled by the legitimate controller (i.e., elements of the data plane) to trigger several other types of attacks (instigate network flows, divert traffic, etc.). The use of social engineering, brute force user account/password cracking may also be used as a technique to spoof or steal user credentials	AS-DA all data assets AS-US all user assets AS-OS-02 Native API AS-OS-04 Operating system
	Identity spoofing		AS-DA all data assets AS-US all user assets AS-OS-02 Native API AS-OS-04 Operating system
	IP – MAC spoofing	IP or MAC spoofing is used to gain unauthorized access to a computer. The attacker impersonates a trusted source address.	AS-NE-02 Network Interfaces

			AS-NE-03 Network Controller
Data breach, leak, theft and manipulation of information	Network product log tampering	if a network (physical/virtual) or computational device do not securely store log files, an attacker, for example can inject, delete or otherwise tamper with the contents of the logs typically for the purposes of masking other malicious behavior.	AS-NE-02 Network Interfaces AS-NE-03 Network Controller AS-OS-01 Embedded System Firmware AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating systm
	File Write Permission Abuse	File write permissions which are far too liberal are potentially vulnerable and can be abused by an attacker to cause DoS – e.g., file with weak password can be altered and change the admin password, causing impossibility for the administrator to access.	AS-DA all data assets AS-OS-02 Native API AS-OS-04 Operating System AS-OS-05 Containers/VMs AS-SO-03 DB management systems
	Ownership file misuse	Files owned by a user on a device, or storage are altered improperly and illegitimately by a user different than the owner – then the attacker can conduct several other types of attacks (e.g., data theft, DoS, etc.)	
	Breach of customer data	Data breach or theft means that a forceful attack against a system, service or application of the digital infrastructure is carried out with the intentions to steal data (stored or in transit) Data leakage is the exploitation of a vulnerability or an unintentional disclosure with the result to leak data towards unauthorized destinations.	AS-DA all data AS-US-02 end-user
	Theft of personal data		AS-DA all data AS-US all users
	Theft and/or leakage of data from cloud computing		
	Theft/breach of security keys		
	Theft and/or leakage from network traffic		
	Unauthorized access to user plane data	Attackers may gain unauthorized access to user data due to insufficient access management or lack of awareness, which causes unintentional data disclosure.	AS-DA-01 Backup data AS-DA-03 Operation Data
	Unauthorized access to control plane data	Attackers may gain unauthorized access to control plane date due to insufficient access management or lack of awareness, which provides the opportunity to alter configurations, leak service-related data, and cause DoS.	AS-DA-02 Configuration data AS-DA-04 System Data AS-DA-06 Audit data
Unauthorized activities/ne	Brute force	The attacker submits a flood of passwords and passphrases towards a device (physical or virtual), a service or an application systematically until the correct is found.	AS-OS all system software assets AS-SO all software assets

twork intrusions	Port knocking	A method of externally opening ports on a firewall of a computational device, a server (physical or virtual), a network device by generating a connection attempt on a set of prespecified closed ports. Once a correct sequence of connection attempts is received, the firewall rules are dynamically modified to allow the host which sent the connection attempts to connect over specific ports.	AS-HW-03 Computational device AS-OS-02 Native API, AS-OS-03 Hypervisor, AS-OS-04 Operating System,
	Lateral movement	After the initial access, lateral movement is the attacker's technique to move deeper into the network with a persistent attack in search of sensitive data and high-value assets. The attacker uses tools to gain privileges from resources accessed in the compromised area.	AS-OS all system software assets AS-SO all software assets AS-NE-02 Network interface
Manipulation of hardware and software	Manipulation of hardware equipment	The threat considers the inclusion of concealed hardware or software in the product by a vendor or supplier. This threat may occur at an initial stage of the product implementation or during maintenance with the application of uncontrolled updates and new features.	AS-HW all hardware assets
	Software backdoor		AS-SO all software assets
	Manipulation of the network/system resources orchestrator	The threat considers the manipulation of the network/system resources orchestrator configuration to perform an attack. This threat includes modifying a function behaviour by altering the settings in the orchestrator and consequently compromising the separation between functions.	AS-OS-02 Native API AS-OS-03 Hypervisor AS-OS-04 Operating system AS-OS-05 Containers/VMs AS-SO all software assets
	Memory scraping	This threat arises when an attacker scans the physical memory of a software component in order to extract sensitive information that it is not authorized to have.	AS-DA, All Data assets
	Side channels attacks	The threat involves extracting information on existing flow rules used by network or service elements. The threat can be realized by exploiting patterns of network or service operations (e.g., exploiting the time required for establishing a connection).	AS-HW all hardware assets
	False or rogue gateway	The open nature of edge gateways, where even user-owned devices can become full-fledged participants (e.g., personal cloudlets, TV smart-box, etc.), creates a scenario where malicious actors can deploy their own gateway devices with the same result as in the Man-in-the-Middle.	AS-NE-02 Network Interface AS-NE-03 Network Cpntroller AS-NE-04 Networkf
Legal	Breach of service level agreement	Failure to carry out obligations a) defined by the law, b) defined by service functional requirements, c) contractual agreements.	AS-US-01 System Users AS-US-02 End Users AS-US-03 Contractors, sub/contractors

4 ESTIMATION OF THE IMPACT OF AN INCIDENT (PER OES/DSP)

The criteria that were specified for the assessment of the severity of incidents based on both the ENISA guidelines as well as applications of other member- states are the following:

- Affected population-geographical distribution
- Impact on the state's economy
- Public services, national security
- Threat to human life
- Impact on public opinion
- International public relations/impact on other states
- Cross-sector interdependencies
- Environmental impact
- Recovery time following an incident

4.1 Energy Sector

Impact level	Sector criteria	Quantitative criteria
Low (L)	▪ Affected population-geographical distribution ▪ Impact on the state’s economy ▪ Public services, national security ▪ Impact on public opinion ▪ International public relations/impact on other states ▪ Cross-sector interdependencies ▪ Environmental impact ▪ Recovery time following an incident	▪ Affected population – geographical distribution (town level && up to 20,000 people) || ▪ Impact on public opinion (regional level) && ▪ Recovery time following an incident (<3 hours)
Medium (M)		▪ Affected population – geographical distribution (municipal level && up to 150,000 people) || ▪ Public services (YES) || ▪ Impact on public opinion (national) || ▪ International public relations (YES) || ▪ Cross-sector interdependencies (affected only 1 sector) && ▪ Recovery time following an incident (>3 hours)
High (H)		▪ Affected population – geographical distribution (larger than municipality level && > 150,000 people) || ▪ Severe impact on state ‘s economy (>500,000,000 €) ||

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

Impact level	Sector criteria	Quantitative criteria
🟥		▪ National security (YES) || ▪ Threat to human life (YES) || ▪ Impact on public opinion (national) || ▪ Impact on other states (YES) || ▪ Cross-sector interdependencies (affected >1 sectors) || ▪ Environmental impact || ▪ Recovery time following an incident (>6h)

4.2 Transportation Sector

Impact level	Sector criteria	Quantitative criteria
Low (L)	▪ Affected population-geographical distribution ▪ Impact on the state's economy ▪ Public services, national security ▪ Impact on public opinion ▪ International public relations/impact on other states ▪ Cross-sector interdependencies ▪ Environmental impact ▪ Recovery time following an incident	▪ Affected population-geographical distribution (town level && up to 10,000 people) || ▪ Impact on public opinion (regional) && ▪ Recovery time following an incident (<5h)
Medium (M)		▪ Affected population-geographical distribution (municipal level && up to 75,000 people) || ▪ Public services (YES) || ▪ Impact on public opinion (national) || ▪ International public relations (YES) && ▪ Recovery time following an incident (>5h)
High (H)		▪ Affected population – geographical distribution (larger than municipality level && > 75,000 people) || ▪ Severe impact on state 's economy (>500,000,000 €) || ▪ National security (YES) ||

Impact level	Sector criteria	Quantitative criteria
🟥		▪ Threats to human life (YES) || ▪ Impact on public opinion (national) || ▪ Impact on other states (YES) || ▪ Cross-sector interdependencies (affected >1 sectors) || ▪ Environmental impact || ▪ Recovery time following an incident (>12h)

4.3 Banking Sector

Impact level	Sector criteria	Quantitative criteria
Low (L)	▪ Affected population-geographical distribution ▪ Impact on the state’s economy ▪ Public services, national security ▪ Impact on public opinion ▪ International public relations/impact on other states ▪ Cross-sector interdependencies ▪ Recovery time following an incident	▪ Affected population-geographical distribution (town level && up to 20,000 people) || ▪ Impact on public opinion (regional) && ▪ Recovery time following an incident (< 3h)
Medium (M)		▪ Affected population-geographical distribution (municipal level && up to 150,000 people) || ▪ Public services (YES) || ▪ Impact on public opinion (national) || ▪ International public relations (YES) || ▪ Cross-sector interdependencies (affected only 1 sector) && ▪ Recovery time following an incident (>5h)
High (H)		▪ Affected population – geographical distribution (larger than municipality level && > 150,000 people) || ▪ Severe impact on state ‘s economy (>500,000,000 €) ||

Impact level	Sector criteria	Quantitative criteria
🟧		▪ National security (YES) || ▪ Impact on public opinion (national) || ▪ Impact on other states (YES) || ▪ Cross-sector interdependencies (affected >1 sectors) || ▪ Recovery time following an incident (>6h)

4.4 Finance Sector

Impact level	Sector criteria	Quantitative criteria
Low (L)	▪ Impact on the state’s economy ▪ Impact on public opinion ▪ International public relations/impact on other states ▪ Recovery time following an incident	▪ Impact on public opinion (regional) && ▪ Recovery time following an incident (< 3h)
Medium (M)		▪ Impact on public opinion (national) || ▪ International public relations (YES) && ▪ Recovery time following an incident (> 3h)
High (H)		▪ Severe impact on state ‘s economy (>500,000,000 €) || ▪ Impact on public opinion (national) || ▪ Impact on other states (YES) || ▪ Recovery time following an incident (> 6h)

4.5 Health Sector

<table>
<tr><th>Impact level</th><th>Sector criteria</th><th>Quantitative criteria</th></tr>
<tr><td>Low (L)</td><td rowspan="3">▪ Affected population-geographical distribution
▪ National security
▪ Threat to human life
▪ Impact on public opinion
▪ Recovery time following an incident</td><td>▪ Affected population-geographical distribution (town level && up to 20,000 people)
||
▪ Impact on public opinion (regional)
&&
▪ Recovery time following an incident (< 3h)</td></tr>
<tr><td>Medium (M)</td><td>▪ Affected population-geographical distribution (municipal level && up to 150,000 people)
||
▪ Impact on public opinion (national)
&&
▪ Recovery time following an incident (> 3h)</td></tr>
<tr><td>High (H)</td><td>▪ Affected population – geographical distribution (broader than municipality level && > 150,000 people)
||
▪ National security (YES)
||
▪ Threat to human life (YES)
||
▪ Impact on public opinion (national)
||
▪ Recovery time following an incident (> 12h)</td></tr>
</table>

4.6 Water Sector

Impact level	Sector criteria	Quantitative criteria
Low (L)	▪ Affected population-geographical distribution ▪ Impact on the state's economy ▪ Public services, national security ▪ Impact on public opinion ▪ International public relations/impact on other states ▪ Cross-sector interdependencies ▪ Environmental impact ▪ Recovery time following an incident	▪ Affected population-geographical distribution (town level && up to 20,000 people) || ▪ Impact on public opinion (regional) && ▪ Recovery time following an incident (< 12h)
Medium (M)		▪ Affected population-geographical distribution (municipal level && up to 150,000 people) || ▪ Public services (YES) || ▪ Impact on public opinion (national) || ▪ Cross-sector interdependencies (affected only 1 sector) && ▪ Recovery time following an incident (> 12h)
High (H)		▪ Affected population – geographical distribution (larger than municipality level && > 150,000 people) || ▪ Severe impact on state 's economy (>500,000,000 €) || ▪ National security (YES) ||

Impact level	Sector criteria	Quantitative criteria
🟧		▪ Threat to human life (YES) || ▪ Impact on public opinion (national) || ▪ Cross-sector interdependencies (affected >1 sectors) || ▪ Environmental impact || ▪ Recovery time following an incident (> 24h)

4.7 Digital Infrastructure Sector

<table>
<tr><th>Impact level</th><th>Sector criteria</th><th>Quantitative criteria</th></tr>
<tr><td>Low (L)</td><td rowspan="3">▪ Affected population-geographical distribution
▪ Impact on the state’s economy
▪ Public services, national security
▪ Impact on public opinion
▪ International public relations/impact on other states
▪ Cross-sector interdependencies
▪ Recovery time following an incident</td><td>▪ Affected population – geographical distribution (up to 50,000 people)
||
▪ Impact on public opinion (regional level)
&&
▪ Recovery time following an incident (<3 hours)</td></tr>
<tr><td>Medium (M)</td><td>▪ Affected population – geographical distribution (up to 250,000 people)
||
▪ Public services (YES)
||
▪ Impact on public opinion (national)
||
▪ International public relations (YES)
||
▪ Cross-sector interdependencies (affected only 1 sector)
&&
▪ Recovery time following an incident (>3h)</td></tr>
<tr><td>High (H)</td><td>▪ Affected population – geographical distribution (>250,000 people)
||
▪ Severe impact on state ‘s economy (>500,000,000 €)
||
▪ National security (YES)
||</td></tr>
</table>

Impact level	Sector criteria	Quantitative criteria
🟥		▪ Threat to human life (YES) || ▪ Impact on public opinion (national) || ▪ Impact on other states (YES) || ▪ Cross-sector interdependencies (affected >1 sectors) || ▪ Environmental impact || ▪ Recovery time following an incident (>6h)

4.8 DETERMINATION OF THE SEVERITY OF INCIDENTS FOR DSPs

Based on ENISA's study [32]. Properties mentioned in the following table may be:

- integrity affected (information or output provided altered)
- confidentiality affected (interception, unauthorized access)
- availability affected (service degraded, interrupted and unusable)
- authenticity affected (cannot be trusted)

Impact level	Sector criteria	Quantitative criteria
Low (L)	▪ Geographical coverage ▪ Disruption extent ▪ Population affected and incident duration (user time)	▪ Just 1 country || ▪ >1 properties affected || ▪ A>= 1,000,000 user hours for 1-hour interval && B>=25,000 users or >= 10,000 dependent users or services || ▪ A>=1,000,000 user hours for 1-hour interval && C>= 1h || ▪ Impact on public opinion (regional)
Medium (M)		▪ >2 properties affected || ▪ A>=1,500,000 user hours for 1-hour interval && B>=50,000 users or >=20,000 dependent users or services || ▪ A>=1,500,000 user hours for 1-hour interval && C>=2h ||

Impact level	Sector criteria	Quantitative criteria
🟨		▪ Public services (YES) || ▪ Impact on public opinion (national) || ▪ International public relations (YES) || ▪ Cross-sector interdependencies (affected only 1 sector)
High (H)		▪ Loss of integrity, authenticity, or confidentiality of the stored, transmitted, or processed data || ▪ A>=5,000,000 user hours for 1-hour interval && B>affected only 100,000 users or >=50,000 dependent users or services || ▪ A>=2,000,000 user hours for 1-hour interval && C>=3h || >1,000,000 € loss for >=1 user || ▪ >3 following conditions are applicable: || ▪ National security (YES) || ▪ Threat to human life (YES) || ▪ Impact on public opinion (national) || ▪ Impact on other states (YES) ||

Impact level	Sector criteria	Quantitative criteria
🟥		▪ Cross-sector interdependencies (affected >1 sectors)

5 UTILITY OF THE RESULTS FOR THE FOLLOWING CITYSCAPE PHASES

The study presented in the previous study was performed in order to act as a future reference for the threat landscape for the NIS directive critical domains, that have huge impact in the livelihood and wellness of citizens.

Nevertheless, the results of the study are also utilized for the future phases of the CitySCAPE analysis and development process. In the following lists, we summarize which CitySCAPE Tasks are influenced by the study, and then we specify the exact activities that justify the deliverable impact.

The CitySCAPE tasks potentially impacted by the deliverable are the following:

- The second part of Task 2.2 "Cross-domain threat analysis" that contains the System Modelling, Risk Analysis and Management for the Multimodal Transport Systems targeted by CitySCAPE.
- The Task 2.3 Mechanisms of cascading threats (across multimodal ecosystem).
- The Task 2.4 Security assurance methodology and tools.
- The Task 5.5 Risk analysis and impact assessment engine.
- The Task 5.6 Financial impact assessment engine

The presented results are used in the following manner:

- The assets for each domain may vary significantly with completely different functional objectives and requirements. However, the investigation showed that in the current cyber-environment, the generic structure of a platform is quite similar. Generally, the same wired and wireless networks are used, functions and functionalities are hosted in the cloud, structurally identical automations, IoT and mobile devices are exploited, mobile applications and webservices are used for monitoring and management, data are utilized to produce knowledge, hardware and software components are decomposed at the same basic set of elements (operating systems, processing units, APIs, etc.). This ascertainment led to the definition of basic assets, i.e., a set of assets that through networking, relationships and interfaces can form any asset for any of the domains of OESs and DSPs. The identified basic assets are presented in Table 2and have been the basis for the development of the hierarchical risk model of D2.3 that allows reusability, adaptability, and extendibility of results – for all NIS directive domains and DSPs. Therefore, the CitySCAPE risk model and analysis can be applicable in all domains whatsoever and not only at the multi-modal ecosystem, although tweaked and populated to specifically fit it.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

- The threats of the transport domain were used as a basis for the list of threats identified at the risk analysis. The specific list was also enrichened with data from the other domains. Given the asset structural similarity, seemingly irrelevant threats, e.g., at the water supply automation can be treated as a potential threat for the multimodal transport system (e.g., connected vehicle automation). Nevertheless, in hindsight, a higher-level threat taxonomy also confirms the similarity among the inter-domain threat landscapes. In the context of D2.3, a homogenization has been performed in order to unify terminology and descriptions used in different sectors describing a structurally and functionally identical threat.
- The totality of the identified threats is used to populate the list of threats of the RITA CitySCAPE tool that will be used by the dynamic risk analysis to calculate the risk scores and associated impacts.
- In the presented analysis, the identified threats are organized in groups called high-level threats. Our investigation concluded that the so-called high-level threats (even for ENISA) are practically impacts or consequences rather than threats. Thus, system failure is not a threat, rather than an impact caused by a threat. This finding facilitates the cascading threat propagation algorithm of Task 2.3, where the rationale relies in the following simple scheme: implementation of a threat on asset A caused and Impact. If asset A is in a sharing relationship with asset B, then the Impact instantiates as threat on asset B causing a cascading effect. Additionally, the study completeness allows as to follow the same tactic when investigating cascading threats from different domains, rather than from different assets.
- The impact assessment methodology presented in the deliverable identifies levels depending on the effect of a threat in the proper operation of the society, state, and government. As such, these criteria will be utilized for the development of the FIMCA (Financial Impact Assessment) engine, as well as the RITA engine for the quantification of the impact for an (asset, threat) ordered pair.

6 CONCLUSION

This document includes a detailed investigation of the current threat landscape against the major Operators of Essential Services (OES) and the Digital Service Providers (DSP).

- First, a presentation of the NIS directive and the necessary set of definitions is provided.
- Then a methodology for the identification of an Operator of Essential Services according to the NIS is presented.
- As a next step, the common elements among OESs and DSPs are identified according to common functional areas; dependence on DSPs and digital infrastructure; and interdependencies between fields.
- The threat landscape is analysed per domain/sector:
    - Energy,
    - Transportation,
    - Health,
    - Finance,
    - Banking,
    - Water Supply/Facilities.

  For each sector, the type of involved actors/entities is described, as well as a set of rules for the classification of service is provided.
- Finally, a methodology for incident classification per OES and DSP depending on impact and criticality is defined.

The specific deliverable paves the way for the threat analysis, the risk analysis and the cascading methodology that completes the work of CitySCAPE WP2.

7 REFERENCES

[1] "Methodologies for the identification of Critical Information Infrastructure assets and services," European Union Agency for Network and Information Security, December 2014

[2] "Identification of Operators of Essential Services," ENISA, November 2017

[3] "Incident notification for DSPs in the context of the NIS Directive," ENISA, February 2017.

[4] "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," EUROPEAN COMMISSION, 2017.

[5] "Identification of Operators of Essential Services - Reference document on modalities of the consultation process in cases with cross-border impact," CG Publication - NIS Cooperation Group, 2018.

[6] "Reference document on Incident Notification for Operators of Essential Services - Circumstances of notification," CG Publication - NIS Cooperation Group, 2018.

[7] "Developments on NIS Directive in EU Member States," Bird&bird, June 2018.

[8] "Network and Information Systems Security (Incident Reporting)", 2019 decision by Republic of Cyprus.

[9] "METHODOLOGY FOR DETERMINING OES (Spanish Approach)," Centro Criptologico National, 2018.

[10] "Security of Network and Information," UK Department for Digital, Culture, Media and Sport, January 2018.

[11] "Baseline Security Recommendations for IoT", ENISA, November 2017.

[12] "Smartphone Secure Development Guidelines", ENISA, February 2017,

[13] "Cloud Computing Security Risk Assessment", ENISA

[14] ENISA Good practices for IoT and Smart Infrastructures Tool https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

[15] ENISA (2018, November) Good practices on interdependencies between OES and DSPs

[16] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," in IEEE Control Systems Magazine, vol. 21, no. 6, pp. 11-25, Dec. 2001, doi: 10.1109/37.969131.

[17] ENISA (2020, February 24). Procurement Guidelines for Cybersecurity in Hospitals. Retrieved from: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[18] ENISA (2021, January 18). Cloud Security for Healthcare Services. Retrieved from: https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services

[19] Hewit, K. (2020, July 27). Cybersecurity in Banking: Three Top Threat Trends to Know. Retrieved July 2021, from Security Scorecard: https://securityscorecard.com/blog/cybersecurity-in-banking-three-top-threats-trends-to-know

[20] Akamai. (2019, July 31). Akamai Threat Research: Phishing and Credential Stuffing Attacks Remain Top Threat to Financial Services Organizations and Customers. Retrieved July 2021, from Akamai: https://www.akamai.com/us/en/about/news/press/2019-press/state-of-the-internet-security-financial-services-attack-economy.jsp

[21] Bitglass. (2019, December 16). Bitglass 2019 Financial Breach Report: More than 60% of All Leaked Records in Past Year Exposed by Financial Services Firms. Retrieved July 2021, from Business Wire: https://www.businesswire.com/news/home/20191216005207/en/Bitglass-2019-Financial-Breach-Report-60-Leaked

[22] Horne, E. (2020, October 12). How the Financial Services Industry Faces New Data Security Challenges with BYOD and Mobile Device Use. Retrieved July 2021, from Hypori Virtual Mobility: https://hypori.com/blog/bank-data-security/

[23] ENISA (Nov 2018). Financial fraud in the digital space. Retrieved from: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/financial-fraud-in-the-digital-space

[24] Hermano, J. (2019). “Cybersecurity Risk & Responsibility in the Water Sector”. Retrieved from: https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance

[25] New York Times (2018, May 27). “A Cyberattack Hobbles Atlanta, and Security Experts Shudder”. Retrieved from: https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

[26] Kumar, M. (2016, April 29). “Ransomware virus shuts down Electric and Water Utility”. Retrieved from: https://thehackernews.com/2016/04/power-ransomware-attack.html

[27] InfoSecurity Magazine (2017, September 20). “Why 2017’s Phishing Attacks Teach Us All to Beware”. Retrieved from: https://www.infosecurity-magazine.com/opinions/why-2017-phishing-attacks-teach/

[28] Pritam, N. & Ward, C. (2016, April 29). “Verizon's 2016 Data Breach Investigations Report finds cybercriminals are exploiting human nature”. Retrieved from: https://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human

[29] ENISA (Dec 2016). Securing Smart Airports. Retrieved from: https://www.enisa.europa.eu/publications/securing-smart-airports

[30] ENISA (Nov 2020). RAILWAY CYBERSECURITY. Retrieved from: https://www.enisa.europa.eu/publications/railway-cybersecurity

[31] ENISA (Dec 2015). Cyber Security and Resilience of Intelligent Public Transport. Retrieved from: https://www.enisa.europa.eu/publications/good-practices-recommendations

[32] "Incident notification for DSPs in the context of the NIS Directive," ENISA, February 2017.

[33] ENISA (Jan 2019-Apr 2020). The year in review ENISA Threat Landscape. Retrieved from:https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport

[34] ENISA (Jan 2019-Apr 2020). Cryptojacking (ENISA Threat Landscape). Retrieved from: www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-cryptojacking

[35] TechAdvisory.org (2018, November 8). Outdated firmware: An overlooked threat. Retrieved from: https://www.techadvisory.org/2018/11/outdated-firmware-an-overlooked-threat/

[36] Slowik, J. (2019). "CRASHOVERRIDE: Reassessing the 2016 ukraine electric power event as a protection-focused attack," Dragos report [Online]. Available at: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

[37] Johnson, B.; Caban, D.; Krotofil, M.; Scali, D.; Brubaker, N.; Glyer, N. (2017). "Attackers deploy new ICS attack framework "TRITON" and cause operational disruption to critical infrastructure". Retieved from: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploynew-ics-attackframework-triton.html

[38] Slowik, J. (2018). "Anatomy of an attack: Detecting and defeating CRASHOVERRIDE" Dragos whitepaper [Online]. Available at: https://www.dragos.com/resource/ anatomy-of-an-attack-detecting-and-defeating-crashoverride/

[39] Falliere, N.; Murchu, L.-O.; Chien, E (2011). "W32. Stuxnet dossier" White paper, Symantec Corp., Security Response, vol. 5, no. 6, p. 29.

[40] ICS-CERT, "Cyber-attack against Ukrainian critical infrastructure," *IR-ALERT-H-16-056-01, U.S Department of Homeland Security*, 2016. [Online]. Available: https://us-cert.cisa.gov/ics/alerts/ IR-ALERT-H-16-056-01

[41] Staggs, J.; Ferlemann, D.; Shenoi S (2017). "Wind farm security: attack surface, targets, scenarios and mitigation" International Journal of Critical Infrastructure Protection, vol. 17, pp. 3–14.

[42] Gündüz, Muhammet & Das, Resul. (2020). "Cyber-security on smart grid: Threats and potential solutions". Computer Networks. 169. 107094. 10.1016/j.comnet.2019.107094.

[43] ENISA (2013, December 17). "Smart Grid Threat Landscape and Good Practice Guide". Retrieved from: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

[44] Kovanen, Tiina & Nuojua, Viivi & Lehto, Martti. (2019). "Cyber Threat Landscape in Energy Sector Cyber Threat Landscape in Energy Sector". Retrieved from: https://www.researchgate.net/publication/338215941_Cyber_Threat_Landscape_in_Energy_Sector_Cyber_Threat_Landscape_in_Energy_Sector

[45] Kyriakidis, A. (2015). "DDoS Attacks from botnets on critical Smart Grid infrastructure". Retrieved from: https://ee.auth.gr/wp-

content/uploads/participants-database/botnet_smart_grid_kyriakidis.pdf

[46] Wikipedia. ‘*Ransomware*’. Retrieved from: https://en.wikipedia.org/wiki/Ransomware#History

[47] Goodchild, J. (2018, November 2). “How an IoT Botnet Could Breach the Power Grid and Cause Widespread Blackouts”. Retrieved from: https://securityintelligence.com/how-an-iot-botnet-could-breach-the-power-grid-and-cause-widespread-blackouts/

[48] Alert Logic (2015, August 11). “Alert Logic Cloud Security Report Warns Energy Sector of Threats”. Retrieved from: https://www.alertlogic.com/press-releases/alert-logic-cloud-security-report-warns-energy-sector-of-threats/

[49] Flå, Lars & Borgaonkar, Ravishankar & Tøndel, Inger Anne & Jaatun, Martin. (2021). Tool-assisted Threat Modeling for Smart Grid Cyber Security. 1-8. 10.1109/CyberSA52016.2021.9478258.

[50] ENISA Threat Landscape for 5G Networks, Dec 2020 https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[51] Threat Landscape and Good Practice Guide for Internet Infrastructure, ENISA, Jan 2015 https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure

[52] Privacy, Security and Identity in the Cloud, Giles Hogben, ENISA https://www.enisa.europa.eu/topics/cloud-and-big-data/Cloud_Identity_Hogben.pdf

[53] Good Practices and Recommendations on the Security of Big Data Systems, ENISA, Dec 2015

[54] Towards secure convergence of Cloud and IoT, ENISA, Sep 2018 https://www.enisa.europa.eu/news/enisa-news/towards-secure-convergence-of-cloud-and-iot

[55] Security Framework for Governmental Clouds, ENISA, Feb 2015 https://www.enisa.europa.eu/publications/security-framework-for-govenmental-clouds