INTERNATIONAL
HELLENIC
UNIVERSITY

Contemporary Cyber Threats to Critical Infrastructures: Management and Counter-measures

Konstantinos Mitsarakis

SID: 3307210006

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Cybersecurity

APRIL 2023

THESSALONIKI – GREECE

Contemporary Cyber Threats to Critical Infrastructures: Management and Counter-measures

Konstantinos Mitsarakis

SID: 3307210006

Supervisor:	Assoc. Prof. Konstantinos Rantos
Supervising Committee Members:	Dr Nikolaos Serketzis
	Dr Nikolaos Vretos

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Cybersecurity

APRIL 2023

THESSALONIKI – GREECE

Abstract

This dissertation was written as a part of the MSc in Cybersecurity at the International Hellenic University.

Nowadays, the unobstructed functioning of society is increasingly contingent upon a broad spectrum of technological solutions. This assertion holds true for the services that cover the daily needs of citizens, the so-called critical infrastructures. Nonetheless, an undue reliance on technology, in excess of the automation and amenity it affords, constitutes the most vulnerable link in the flawless provision of those essential services, thereby threatening the welfare of citizens. It has become manifest that critical infrastructures constitutes one of the principal targets of cyber attacks, with a considerable impact on the economic and social life, as well as on the overall prestige of the state.

The objective of this dissertation is to provide a comprehensive approach to safeguarding critical infrastructures against contemporary cyber threats, thereby enhancing their overall robustness and resilience. This is achieved first by scrutinizing the diverse elements that facilitate these threats and subsequently by implementing suitable strategies for their mitigation via suitable actions and management at both technical and administrative aspects, exhibiting the necessity to embrace a more expansive cybersecurity strategy. Within this context, the relevant legal context for cybersecurity is presented, followed by an investigation of the primary risk factors and the attack surface. Additionally, an analysis of the main cyber threats and attack techniques is also provided. Furthermore, this study outlines the fundamental measures, as stated in the literature corresponding to each case, necessary for mitigating cyber threats in critical infrastructure organizations, encompassing all stages from prevention to incident management.

Konstantinos Mitsarakis

06/04/2023

Contents

Table of Tables

Table of Images

1 Introduction

The current era is experiencing significant changes that are fundamentally transforming the technological establishment. Concepts such as the Internet of Things, Cloud, Digital Transformation, Artificial Intelligence and Cybersecurity have entered our lives, either knowingly or unintentionally, to an extent and in ways that are not immediately apparent at first sight. The use of technology has infiltrated fundamental societal structures and systems that are deemed indispensable for upholding the social coherence and the welfare of citizens, namely the Critical Infrastructures or Essential Services Operators (ESOs) [1].

However, this reliance of critical infrastructure on digital systems has led to the emergence of a conducive environment for criminal activity aimed at exploiting the potential vulnerabilities of the expanded attack surface of this infrastructure [2]. This situation is further aggravated by the anonymity provided by the internet [3], the absence of geographical borders in cyberspace, and the emergence of new profit-making avenues, thereby reinforcing the motivation of cybercriminals and increasing the number of potential attackers [2]. Moreover, the concentration of digital services in a decreasing number of private companies creates uncertainties in establishing a resilient environment, while the public's lack of confidence in cybersecurity poses challenges to its adoption.

The problem is amplified to a greater extent, as cyber attacks on critical infrastructure are now an element of the asymmetric, undefined and often undeclared war between rival states. Infrastructures such as power plants, drinking water and wastewater treatment plants, financial institutions, and digital providers have become a realm of electronic warfare. This is owing to the fact that even a minor disruption in the operations of these systems has a disproportionate impact on the daily existence of a significant portion of the population, thereby generating serious predicaments for the target state and jeopardizing national security, national economy, public health or any combination thereof [4]. Furthermore, the disturbance of a particular critical infrastructure has an adverse effect on the seamless operation of other infrastructures, as they are interconnect-

ed at the physical, logical, or informational level [5]. Within this framework, cybercriminals target every individual, enterprise, public organization, and even nations, posing a threat to their fundamental rights, privacy, legal existence, and even survival. It is evident that cybersecurity is no longer a choice but rather an indispensable social requirement [6].

Therefore, it is crucial to implement the appropriate security measures, both at an organizational and technical level, in order to manage cyber-attacks, which require a combination of multiple actions. Specifically, this entails conducting thorough risk assessments, implementing early detection and prevention measures, executing effective responses, and achieving full and successful recovery from cyber-attacks. Additionally, mitigation strategies should be in place to minimize the impact of an attack if all other measures fail to achieve the desired degree of protection.

In order to effectively combat modern threats, it is essential to implement a comprehensive security framework that encompasses all the components of critical infrastructure information systems, including hardware, software, processes, people, and data [7]. This holistic approach is necessary to address the complex and interconnected nature of cyber threats and ensure the resilience of critical infrastructures against a wide range of attack vectors.

The aim of this dissertation is to systematically explore all dimensions of cybersecurity in critical infrastructures, encompassing the scope of the attack surface, the associated threats, and the mitigation and management strategies.

It is worth mentioning that given the vast number of critical infrastructures and their distinct characteristics, the objective of this study is to present the general threats and areas of cybersecurity application at a broad level, without delving into specific technicalities for each industry. The scope of this research is of significant interest and may serve as a foundation for a future doctoral thesis.

The dissertation is divided into three parts, each addressing a distinct aspect of the critical infrastructure cybersecurity landscape. The first part presents an overview of current trends in cyber-attacks, providing examples of recent attacks on critical infrastructure both in Greece and abroad. Additionally, the most significant legal and regulatory contexts governing the critical infrastructure sector in Greece and Europe are discussed, along with an overview of key Greek institutions related to cybersecurity.

The second part of the dissertation delves into the threat landscape, providing a theoretical foundation on cyber threats. This section focuses on the threat landscape, actors involved in malicious activities, their objectives, and elements at risk.

Part three explores the attack surface of critical infrastructures, identifying potential attack vectors and contemporary cyber threats. This section consists of three chapters that investigate the attack surface by categorizing it into different dimensions, including critical infrastructure sectors, attack surface domains, and the attack types that deemed to be of utmost significance currently.

Finally, the concluding section provides an overview on how critical infrastructure operators can adopt security frameworks proposed by literature and engage best practices to address, manage and mitigate cyber threats. The conclusions of the dissertation summarize the key findings and highlight the most important aspects that should be taken into consideration to enhance cybersecurity in critical infrastructures.

1.1 Methodology and Relevant Research

The dissertation was developed through a systematic approach and methodology that involved the analysis of various credible sources resulting to the following steps:

1. Comprehensive study of the research area related to cybersecurity protection of critical infrastructures.
2. Identification of the critical elements within this domain that needed to be investigated as well as their related aspects.
3. Establishing a knowledge base for each of these areas to gain a deep understanding of their characteristics and challenges.
4. Analysis and synthesis for the gathered information to identify the key elements that could be further explored.
5. Composition of the content of the dissertation based on the knowledge gained from the previous steps and presentation of the findings and conclusions in a structured and coherent manner.

The research process commenced by examining the prevailing legislation and pertinent directives at both the national and European levels, including, but not limited to, the NIS and GDPR directives, which are widely recognized as benchmarks in safeguarding critical infrastructure and personal data. These directives play a crucial role in shaping

the cybersecurity strategy of Europe and Greece, and are applicable across the entire European Union.

Consequently, the authoritative cybersecurity agencies of Europe and America, namely the European Union Agency for Cybersecurity (ENISA), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Department of Homeland Security (DHS), have proven to be invaluable resources for comprehending and exploring the current threat landscape. Specifically, the annual ENISA reports [8], [9] on the threat landscape offer extensive insights into the primary contemporary cybersecurity risks, while numerous supplementary materials furnish global cybersecurity guidelines. Notably, the ENISA report [10] on the escalating trend of cybersecurity investments within the European Union warrants attention. Likewise, the ENISA report [11] posits a framework for standardizing the process of identifying impending threats and the future evolution of the threat landscape.

Furthermore, across the Atlantic, CISA, as the United States' federal cybersecurity agency and national coordinator for critical infrastructure security and resilience, serves as a significant information hub for critical infrastructure protection and resilience by offering a plethora of research, guidance, and best practices.

The document in reference [12], conducted by the Institute of International Relations of France, provides a concise outline of cybersecurity risks within the energy sector in France, emphasizing the necessity for inter-state collaboration and harmonization of procedures for responding to threats.

Comparable research has been carried out on the content of globally acknowledged standards, such as ISO/IEC 27001 relating to information security management, and the NIST framework, which offers recommendations for enhancing the cybersecurity of critical infrastructures, alongside the MITRE ATT&CK knowledge base and the OWASP. Moreover, European Union initiatives, such as CONCORDIA, provided a highly valuable source of information, along with the corresponding report [13], which analyzed significant threats and identified countermeasures in distinct attack surface areas. Also, various white papers issued by prominent companies in the industry, such as Microsoft, IBM, and Cisco, were consulted to consider their stance on cybersecurity and recommended best practices for incorporating into the design of information systems.

At an academic level, a thorough literature review of similar theses and dissertations was conducted through university repositories. The PhD thesis of Marianthi Theo-

charidou [7] on "Risk Assessment of Critical Information & Communication Infrastructures" was a significant contribution to this research, as it extensively analyzed the research area of critical infrastructure protection and explored how to assess the criticality of such infrastructures.

The PhD thesis of Georgios Stergiopoulos [14] emphasized the importance of software security and highlighted the interaction among critical infrastructure stakeholders, underlining the significance of protecting all critical infrastructures as an interconnected chain. The thesis of Sotiria Argyropoulou [15] included valuable material on the interdependence of critical infrastructures and conducted a study on risk assessment based on the dependencies of communication and information infrastructures. Additionally, the thesis of Antonia Nikolopoulou [16] examined the implementation of the NIS Directive in the critical infrastructures of EU Member States at the legal and organizational levels proposing the establishment of a cybersecurity strategy in the aviation sector.

As part of the research methodology, a comprehensive literature search was conducted to identify relevant articles published in journals and conference proceedings. To this end, search engines such as Google Scholar, IEEE Xplore, and Scopus were utilized through the institutional account, using search queries such as (but not limited to):

> “cybersecurity critical infrastructures, critical infrastructure AND cyber threats, SCADA threats, critical infrastructure AND cloud, cybersecurity AND IoT, IoT AND critical infrastructures, smart metering AND threats, smart grid AND cyber threats, critical infrastructure AND phishing, critical infrastructure AND social engineering, critical infrastructure AND DoS, supply chain AND cyber threats”

Afterwards, the selected articles were carefully scrutinized, and their style, references and results were subject to a qualitative evaluation. It should be noted that given the ever increasing emergence of novel vulnerability threats, as well as the sheer volume of publications in related fields, there was a profusion of technical references and recurrent ideas, which lay outside the scope of this study. To identify the primary cyber threats to critical infrastructures, the outcomes of the literature search were amalgamated with the threats listed in the ENISA 2022 report concerning critical infrastructures. This enabled the analysis of techniques for mitigation and management, in accordance with the countermeasures recommended in the literature.

PART 1: Trends and Legal Context

2 Cyber Attacks: A Contemporary Threat

Cyber attacks have become an inseparable aspect of everyday life, not limited to times of war between nations but also during periods of peace. The year 2007 marked a turning point when a mere diplomatic dispute led to the complete digital paralysis of the entire Estonian state machinery, thus underscoring the dawn of a new era where cyber attacks jeopardize the modern way of life as a whole [17].

NIST defines the following general definition of a cyber attack [18]:

> *"An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information".*

The aforementioned activities encompass a range of malicious cyber operations, such as computer and network malware infections, service quality degradation or even complete disruption, data theft, malware-enabled vulnerability detection, and website/system/network destruction etc [2]. The classification of cyber-attacks can be made based on their effect on the physical and digital environments, distinguishing between kinetic and non-kinetic attacks. Kinetic cyber-attacks lead to events in the physical world, as seen in the Stuxnet case, whereas non-kinetic attacks only affect the digital realm, such as through information corruption or disclosure [19]. On numerous occasions, attacks are not solely focused on deleting data or disabling infrastructures, but are instead aimed at deliberately causing damage. For instance, in 2018, attackers deliberately attempted to sabotage the operations of an oil company with the intent of causing an explosion [20].

The defensive mechanisms employed by different organizations to safeguard their cyber spaces seem to be inadequate to provide comprehensive protection from the growing

number of security vulnerabilities [21]. Despite significant efforts made globally since 2007, the statistics demonstrate that mitigating and limiting cyber threats that pose a risk to both industry and the general population remains a substantial challenge. There are approximately 71.1 million victims of cybercrimes on an annual basis [22].

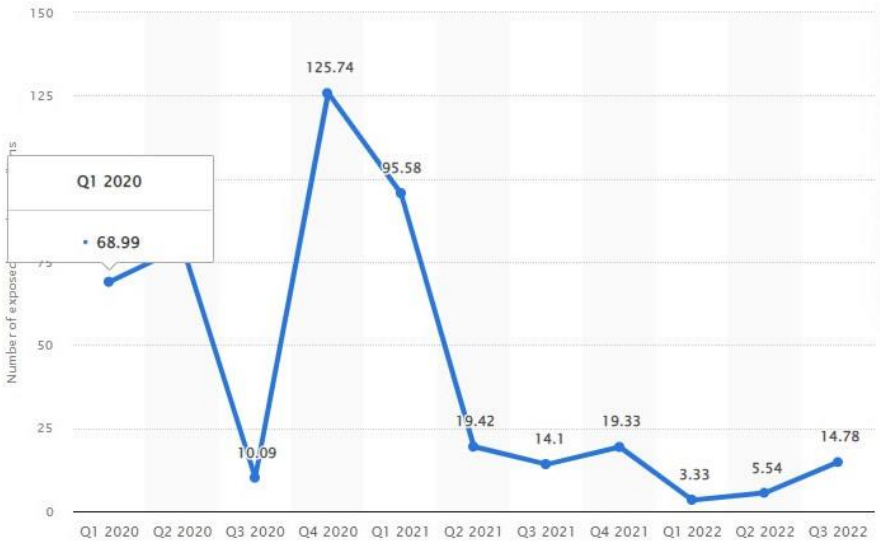

Image 1: Number of exposed records from data breaches [23]

As indicated by the chart presented earlier, it can be observed that in the third quarter of 2022, roughly 15 million data records were compromised worldwide as a result of data breaches, signifying a 37% surge in comparison to the preceding quarter.

In addition to compromising services and endangering citizens, cyber-attacks also carry a financial burden. According to studies, the cost of cybercrime accounts for 1% of global GDP, with small businesses experiencing an average cost of $120,000 to $1.24 million per cyberattack [22]. In the past three years, this burden has surpassed $19 trillion and is projected to reach $23 trillion annually by 2027 [24].

Image 2: Cybercrime projected cost per year [24]

Frequently, individuals and organizational administrations underestimate the risk posed by cyber attacks, viewing it as an abstract concept that does not pertain to their surroundings. Nonetheless, such attacks occur continuously and are a prevailing occurrence in both the domestic and international environment, targeting critical infrastructures directly. In order to comprehend the scale of the issue, a concise depiction of its most distinct characteristics is presented below.

2.1 Significant Cyber Attacks in Greece

Greece is not immune to the threats of cyber attacks aimed at damaging its critical infrastructures, disrupting services, or stealing confidential information. Recent attacks on prominent and significant organizations in the country demonstrate how close the threat is to us. A study cited as [22] revealed that Greece was ranked ninth in the international table of recorded internet-related crimes in 2021.

2.1.1 Telecommunications Provider

In October 2020, the largest mobile network provider in Greece [25], announced the detection of a cyberattack on its systems. The attack resulted in the unauthorized export of a file from one of the company's systems using the Remote File Inclusion (RFI) technique. The file contained information used by the company for network and service optimization, such as phone number, date and time, call duration, device type, age, and gender. Despite the fact that there was no disruption of its essential services and the company denied that the attackers had accessed any of the contents of the conversations and messages, the cyber-attack had serious financial consequences. The Hellenic Data Protection Authority imposed a fine of €6,000,000 on the company [26], and ordered it to cease data processing and destroy the leaked information. The parent company, was also fined €3,250,000 for the exposure of call data of thousands of subscribers.

2.1.2 Large-scale Municipality

In July 2021, the second most populous municipality in Greece [27], suffered a ransomware cyber attack [28]. The attack caused the municipality's systems to become partially or fully non-functional for over two months [29]. In addition, a leak of personal data belonging to natural persons was discovered and the cybercriminals demanded ransom in exchange for the data. The situation was so severe that the data of GIS applica-

tions of the municipality were rendered inaccessible [30], with no hope of recovery. Consequently, the municipal service lost thirteen years of archival material.

2.1.3 Postal Services

A very large greek postal services organization recently reported a cyber attack on its information systems [31] on March 21st, 2022, which was perpetrated through the use of malicious software and it resulted in the complete isolation of the company's data center. The attack targeted the encryption of critical systems for the operational functionality of the organization and started from zero-day malware that was installed on a workstation and connected to a computing system through the https reverse shell technique, which was controlled by a cybercriminal group. The entirety of the functionality of the systems was restored after a period of seventeen days [32], and in addition to the impact on operational functions, there was an immediate financial impact. This is evident in the Program of Acts Posting on the Internet (Diavgeia), where the administration was forced to engage in at least nine procurements to external providers [33] in order to mitigate the impact of the attack, at a total cost of €1.847.942.

2.1.4 Gas System Operator

On August 20th, 2022, the Greek organization responsible for operating, managing, exploiting, and developing the national natural gas system (NNGS) and its interconnections, disclosed a cyber attack on a portion of its information infrastructure [34]. Cybercriminals attempted to unlawfully access electronic files, resulting in a confirmed impact on the availability of some systems and potential leakage of files and data. In response, the organization proactively disabled most of its information infrastructure services and chose a gradual restoration approach, choosing not to negotiate with the cybercriminals.

2.2 Notable Cyber Attacks on Critical Infrastructures Abroad

As expected, on a global scale, there has been an increase in cyber attacks on critical infrastructures in recent years, with increasingly sophisticated methods and techniques. The following chart presents the evolution of the most significant cyber attacks of the last five years related to state interventions and cyber espionage in government services, defense and high-tech companies, or economic crimes with losses exceeding one mil-

lion dollars [35]. It is noteworthy that these attacks constitute only a small subset of the total number of cyber attacks, indicating the magnitude of the problem.

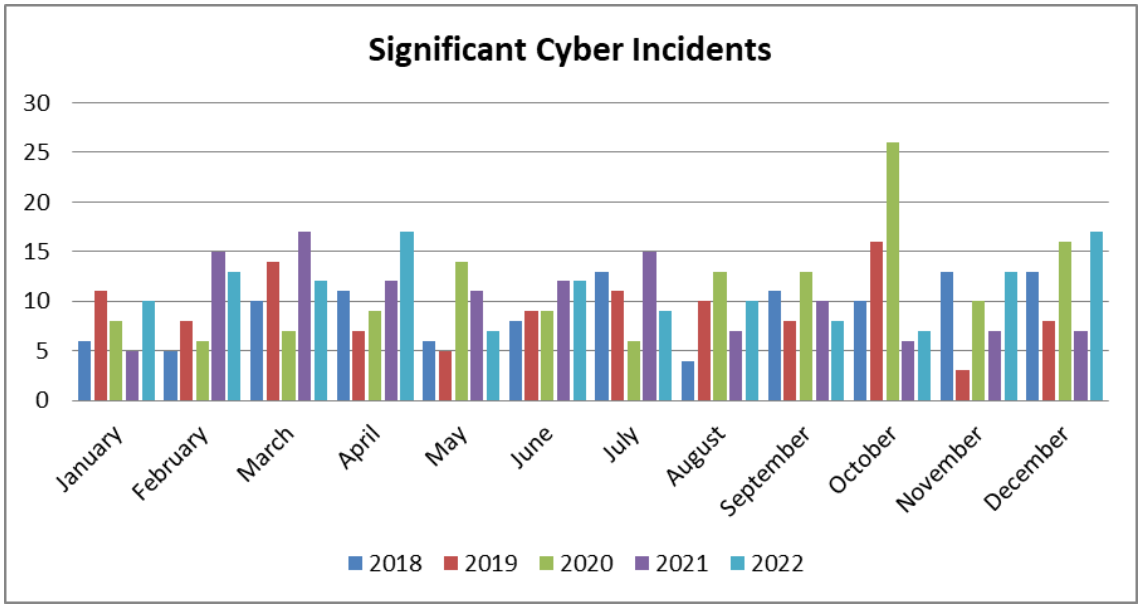

Image 3: Cyberattacks costing more than $1 million (data provided by [35])

In the following subsection, we present the description of some of the most characteristic cyber attacks that have targeted critical infrastructures worldwide.

2.2.1 Stuxnet

In 2010, the malicious software Stuxnet emerged, specifically designed to target Industrial Control Systems (ICS) [36]. This case is particularly notable as it targeted the logical programmable controllers manufactured by Siemens that were used in the Iranian nuclear program, delaying it for years by gradually and without trace destroying the centrifuges used in nuclear material separation, [37]. Analysis of Stuxnet revealed that it combined zero-day vulnerabilities, anti-detection techniques, and specialized propagation, making it ideal for high-security air-gapped environments.

2.2.2 Water Supply Network in the City of Oldsmar, USA

On the 5th of February 2021, unidentified attackers gained unauthorized access to the SCADA system of the drinking water treatment facilities in the city of Oldsmar, USA, possibly exploiting outdated systems or weak access codes [38]. The assailants utilized the SCADA system software to increase the quantity of sodium hydroxide, a caustic chemical substance, during the water treatment process. The personnel promptly noticed

the change in dosage quantities and rectified the issue before the authorized change was completed, thus averting a potential ecological disaster and loss of human lives.

2.2.3 Colonial Oil Pipeline

On May 7, 2021 [39], the administrator of the largest pipeline system for oil refining products in the United States fell victim to a ransomware attack and was forced to preemptively disable the infrastructure's pipeline system in order to limit the damage. Due to the scope of the problem, the US government was compelled to declare a state of emergency in at least 18 states [40]. A characteristic of the attack was the use of ransomware-as-a-service (RaaS) software to target the infrastructure's information systems, while at a later stage the perpetrators threatened to release the data.

2.2.4 SolarWinds

Finally, in 2020, one of the largest cyberattacks ever to occur in the United States was identified and officially attributed to Russia. Its defining characteristic was that it was a supply chain attack [41] and an Advanced Persistent Threat simultaneously. Specifically, the attackers introduced malicious software into the source code of the network monitoring and remote management application, SolarWinds, so that they gained illegal access to the information systems of legitimate users during distribution. The attack affected government agencies, critical infrastructures, and private sector organizations, while the CISA considers the removal of the threat actor from the compromised environments to be a significant challenge and extremely complex.

3 Critical Infrastructures and Cybersecurity Legal Context

Cybersecurity is now a matter of primary concern in the European Union. In recent years, significant and systematic efforts have been made both at the level of companies and organizations, as well as at the level of states through the fortification of the regulatory framework with appropriate directives, regulations, and laws related to cybersecurity, in order to combat cyber threats. This step constitutes the first and most important stage in the horizontal approach to addressing all areas of cybercrime, as it defines the nature of cybercrime, identifies the entities responsible for combating it, and establishes general procedures and measures for its mitigation.

Regarding Greece, in 2020 it was ranked 35th in the Global Cybersecurity Index [42] with a score of 94/100, which evaluates the commitment and dedication of countries to implementing measures regarding cybersecurity across dimensions such as legislation, technology, organization, capacity building, and cooperation.

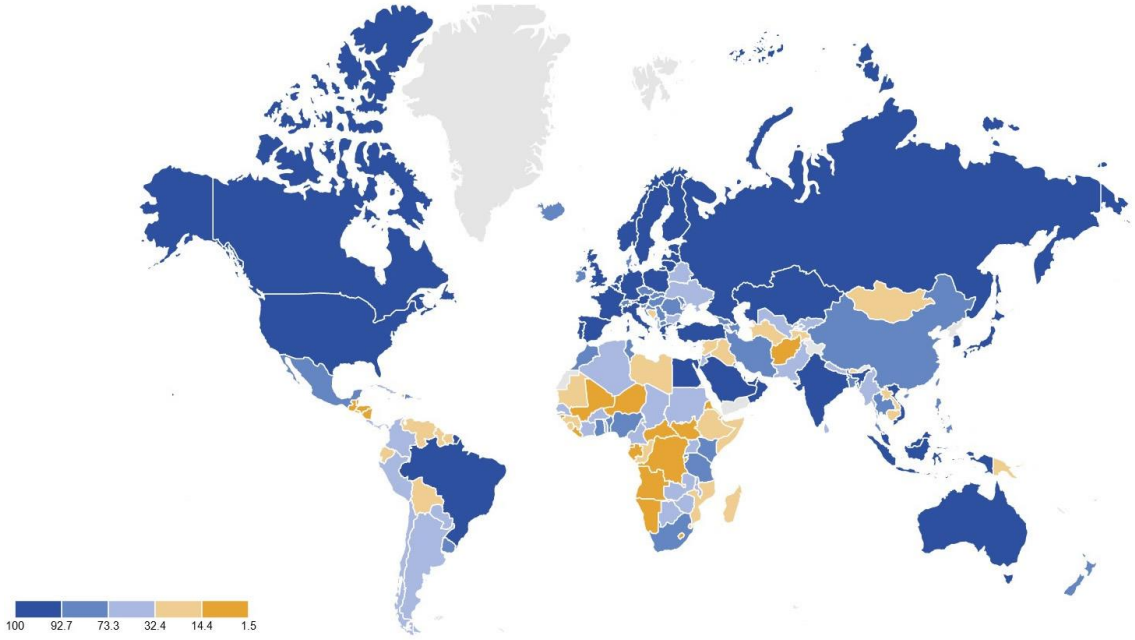

Image 4: Global Cybersecurity Index 2020 [42]

The effort of the involved parties in this matter has a longstanding history and comprises of three distinct stages over the years. The first stage, known as the compliance era (2008-2012), recognized the significance of cybersecurity and established fundamental regulatory standards. From 2012 to 2018, the focus shifted towards risk management and resilience, whereas the period spanning 2018 to 2025 is regarded as the era of indispensability for the implementation of security measures at all levels, both within and beyond organizations [43]. The critical milestones of this progression are outlined below.

3.1 Cybersecurity at the National Level

A multitude of regulatory provisions have been created to combat malicious activity directed at critical infrastructures, which either explicitly or implicitly address the cybersecurity of these entities. At this point, the most significant legal framework, guidelines, and regulations that encompass the cybersecurity of critical infrastructures are presented, acting as a deterrent for the perpetration of cyber attacks.

3.1.1 Budapest Convention

The adoption of the Budapest Convention [44] in 2001 by the Council of Europe, which establishes a uniform framework for the criminalization of digital crimes, is regarded as a pivotal moment in acknowledging the significance of tackling cyber threats. It defines the mandatory steps that each state should take to combat crimes that violate the confidentiality, integrity, and availability of data and computer systems, computer fraud, offenses concerning data content (such as child pornography), and copyright-related offenses. The aforementioned convention also establishes law enforcement measures and penalties for these types of crimes, as well as guidelines for cross-border cooperation. The Greek state ratified the Budapest Convention in 2016 through the enactment of Law 4411/2016. This law also adopted the provisions of EU Directive 2013/40/EU, which calls for a unified approach to criminal law in response to attacks against information systems and critical infrastructures.

3.1.2 Directive 2016/1148 (NIS) on Network and Information Security in the EU and NIS 2

As part of its efforts to enhance cybersecurity in critical infrastructures, the European Union implemented the 2016/1148 Directive, also known as the Directive on Security

of Network and Information Systems (NIS). The directive aims to improve and standardize the level of security in network and information systems across the EU that is deemed critical, including Digital Service Providers and Essential Service Operators. The directive is a significant milestone in a series of actions to mitigate significant disruptions to critical infrastructures. Important provisions of the NIS Directive include:

- Mandating every Member State to design a strategy to promote the security of network and information systems.
- Strengthening cross-border cooperation between Member States through the Cooperation Group, while ensuring the protection of their national interests.
- The directive establishes the competent authorities and a single contact point, and defines the way in which they cooperate and communicate with each other. It also strengthens the capability for a unified response to cybersecurity incidents by creating Computer Security Incident Response Teams (CSIRTs) and Computer Emergency Response Teams (CERTs).
- It establishes the basis for the prevention, detection, response, and mitigation of incidents and risks to network and information systems through appropriate technical and organizational measures and procedures, for which the responsibility now lies with the critical infrastructure operator.
- The Directive also obligates operators to notify incidents deemed to have a significant impact on the provision of essential services.

The aforementioned Directive entails an obligation for Greece to develop a national strategy for securing network and information systems. This will ultimately result in the adoption of the National Cyber Security Strategy by the Greek state.

Directive 2022/2555 (NIS 2) serves as an additional measure to the NIS Directive and complements it, advancing towards a more comprehensive and harmonized approach to cybersecurity within the EU. As stated in reference [45], the directive expands its reach to a larger section of the economy, encompassing small businesses that hold significant societal roles, categorizing them as either key or important entities. Moreover, it eliminates disparities among member states regarding the definition of FIUs and establishes a baseline for incident notification and risk management. Furthermore, it establishes the European Network of Cyber Crisis Liaison Organisations (EU-CyCLONe).

Law 4577/2018, Ministerial Decision 1027/2019

The NIS Directive was implemented into Greek legislation via Law 4577 of 2018 [1]. Ministerial Decision 1027/2019 while Government Gazette 3739/B/8-10-2019 further specified important implementation issues and procedures. This legislative text expands the scope of the framework for action, as it delineates the responsibility of organizations for their actions, including those of their partners. It also outlines the sanctions and procedures for their imposition in the event of a failure to meet the obligations set forth in the legislative framework. Additionally, it provides precise qualitative and quantitative criteria for identifying a facility as an operator of an essential service. A facility is considered such and operator if it provides a service that relies on digital systems and covers at least one of the following areas [46]:

Table 1: Sectors and subsectors of essential services providers [46]

Sector	Subsector
Energy	Electricity
	Petroleum
	Gas
Transportation	Aviation
	Railway
	Maritime
	Road transport
Banks	
Financial Market Infrastructures	
Healthcare	
Water	
Digital Infrastructures	

Simultaneously, the document outlines in abstract form the manner in which suitable technical and organizational measures, as well as fundamental security requirements, must be adhered to. The framework for this compliance must be detailed within each organization's security policy. A noteworthy component of this Information Security Act is the creation of the Information and Network Security Officer position within the organization. This individual is tasked with supervising the implementation of the pertinent obligations. As for NIS 2 Directive, the deadline for implementing the measures required to comply with it by the Greek state is December 24, 2024 [45].

For the purpose of providing a more comprehensive and thorough discussion, it is necessary to enumerate the 16 key critical infrastructure sectors identified by the United States [47], which will allow the reader to familiarize themselves with the critical infrastructure sectors of the largest economy in the world:

Table 2: US Critical Infrastructure Sectors [47].

Chemical industry	Communications	Dams	Emergency Services
Financial Services	Government Facilities	Information Technology	Transportation Systems
Commerical Facilities	Critical Manufacturing	Defence Industrial Base	Energy
Food and Agriculture	Healthcare and Public Health	Nuclear Reactors, Materials, and Waste	Water and Wastewater

3.1.3 European Cybersecurity Strategy

The European Union is engaged in several initiatives and partnerships with various stakeholders to advance a transparent, resilient, and secure cyberspace rooted in the values of the rule of law, as set forth by its principles and within the wider context of the EU Defense Strategy [48]. In accordance with this objective, the European Union adopted the European Cybersecurity Strategy in February 2013, and a revised version was subsequently published in December 2020. The overarching goal of this strategy is to guarantee the quality of digital services for the betterment of citizens, while also safeguarding the fundamental values of the European Union [49].

The European Union has demonstrated its commitment to the European Cybersecurity Strategy by approving a significant increase in funding [50], which is four times higher than the current budget, for the next seven years [51]. This increase in funding is intended to enable the integration of cybersecurity across all of the EU's key activities. One of the main objectives of this strategy is the establishment of a European Cyber Shield, which will be achieved through various means such as cooperation, collective secure information and knowledge sharing, skills development, strengthening networks and interconnected devices, building additional European infrastructure, supporting the supply chain, diplomatic means to strengthen defence [52], and increasing participation in standardisation processes.

3.1.4 National Cybersecurity Strategy

In alignment with the European Union, Greece issued its National Cybersecurity Strategy 2020-2025 in December 2020, outlining a five-year plan and action plan to achieve its cybersecurity objectives [53]. The primary aim of the strategy is to establish a secure internet environment, infrastructure, and services that promote prosperity and enhance citizens' confidence in adopting new digital products and services while safeguarding their fundamental rights. The National Cybersecurity Strategy 2020-2025 specifies sectoral objectives in a detailed framework of actions. It emphasizes the need for a unified response to threats and sets out measures to limit the scope and impact of cybersecurity incidents. It also analyzes the expanded attack surface, maps the main modern types of cyber-attacks, classifies the sources of threats, and presents the revised institutional shielding of the country against cyber threats. Furthermore, the strategy highlights the importance of strengthening the culture of the entire society (citizens, public/private sector) through capacity building, promoting awareness, and raising awareness of cybersecurity issues. Additionally, it emphasizes the promotion of research and development through the investment environment.

3.1.5 Cybersecurity Act

In June 2019, the European Union strengthened its cybersecurity legislative framework by enhancing the role of the European Cybersecurity Agency and establishing a unified certification scheme for products and services across the EU, while also creating the European Cybersecurity Certification Group (ESGCG) [54]. The primary aim of certification is to enable users to evaluate the cybersecurity risk associated with a specific product, service, or process by establishing a shared understanding among stakeholders from various member states through the EU Cybersecurity Certification Framework.

3.1.6 GDPR Regulation (EU) 2016/679

As of 25 May 2018, all EU member states were required to comply with the General Data Protection Regulation (GDPR) [55]. Greece ratified the implementing law in 2019 [56]. One of the main goals of the GDPR is to safeguard the personal data of EU citizens by regulating and limiting the processing of personal data and protecting them against breaches.

The concept of personal data encompasses information that permits the identification of individuals either directly or indirectly, and it is deemed a valuable asset that merits

safeguarding. The primary principles set forth in the Regulation furnish a structure for the just, equitable, and transparent handling of data, which is restricted to defined objectives. The data collected must be both precise and indispensable, retained for no longer than necessary, and while stored, must be assured of its integrity and confidentiality by data controllers, who bear responsibility and accountability for these obligations by design and by default. The necessity for a Data Protection Officer (DPO) is determined based on the scale of processing and the nature of data. The DPO is responsible for advising the controller, monitoring compliance with GDPR, and cooperating with supervisory authorities when necessary. Failure to comply with GDPR may lead to severe financial penalties, which underscores the importance of compliance. This creates an impetus for cybercriminals who attempt to gain unauthorized access to data, subsequently coercing legitimate data controllers into paying for the data's release, thus attracting regulatory consequences.

3.1.7 Electricity Sector Risk Preparedness Plan

The Hellenic state, acknowledging the crucial nature of the electricity sector and the necessity of readiness to confront and handle crises in this domain, approved a relevant scheme in September 2022 [57]. According to this the risks are classified in terms of their likelihood of occurrence and the magnitude of their impact. Among the most prominent risks are cyber attacks, and the plan outlines specific measures to mitigate their effects at the national level. Additionally, the plan describes the crisis management mechanisms for cybersecurity incidents.

3.2 Cybersecurity entities

The growing complexity of cyber threats requires a coordinated response from both public and private actors. In Europe, the protection of critical infrastructures follows a particular model where the state establishes a dedicated organization responsible for safeguarding critical infrastructures, which in turn formulates policies to address cyber threats [58].

It appears that the Greek state has adopted a mature stance towards the subject of cybersecurity, and has established multiple entities with distinct responsibilities to address and enhance protection and cybersecurity measures for critical infrastructures. As such, it is essential to detail the specific duties of these entities.

3.2.1 National Cybersecurity Authority

The National Cybersecurity Authority has been upgraded to the General Directorate of Cybersecurity and is part of the General Secretariat of Telecommunications & Post of the Ministry of Digital Governance. It serves as the National Competent Authority and the primary point of contact for network and information system security throughout the country. Additionally, it is responsible for developing and managing the National Cybersecurity Strategy. It collaborates with other relevant authorities, outlines suitable organisational, technical, and operational measures required by Critical Infrastructure Operators, coordinates these Operators, and establishes the framework for managing any cybersecurity incidents [53].

3.2.2 National Authority for Mitigating Cyber Attacks - National CERT

The aim of the National Cyber Attack Response Authority, also known as the National Computer Emergency Response Team (CERT), is to ensure the prevention, timely detection, and effective response to cyber attacks within its jurisdiction. Specifically, it provides support to the Presidency of the Government, the Ministries, and their associated entities, with the exception of the Ministry of National Defence, in preventing, detecting, and responding to cyber attacks aimed at them [53]. Also, it collaborates with other Computer Security Incident Response Teams (CSIRTs) [59], public sector agencies, and national and international entities responsible for cybersecurity matters, coordinating actions in case of critical situations and implementing the National Strategy for responding to cyber threats both national and international level [60].

3.2.3 Cyber Defence Directorate

The Cyber Defence Directorate, which is under the Hellenic National Defence General Staff and attached to the Ministry of National Defence, is responsible for incident response in the military sector and critical infrastructure operators, serving as the Greek Computer Security Incident Response Team (CSIRT). However, its mandate is limited by legislation when cyber attacks target purely civilian entities, as the National Cyber Attack Response Authority - National CERT is responsible for responding to such incidents [53], [1].

3.2.4 European Cybersecurity Organization (ENISA)

ENISA was established in 2004 as per Regulation 460/2004 [61] with the purpose of promoting a culture of network and information security across Europe and ensuring a high common level of cybersecurity. The organization's role was subsequently strengthened in 2019 through the implementation of the Cybersecurity Act. Apart from its advisory and coordinating role, ENISA is involved in the collection and analysis of information security data and contributes to the Union-wide response in the event of large-scale cross-border cybersecurity incidents and crises [54]. In essence, ENISA is instrumental in shaping EU cyber policy, enhancing the reliability of ICT products, services, and processes through cybersecurity certification schemes, collaborating with Member States and EU entities, and assisting Europe in preparing for future cyber challenges. It is worth noting that ENISA does not impose any new obligations on private sector entities or Member States.

3.2.5 Hellenic Data Protection Authority (HDPA)

The Hellenic Data Protection Authority is a constitutional independent authority that was created through Law 2472/1997 [62]. Its role is to supervise, regulate and control the implementation of all aspects concerning the protection of individuals' personal data during the processing thereof, as stipulated by Law 4624/2019 [56]. This regulatory body is the designated recipient to whom data controllers must report any data breach incidents within 72 hours of their discovery, providing all necessary information requested by the Authority.

3.2.6 Cybercrime Division

The Cybercrime Division was created through the issuance of Presidential Decree 178/2014 (A' 281), and operates directly under the auspices of the Chief of the Hellenic Police. The division is tasked with the investigation of cybercrime cases [63]. Its primary responsibilities involve the prevention, investigation, and eradication of criminal activities and disruptive behavior perpetrated through the use of the internet.

3.2.7 Hellenic Telecommunication & Post Commission (EETT)

This Independent Administrative Authority operates in accordance with the regulations specified in Government Gazette 82/A/2012 [64]. It serves as the National Regulatory Authority (NRA) in the domains of electronic communications and postal services.

3.2.8 Hellenic Authority for Communication Security and Privacy (ADAE)

Established in 2003 [65], this independent authority operates with administrative autonomy and aims to safeguard the confidentiality of correspondence, ensure the freedom of communication through any means, and enhance the security of networks and information.

3.2.9 Center for Security Studies (KEMEA)

Supervised by the Ministry of Citizen Protection (Law 3387/2005 A' 224) [66], this organization serves as an advisory, consultative, and research entity concerning security policy matters, while simultaneously engaging in collaboration with other national and international bodies to promote security.

PART 2: Threat Landscape

4 Contextualizing Cyber Threats

Cybersecurity threats are intricately linked to a rapidly changing and dynamic environment that is influenced by a multitude of factors. This environment is known as the threat landscape and includes a spectrum of potential and actualized risks that can have adverse effects on the cybersecurity of all involved parties. The magnitude of the target in question, as well as its impact on society, directly correlates with the level of risk involved [53]. The threat landscape comprises various elements, such as the possible perpetrators of cyber-attacks, including both the entities responsible for carrying out the attacks and those who initiate them. It also encompasses the underlying motives that drive each attacker, the circumstances that prompt such attacks, and the methods and techniques employed to exploit system vulnerabilities [8]. These fundamental concepts are interconnected and have a significant impact on the overall cybersecurity ecosystem.

4.1 Understanding the Concept of Cyber Threats

To begin with, it is crucial to establish a clear definition of the term "cyber threat." There are numerous definitions in the literature, one of which is the following from NIST [67]:

> “Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.”

In a simpler form, a threat could be defined as any factor that has the potential to compromise security and jeopardize the valuable assets - information and property - of its possessor. These assets can be categorized as either tangible or intangible. The former

encompasses physical assets such as hardware, computing platforms, and other technological devices, while the latter includes software, human resources, data (including customer, identification, financial, etc.), processes, services, intellectual property, confidential corporate information, and the proper functioning of facilities [68].

Table 3: Asset categories [68].

Asset class	Description
Materials resources and infrastructure	Material assets such as buildings, infrastructure, equipment, and natural resources (e.g., water and electricity), as well as the organization's facilities and infrastructure.
System capacity	The system's capacity to operate efficiently and as intended.
Human resources	The personnel of the organization.
Intellectual property	Anything that contains confidential information and provides the organization with a competitive advantage.
Data and information	All data and information in any format.
Derivative non-tangible	The organization's image, reputation, and the confidence of others in it, which depend on the organization's ability to protect its assets.

Likewise, cybersecurity incidents or cyber-attacks can be characterized as unfavorable events resulting from undesirable internal and/or external factors that violate established rules, thus impeding individuals and organizations from either preventing access to a specific piece of information or accessing information in its intended form at a particular time, exposing confidential information, or altering or destroying information or material. These two concepts should not be conflated, as the threat does not consist of the attack per se, but rather the potential for the attack to take place.

To summarize, cyber threats arise from the exploitation of system security vulnerabilities by individuals, groups, organizations, or government entities with the aim of causing a security incident that compromises at least one of the key security properties. Each of these entities, referred to as a threat actor, has distinct interests and objectives that it seeks to achieve by executing the attack and is determined by a combination of one or more threat dimensions, except in cases of unintentional human error. Attackers may target information and assets that are physical (e.g., information storage devices), logical (e.g., services), or intangible (e.g., reputation), depending on the perceived benefits of undermining these assets [13].

It is evident that cyber threats have a variety of impacts such as data loss or corruption, mechanical equipment damage, service unavailability, economic costs, reputational

damage, loss of customer trust, and in severe cases, potential risks to human safety and the environment [68].

Based on the above discussion, a threat is the result of a combination of three elements [69]: the attacker's motives and objectives, their capabilities to execute the attack, and the opportunities available to them (such as time, knowledge, and exploitable vulnerabilities).

Threat = Capability + Intent + Opportunity

Viewed from the organization’s perspective, the combination of attacker motivation and capability is a passive factor, as it is beyond their control. However, the opportunity dimension represents an area that organizations can actively manage through the implementation of appropriate technical and organizational measures, such as system hardening, authentication controls, and awareness initiatives.

Image 5: Components of cyber threats [69]

As depicted in the aforementioned figure, the overlap of each component with the others delineates distinct scenarios brought forth by threat actors.

- The imminent threat arises from the conjunction of hostile intent and capability, but its materialization necessitates the presence of opportunity.
- The potential threat is engendered by the combination of capability and opportunity, but its fruition hinges on the inclusion of hostile intent.
- The actual threat is the combination of hostile intent and opportunity, with the attacker's capability being a requisite component for its actualization.

The correlation between the attackers' capabilities and motivations and the potential threats they pose is readily apparent. This relationship gives rise to the concept of risk, which refers to the anticipated loss of security of an asset, whether it is information or property, due to the exploitation of vulnerabilities by an attacker. It should be noted that while a threat is a negative occurrence, risk is the likelihood and consequences of the negative event. It follows that the higher the number of threats and vulnerabilities, the greater the risk posed to the organization.

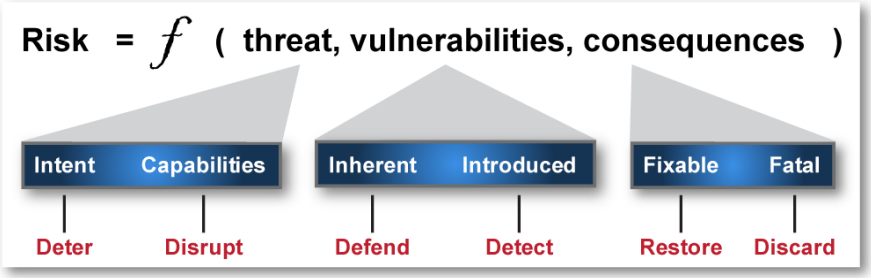

Image 6: Cyber threat risk [70]

The risk posed by cyber threats can be conceptualized as a function of the threats themselves, the vulnerabilities inherent in the system, and the potential consequences of a successful breach. In line with the previously discussed components of threats, vulnerabilities can be either intrinsic or extrinsic, and the impacts of a breach can be classified as either manageable or catastrophic. While it is impossible to completely eliminate risk, it is important to consider the interconnectedness of all risk parameters as a single system [70]. Risk reduction is accomplished through the minimization of its individual elements, namely probability, vulnerability, impact, and duration/severity of impact. To mitigate the potential impact, it is crucial for the infrastructure to be resilient. Resilience is the ability of the system to withstand an adverse event, with no service interruption or, if unavoidable, to restore the service promptly, while keeping the risk of service outage minimal. A system or asset that is completely resilient would ideally have zero risk of any outage, irrespective of the threats posed [71].

4.2 The CIA Triad

To delve further, incidents related to cybersecurity are intertwined with information assets, arising from the inability to secure or violation of one or more of the Confidentiality, Integrity, Availability traits that constitute the essential design of a sturdy

and resilient information system, known as the CIA triad. These principles are considered foundational in information security [72], [73]:

- Confidentiality: processing of information must be restricted to authorized individuals, entities, or processes.
- Integrity: the format of the information must be processed in a manner that ensures it remains in its correct and accurate form, with the ability to provide evidence of this fact.
- Availability: Information should be accessible to authorized users at any time when requested.

In conjunction with the aforementioned characteristics, additional properties of great significance are Authenticity, which pertains to the verification of the identity of different entities, Accountability, which pertains to the determination of responsibility in the event of information misuse, Non-repudiation, which pertains to the ability to demonstrate that any event originated from a particular entity, and Reliability, which pertains to the predetermined consistency of the results related to information processing [72]. The figure depicted below illustrates the expanded set of information security attributes within the ecosystem.

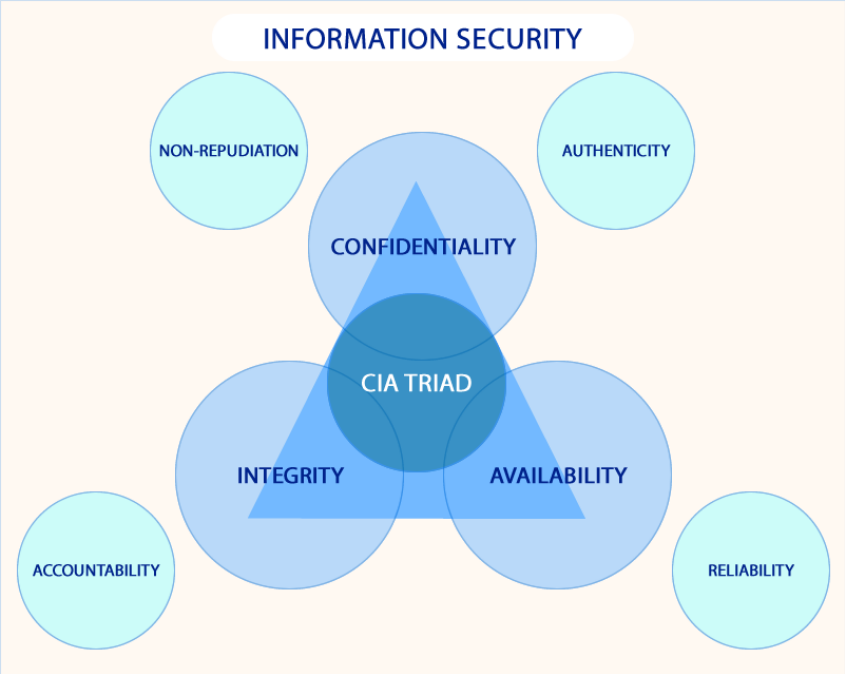

Image 7: The ecosystem of Information Security

The subversion of any of the aforementioned properties represents the ultimate objective of various actors with distinct intentions, producing negative consequences on the

system. Therefore, cybersecurity endeavors to implement countermeasures, encompassing techniques, procedures, and actions, to diminish threats by eliminating and preventing vulnerabilities or minimizing their impact. The objective of such measures is to safeguard the vital security attributes of information infrastructure components.

Each sector of critical infrastructures is exposed to specific risks and recognizes distinct threats regarding each information security aspect. The banking and financial sector, for instance, perceives confidentiality threats differently from the more technical infrastructures. In the context of nuclear power plants, the availability and integrity of the information assets that constitute their operations are regarded as the primary concern, whereas confidentiality may be accorded less importance. Industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and similar automation systems are highly valued assets whose compromised functionality would have significant repercussions [74]. Analogously, the proper functioning of brakes in vehicles is essential, as opposed to the confidentiality of saved radio stations. It is essential to note that this point does not negate any of the elements that comprise the overall cybersecurity ecosystem.

While the theoretical underpinnings of the CIA triad may not appear to have practical implications for everyday life, it is evident that the cybersecurity of critical infrastructures is an exception. For instance, the cyberattack on the water supply network of Oldsmar in the US exemplifies the potential risk to citizens' lives arising from a breach of data integrity. Similarly, the Stuxnet attack affected the availability of systems by causing significant delays in the Iranian nuclear program. The telecommunication provider incident, which resulted in the unauthorized disclosure of personal data, illustrates the importance of maintaining confidentiality to avoid regulatory non-compliance and potential harm to data subjects.

4.3 Cybersecurity Threat Factor Classification in Critical Infrastructures

At present, cyber threats to critical infrastructures extend, either independently or as a whole, to specific dimensions that constitute the attacks.

4.3.1 The Influence of Technology

In the present era, critical infrastructure systems face significantly greater exposure than in the past. The shift from traditional processes to digital applications and the need for interconnectedness between different systems has significantly expanded the attack surface, making previously isolated systems accessible not only within the internal network but also beyond to internet-accessible infrastructure.

The introduction of Internet of Things (IoT) devices into crucial infrastructure networks, although a major advancement that enables more efficient performance and communication, increases the risk of unauthorized access [75] due to the large number and heterogeneity of devices required.

Moreover, the adoption of software as a service in the cloud has further increased the attack surface by exposing data to new risks that did not previously exist. The need to reduce costs and standardize systems has led to the abandonment of proprietary technology solutions in favor of commonly available market solutions, whose vulnerabilities may be known to attackers.

In many cases, the infrastructure design was implemented several decades ago when technologies and implementation techniques were completely different, without security logic by design and by default, rendering these solutions unsuitable for the modern era [76]. The continuous advancement of hardware capabilities, along with the rapid development of artificial intelligence, enables attackers to detect and exploit new vulnerabilities at an accelerated pace.

Moreover, while implementing security best practices and keeping pace with technological advancements are crucial, they also result in significant administrative and financial costs, causing many organizations to use outdated technological solutions in both hardware and software [12]. This, in turn, creates security gaps that can be exploited by attackers to serve their purposes, whether they are known or zero-day vulnerabilities. A prime example of this issue is the Tokyo Electric Power Company (TEPCO), which operates the Fukushima nuclear power plant. In 2014, TEPCO was using 48,000 terminals that were running the Windows XP operating system [77], for which Microsoft had already stopped providing security upgrades.

The aforementioned factors, coupled with inadequate staff training, and the consequent lack of awareness and culture surrounding cybersecurity on the part of both personnel (e.g. utilization of USB flash drives) and management (e.g. deficiency of security poli-

cies and appropriate procedures), result in infrastructures being vulnerable to risks that could have been readily alleviated by the implementation of sound security practices.

On the other hand, technological advancements have bestowed hackers with novel tools and channels of communication (such as the Dark Web and Tor network), which enable them to remain anonymous, thus rendering their detection exceedingly challenging and time-intensive [78].

4.3.2 The Social Dimension Within the Context of Critical Infrastructure Security

The Covid-19 pandemic has caused significant disruptions to various facets of society, including the economy, social structures, familial life, working conditions, education, and mobility across borders. These changes have resulted in a newly expanded attack surface, as modifications in technology usage brought about by new demands and behaviors have given rise to new vulnerabilities and threats that were previously either nonexistent or limited in scope. This is due to the fact that work and educational processes have become predominantly reliant on digital infrastructure [79]. According to studies, the COVID-19 pandemic has resulted in a 600% increase in cybercrime [22].

The limitations on human contact brought about by the Covid-19 pandemic have resulted in a hurried adoption of new digital communication channels, leading to a significant surge in data transmission [80]. Unfortunately, the urgent nature of the measures implemented did not allow for the necessary time to establish a culture of secure information asset use among staff, nor for the required technical preparations to enable timely work from home (WFH) arrangements. For instance, in 2020, there was a 41% increase in RDP endpoints [81], which made it extremely challenging for IT staff to configure and manage all the essential information assets, thus leading to an increase in security breaches [82]. Additionally, the infrastructure was not adequately prepared for the surge in data usage, which facilitated distributed denial of service attacks as bandwidth had to be allocated for remote working solutions. Consequently, attackers exploited this situation by using the pandemic's created needs (such as parcel deliveries and public information on the pandemic's progress) to deceive people through misleading emails, fake applications, and other means [79].

In addition to the impact of technology, it is worth noting that the institutional framework for teleworking in Greece was only completed two years after the onset of the pandemic, in June 2021, with the passing of a law which outlined the technological

means for protecting the information of remote workers [83]. The HDPA also issued guidelines two months later, aimed at improving the protection of personal data [84].

The convergence of various factors, such as the BYOD culture and the blurring of boundaries between personal and professional use, has resulted in the mixing of personal and corporate data and the sharing of information across multiple devices and locations, which are typically not as well secured due to the lack of necessary knowledge or technology [43]. Consequently, this has led to an increasing vulnerability in maintaining data confidentiality, particularly for critical infrastructures such as healthcare facilities that handle large amounts of personal and sensitive information, making data breaches in the healthcare industry among the most costly [85]. During the pandemic, hospitals have become a prime target for cyber attacks due to their critical role, limited countermeasures, and operational pressures [79]. The evidence indicates that the costs associated with data breaches involving teleworking were significantly higher than those of traditional breaches [85].

The digitization of social life has resulted in the emergence of new communication patterns that are more susceptible to social engineering attacks and threat detection through social networks. Additionally, social networks have introduced changes to the way people socialize, which has contributed to the risk of identity theft and the accumulation of personal data. As a result, identity fraud has become a significant concern, where these data are exploited for malicious purposes [86].

The adoption of intangible money and cryptocurrencies has brought about significant changes in the financial landscape. This has led to the diversification of financial transactions, resulting in a more straightforward and less transparent process for collecting funds from illicit activities. The adoption of cryptocurrencies has also increased the activity of cybercriminals through the use of illegal marketplaces [78]. Unlike traditional banking, cryptocurrencies lack a centralized supervisory authority and a regulatory framework, making them an ideal medium for trading rewards derived from criminal acts. The increased anonymity of cryptocurrency traders further exacerbates the situation, as it provides cybercriminals with the opportunity to profit from their criminal activities [87].

4.3.3 Motivational Factors of Malicious Actors in the Digital Environment

The objectives of every attacker are directed towards four broad domains that are often interrelated. The initial domain concerns cybercrime that is linked to the exploitation of the victim's information, typically for personal gain. The second domain pertains to cyberterrorism, which involves the utilization of violence via the internet for pursuing particular objectives. This is followed by cyber espionage, which involves the act of secretly gathering confidential information. Lastly, the fourth domain refers to cyber warfare, which involves the conduct of war through the internet [88].

Despite the existence of a strict legal framework aimed at preventing online criminal activities, the allure of such actions persists. The motives that drive attackers to engage in cyber-attacks represent a critical dimension of this issue, particularly given the vital nature of critical infrastructures. As such, the factors contributing to these motivations differ from those present in other domains. The following are among the most significant components that shape these motivations.

On the pursuit of utilitarian objectives

Acquiring some form of gain at the expense of either individuals or legal entities is a critical element in committing cybercrime and is associated with corrupting the victim's information or stealing their data, regardless of whether the attackers work independently or on behalf of others [88]. These benefits may be motivated by revenge or may be purely for the amusement of the attackers, enhancing their self-esteem and elevating their prominence and recognition among specific groups in their network, or, most frequently, they may be driven by economic incentives.

One way in which victims may be exploited is through direct theft of assets, such as illegal money transfers or the opening of fake bank accounts. However, other methods involve unauthorized access to victim data and information (e.g. extortion) or the manipulation of their data (e.g. ransomware), followed by blackmailing for non-disclosure or restoration to their previous state. In the case of Colonial Oil Pipeline, there are reports indicating that the company paid a ransom of $5 million in bitcoin to regain access to their systems and resume operations [89].

Another motive for cyber-attacks is to sell stolen data, such as credit card numbers, phone numbers, and passwords, on the online black market for use in other criminal activities. The value of the data is determined by various factors, such as its type (e.g. per-

sonal or financial data), the sector of the business to which it pertains, whether it grants access to an internal corporate network, and the profits of the business to which the data belongs.

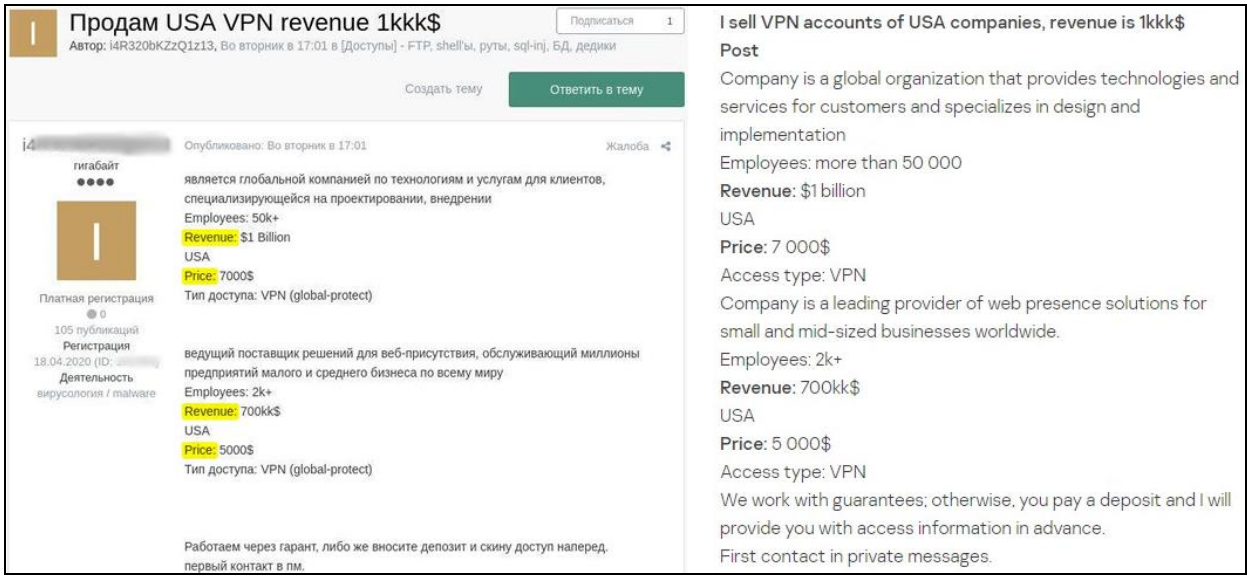

Image 8: VPN sale of corporate VPN credentials [90]

Indeed, there have been instances of the sale of access credentials to SCADA systems, which are part of critical infrastructures. Additionally, the sale of personal data belonging to military personnel has resulted in the indirect compromise of military operations [91].

Ideological motivations

In addition to the legitimate use of cyberspace for information dissemination and expression of ideas, the internet has also become a battleground where the most radical ideologues employ cyber violence, such as hacktivism, to impose their extremist agenda. These individuals or groups utilize cyber-attacks to promote their preferred ideology without intending significant damage to systems or the public. However, some attacks are more extreme and aim to create fear, degrade essential services, or even cause human losses, as in the case of cyberterrorism [92]. The issue of terrorist attacks targeting critical infrastructures through digital means has been a long-standing concern. Such attacks are often carried out using unconventional methods, as they are anonymous, conducted remotely, and cost less than traditional forms of terrorism. Furthermore, they have a significant impact on a large number of targets and the general population, which is further amplified by the extensive media coverage they receive [74]. There is a belief that the level of online presence is one of the key factors in target selection [93], which

puts critical infrastructures at a higher risk due to the nature of their operations that require them to provide easily accessible information and services to the public.

This particular dimension is a unique case as it lacks the element of anonymity, as the attackers intentionally take responsibility for the attack in order to use publicity as a weapon to achieve their goals. This makes them particularly dangerous as they do not have to conceal their actions, and their attacks can be more straightforward [93]. The United States anticipates that this type of terrorist activity will increase in the near future due to the enhanced capabilities of the new terrorist groups' cadres [94].

Cyber threats in the context of geostrategic and political dynamics

The utilization of malicious software to surveil and obstruct sensitive information for political, military, or economic objectives of hostile states and entities with competing interests (known as cyber espionage) has become an established reality. The interception of information from rival states for national purposes is more relevant than ever, and cyber has become the fifth domain of warfare, following land, sea, air, and space [95], and a significant priority for the EU's comprehensive strategy [96].

In contrast to other domains, the traditional doctrine of blame, retaliation, and deterrence is not readily applicable in cyberspace, as attackers are not easily identifiable in the same manner as in physical space. Additionally, the origin of an attack may be entirely different from the location from which it is launched, placing the responsibility for accountability with the local authorities under the law applicable there rather than the affected state, further complicating the situation [97]. Furthermore, what may be considered illegal under the laws of one state may have an entirely different legal treatment in another, exacerbating the complexity of the issue. Certain nations, including China, Russia, and Ukraine, lack extradition treaties with the United States, which poses a formidable challenge to prosecuting hackers who reside within their territories [2].

It is crucial to acknowledge that despite the fact that cyberattacks occur in the virtual realm, their repercussions are promptly perceived in the physical world, particularly if the attack involves the interference of an essential service. This domain has been employed with significant effectiveness in recent times, as exemplified by the military conflict [98] between Russia and Ukraine [99], which has featured a hybrid warfare strategy aimed at disrupting the critical infrastructures, supply chains, and intellectual property of the European Union and its constituent Member States [95]. An international guideline [100] has already been issued by a coalition of nations to enhance the readi-

ness and resilience of critical infrastructures [101]. Furthermore, the EU's mobilization was promptly followed by the Versailles Declaration [102], which emphasizes, among other matters, the strategic significance of cybersecurity and the imperative to safeguard critical infrastructures [103]. Smaller countries such as North Korea and Iran share a similar viewpoint, but from an opposing perspective, as they exploit the excessive reliance of rival nations on technology, aiming to disrupt their control and management procedures in the event of a conflict (contr & com) [97].

From a geopolitical perspective, various countries have engaged in extensive cyber espionage activities [35]. While the United States views cyber espionage as a justifiable measure for national security purposes, it opposes the exploitation of commercial information obtained through industrial espionage. This issue has been acknowledged at the highest levels of leadership, as exemplified by the Chinese president's agreement to terminate China's practice of industrial espionage following consultations in 2015, and President Obama's warning to Russia in 2016 not to attempt to hack into polling station information systems during the forthcoming US elections, thereby rendering cyber attacks a direct threat even to democracy itself [104]. Apart from targeting digital assets, attackers are also focusing on government and university officials, who are deemed to be easy targets for intelligence gathering due to geopolitical considerations [105].

At the political level, the Pegasus case is one of the most common examples of cyber threats, wherein the Israeli company NSO monitored thousands of individuals, including 14 world leaders [8]. Another notable example is the leak of nearly 20.000 emails from the Democratic National Committee, which aimed to disrupt the smooth functioning of the 2016 US presidential election and posed a direct threat to the democratic process [88].

4.4 A review of Malicious Threat Actors and Their Modus Operandi

Threats to critical infrastructures are distinguished between those caused by external factors (natural disasters, human error, etc.) and those caused by adversaries [106], [73]. In the former case, the threats occur without a specific intent, whereas in the latter case, threats are deliberately planned with malicious intent to bypass security systems, usually by exploiting a security vulnerability, with the aim of causing harm to the victims. It is not uncommon for instances of disruption of services caused by a natural disaster to

become a catalyst and an opportunity for an adversary to launch a cyber attack, amplifying its impact. In general, it is a combination of the target environment, vulnerabilities, and capabilities of the attacker [106].

Hostile threats possess certain characteristics that distinguish them, including factors such as "by whom," "why," "where," "for how long," and "how" they are implemented. These characteristics translate into key attributes of hostile threats, which encompass the identity of the attacker, their objectives, the level of impact they intend to cause, their capabilities, and the methods they are capable of and willing to employ to execute their attacks.

Research has revealed that specific characteristics have a direct correlation with the occurrence of an incident. These include the attacker's level of knowledge of the targeted systems, the amount of time they have at their disposal, and their persistence in carrying out the attack. The severity of the incident is also directly related to the attacker's motivation, their skills, and the time window they have to launch and sustain the attack.

These attacks are typically executed through various attack vectors, including digital, physical, social engineering, and supply chain [106]. Each attack vector can impact one or more of the following categories [8]:

- Damage to the victim's reputation through negative publicity.
- Destruction of information.
- Direct or indirect economic loss.
- Damage to national security.
- Physical damage and/or casualties.
- Social unrest in the wider society due to disruption of critical infrastructures.

Various classifications of threat actors have been proposed based on two key factors: a) the attacker's objectives, and b) the resources required to execute an attack, such as technological expertise, financial backing, and time. The United States Department of Defense has established six distinct levels of threat actors based on these criteria [70]. The first level consists of "script kiddies" who lack specialized technical knowledge and use off-the-shelf tools for malicious purposes. At the second level, attackers possess significant knowledge and are typically cybercriminals who seek financial gain. Moving forward to the subsequent two levels, the attackers' proficiency, organisation, and financial resources increase substantially, allowing them to discover new vulnerabilities that

have not been exploited in the past. At the fourth level, it is not uncommon to see some form of collaboration with government agencies to launch attacks. The following two levels involve states with the objective of creating new vulnerabilities to use them for large-scale targets, such as critical infrastructures. The last level pertains to modern warfare doctrine and includes a comprehensive attack on all theatres of war.

It is noteworthy that, as the levels advance, the monetary and technological investments of the actors increase exponentially, either by the attackers themselves or third parties, amounting to billions of dollars at the highest level. However, the methods and tools used in high-level attacks are often analogous to those used in lower levels for camouflage purposes, thereby diminishing the likelihood of detection [70].

Despite their origin, cyber attacks targeting critical infrastructures have increased in recent years, with both state and non-state actors being responsible [95]. An attack that illustrates this is the one that was allegedly launched by China in 2011, which targeted the security company RSA, but the primary objective of the attack appeared to be to undermine US defence by compromising critical weapons system manufacturers in the supply chain [107].

ENISA has a different perspective on defining threat actors and identifies the following distinct categories of threat actors in its 2022 report [8]:

- Cybercriminals: The category of cybercriminals, as a threat actor, aims to gain personal benefits such as financial or reputation gains through various types of attacks. These attacks can include piracy, identity theft, online fraud, the creation and dissemination of malware, and attacks on computer systems and websites. Unlike other threat actors who select targets based on specific criteria, cybercriminals often choose their targets randomly, such as those who respond to an email or unknowingly download malware from a website. In recent times, the use of ransomware attacks by cybercriminals has increased, combining it with supply chain attacks and targeting OT systems to maximize their impact [8]. The COVID-19 pandemic has provided a window of opportunity for these attacks, with cybercriminals utilizing cloud infrastructure for their activities. Furthermore, the pandemic has led to better organization of these actors, with the use of specialized tools such as phishing templates becoming more prevalent [79].

  In addition to direct attacks, cybercriminals possess knowledge about vulnerabilities that exist on the dark web, which they can purchase them even the govern-

ment agencies either to use this information for their own attacks or avoid falling into the hands of rival states [108]. The human factor is often exploited through social engineering, which is a weak point in security. Cybercriminals aim to target as many individuals as possible, using cost-effective methods such as phishing emails [97]. These actors are highly motivated by the discovery of new zero-day vulnerabilities, as they provide greater chances for financial gain, either through direct exploitation or by selling them to third parties in illegal markets on the dark web [8]. The case for this is because defenders have limited ability to mitigate the effects of an unknown vulnerability.

- Hackers-as-a-service: The particular threat actors refers to individuals or groups who possess advanced knowledge and skills in cybersecurity and provide cyber-attack services to customers, primarily to state-actors for espionage and surveillance operating as mercenaries [8], [105]. These actors often target critical infrastructures, coinciding with the interests of nation-states [97]. The 2017 FBI indictment against Russian hackers for illegally accessing Yahoo user emails revealed a typical example of this actor's attack, where they were recruited by a Russian state agency [109]. The Dark Web has witnessed an emerging market for off-the-shelf hacking tools, such as phishing templates and malware, which can be purchased for a fee, facilitating the transition from Level 1 to Level 2 [79], [2]. It is predicted that this actor will continue to evolve in the future [8], with the emergence of new threats such as ransomware as a service (RaaS) [110] and surveillance as a service [105]. The international recognition of the risk posed by cyber espionage has been acknowledged through the agreement of a bilateral treaty between the US and China in 2015, aimed at reducing such operations [111].
- Hactivists: This threat actor is about individuals or groups that conduct attacks driven by ideological motives. This trend has been on the rise in cyber-conflicts beyond the borders of Russia and Ukraine, as evidenced by the monthly updates of the European CERT that report a surge of attacks originating from this actor [35]. In contrast to previous years, hacktivists now target critical infrastructures as well [8], although the Cybersecurity and Infrastructure Security Agency (CISA) considers them a medium-sized threat that primarily focuses on propaganda to achieve their political and ideological objectives [112]. The conflict be-

tween Russia and Ukraine has contributed to an increase in cyber-conflicts, as reflected in the monthly updates from the European Computer Emergency Response Team (CERT), which has seen a surge in attacks launched by hacktivists. An example is the Ukrainian government's request for volunteers to establish a Ukrainian IT Army that caused damage to Russian infrastructure [113], which could potentially lead to the continuation of similar activities by these actors even after the end of the conflict.

- State actors: These are threat actors whose motives are driven by wider geo-strategic and political considerations. These groups are primarily state-sponsored and their objective is to launch targeted attacks on the systems and critical infrastructures of rival states in order to cause maximum damage [53], trend which is expected to increase in the future [8]. State actors are already taking steps to gather information on Industrial Control Systems (ICS) in order to prepare for future attacks, and they are willing to expend considerable time and resources to gather the necessary information to achieve their objectives [8]. These activities are undertaken stealthy to evade detection, thereby enabling the hackers to maintain control over the target systems without being noticed for extended periods forming the attacks most known as Advanced Persistent Threats (APT) which is of an exceptionally severe nature, particularly towards critical infrastructures [2], [114]. APTs are characterized by their persistence and the use of advanced techniques to evade detection and maintain access [115].

  The utilization of cyberspace as a weapon is of paramount importance, as acknowledged by an official report of the US Department of Defense, due to its potential impact comparable to that of the nuclear threat during the Cold War. This report recommends that the US implement robust cybersecurity measures including the development of a strong digital arsenal to counteract cyber attacks.

  Furthermore, it has been asserted that it is of utmost importance to prevent any adversary from obtaining supremacy in cyberspace. It is emphasized that relying solely on a defensive approach is insufficient, and it is therefore suggested that the adoption of an offensive posture is necessary to counter potential threats. However, it must be acknowledged that offensive capabilities carry their own risks, as they could potentially be used against their own side as well [70]. As evidenced by repositories of the European Computer Emergency Response

Team (CERT) and the Cybersecurity and Infrastructure Security Agency (CISA), there is an abundance of cyber attacks targeting even nuclear power plants [116] in the United States.

Owing to their well-organized nature and substantial resources, these actors possess the capability to produce and leverage newly discovered vulnerabilities (e.g. zero-day, supply chain attacks), rendering them particularly hazardous to critical infrastructures [8], [111].

- Internal threats: This kind of actors poses a significant danger to critical infrastructures, despite being mentioned only as a footnote in the particular ENISA's report. These threats stem from the misuse of information assets or the deliberate and intentional attack by an individual who has gained legitimate access to an organization's information systems or information, with the intention to harm the agency's mission, resources, personnel, facilities, information, equipment, networks, or systems. The motivations of insider threats may be compounded by other threat factors such as violence, espionage, sabotage, theft, and cyber-acts [117]. The presumption is that the attack is carried out by a person with access to the resources of the organization or an insider [118].

Table 4: Correlation between threat dimensions and main incentive-based threat factors.

	Threat areas	Cybercriminals			Cyber warfare	
			Cyber terrorism		Cyber espionage	
	ENISA Threat Actors	Insiders	Cybercriminals	Hactivists	Hacker-as-a-service	State actors
Motives	Ideology			□		
	Utilitarian pursuits	□	□			
	Geostrategic and political situation				□	□
		I, II	II, III, IV	IV	IV	IV, V, VI
		DSB Threat Actors				

Comprehending the threats, motivations, and objectives of attackers is essential in enhancing an organization's defensive capabilities, as it allows for the allocation of resources based on anticipated risks. The table presented earlier in this text provides a condensed summary of the preceding paragraphs and demonstrates the connection be-

tween threat factors, as defined by the US Department of Defense and ENISA, and the primary areas of threat. It also outlines the motivations that drive each factor.

Frequently, the nature of an attack can provide insight into the identity of its perpetrators. An attack aimed at breaching confidentiality may indicate the involvement of cybercriminals seeking financial gain through extortion or the illicit sale of intercepted data. Conversely, attacks that disrupt the availability or integrity of systems, and interfere with their normal operation are more likely to have geopolitical motivations [12].

The aforementioned ENISA report highlights that critical infrastructure operators remain a primary target for attackers, irrespective of the incentives driving the attacks.

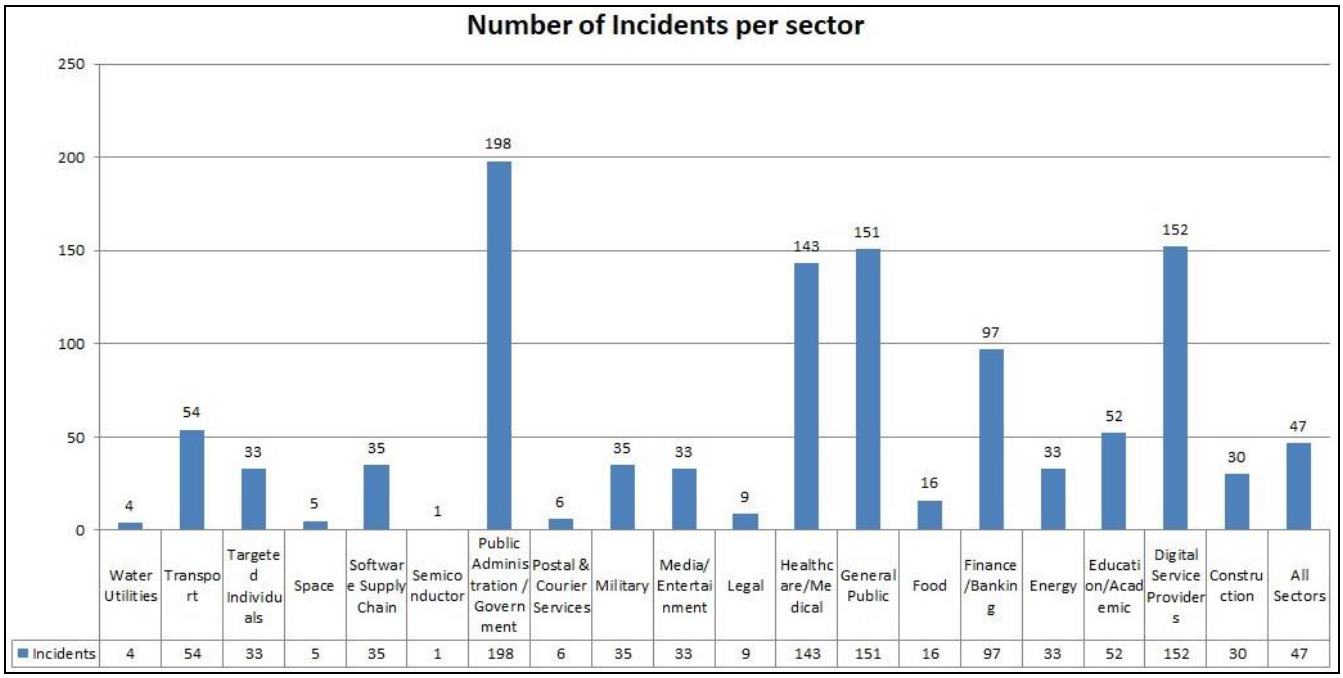

Image 9: Number of incidents per critical infrastructure sector [9]

In 2021, there was a notable increase in the frequency of cyber-attacks against critical infrastructure sectors, including Water (4), Energy (33), Transport (54), and Digital Service Providers (152), as well as a considerable number of military targets (35). These incidents underscore the significance of national-level cyber espionage [9]. Additionally, the health services sector witnessed a significant number of breaches (143) owing, in part, to the high value placed on personal and sensitive data in illegal markets, as well as the unique circumstances brought about by the pandemic [8].

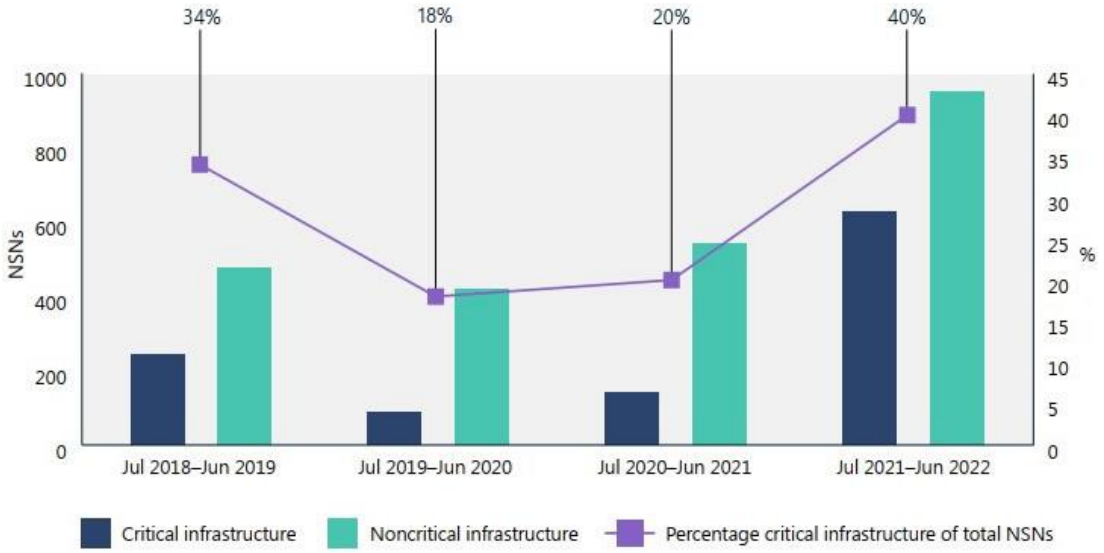

Image 10: Microsoft reports on targeting critical infrastructures [105]

According to Microsoft's Digital Defense report [105], the frequency of cyber attacks targeting critical infrastructures has tripled compared to three years ago.

PART 3: Vulnerabilities, Cyber Threats, and Mitigation Strategies

5 Analysis of Attack Surface in Critical Infrastructures

Identifying the most critical threats associated with critical infrastructures is a pivotal factor in strengthening its cybersecurity posture. This entails prioritizing and specifying necessary actions to counter the identified threats based on the available resources to the organization. However, the dynamic nature of the threat landscape presents a significant challenge, owing to the growing reliance on digital technology, ease of access to advanced tools and resources by attackers, lower technical and cognitive proficiency required to conducting attacks, and the crucial role of critical infrastructures in society. Moreover, the distinct requirements of each critical infrastructure sector further complicate the adoption of a uniform cybersecurity approach. Nonetheless, this does not negate the existence of a common ground in defining the cybersecurity strategy.

5.1 Exploring the Attack Surface

The initial step towards defining cyber threats involves an investigation into the potential methods by which infrastructure may be subjected to attack. It is evident that there is a considerable variation in the type and intricacy of threats over time. Current attack methodologies are not limited solely to vulnerabilities within hardware and software systems, but have progressed to the extent that they are capable of targeting and exploiting the human element, which has become the weakest link in any organization's security posture [119].

Recent attacks demonstrate that the severity of cyber threats has increased significantly, with attacks not only originating from individual hackers but also from coalitions of hacker groups using asymmetric tools such as botnets and tools-as-a-service (SaaS) to carry out their attacks [35]. This trend is further amplified by the support from state

power centers. Moreover, while earlier attacks were limited to basic malware such as trojans that could be mitigated using firewalls, advanced threats have fundamentally transformed the way organisations plan their defence strategies [120].

The increasing reliance of critical infrastructures on third-party application solutions expands the range of potential threats beyond their direct control and supervision [121]. Similarly, critical infrastructure systems are progressively becoming more intricate and advanced, not only in terms of technology, but also with regards to the interdependencies that exist between the different sectors. Moreover, the increasing geographic dispersion of local infrastructures further elevates the risks associated with the need to interconnect and communicate with one another [122]. The continuous operation of Critical Infrastructure Entities is heavily reliant on the availability of electricity, which can be facilitated through direct supply or standby power systems [123], thereby making it the backbone infrastructure [5].

Simultaneously, the rapid pace of technological advancements in the IT sector creates a fundamental challenge in maintaining consistency in technology management and presents novel vulnerabilities [124]. Furthermore, the growing adoption of ICT technologies amplifies this issue [122].

The necessity to handle data from both internal primary sources and external sources, the automated management of critical infrastructure's mechanical equipment, and the interconnection of various ecosystems within the organization require the use of multiple systems and different technologies. This situation is further exacerbated by changes in the business model, the requirement to extend interaction between the internal infrastructure of the organization and the external environment, and the somewhat mandatory exposure of the infrastructure to the external environment, all of which contribute to the precariousness of the situation [7].

Taken together, the aforementioned elements encompass the essential resources needed to cover all critical systems, irrespective of their visibility to external entities, inclusion of internal users or customer interaction points, thereby representing an expanding attack surface. In terms of security considerations, the unifying factor among these components is the attack vectors [125] - the methods and techniques (e.g. email, USB, social engineering, network misconfiguration) utilized by attackers to exploit vulnerabilities, with the ultimate aim of compromising critical infrastructure systems. As is evident, the presence of multiple threat vectors leads to an increase in infrastructure risks, thereby

rendering protection against attacks more challenging. This phenomenon is corroborated by recent surveys indicating that the attack surface has expanded in over 67% of organizations in the past two years. The upswing in the attack surface can be attributed to the adoption of hybrid work models and new technology solutions in the cloud, which leave organizations more susceptible to internet-based threats [126].

In its entirety, the cyberspace can be described as a composite landscape consisting of three interrelated layers [127]:

- The physical layer comprises devices and IT infrastructure, including hardware and infrastructure, which are responsible for storing, transporting, and processing information. To safeguard these elements from physical damage or unauthorized access that could lead to logical access, physical security measures are necessary.
- The logical layer comprises abstractly interconnected elements that communicate with each other through a network using programmatic logic. These elements are susceptible to attacks only through cyberspace.
- The social layer, also known as the cyber-persona layer, is where digital representations of entities are created. It consists of user accounts and the relationships between them.

Considering the aforementioned, a widely accepted method for defining the attack surface is to categorize it into three classifications: [128], [129], [130], [131], [132]:

- The physical attack surface encompasses all computing devices that an attacker can physically access, such as servers, personal computers, laptops, mobile devices, USB drives, IoT sensors, and operational technology (OT) hardware. Additionally, it includes computers that are to be decommissioned but still contain access credentials, as well as paper documents containing confidential information.
- The digital attack surface encompasses all hardware and software connected to an organization's network, regardless of whether it is on-premises or in the cloud. This includes applications, websites, servers, and other similar components.

- Social engineering attack surface includes those attacks that aim to manipulate and deceive users into divulging confidential information or granting access to unauthorized individuals, either through direct or indirect means.

As illustrated in the image presented below, there is a notable discrepancy between the intended visible technological footprint of an organization and its actual exposure to the external environment, resulting in a significant increase in vulnerabilities.

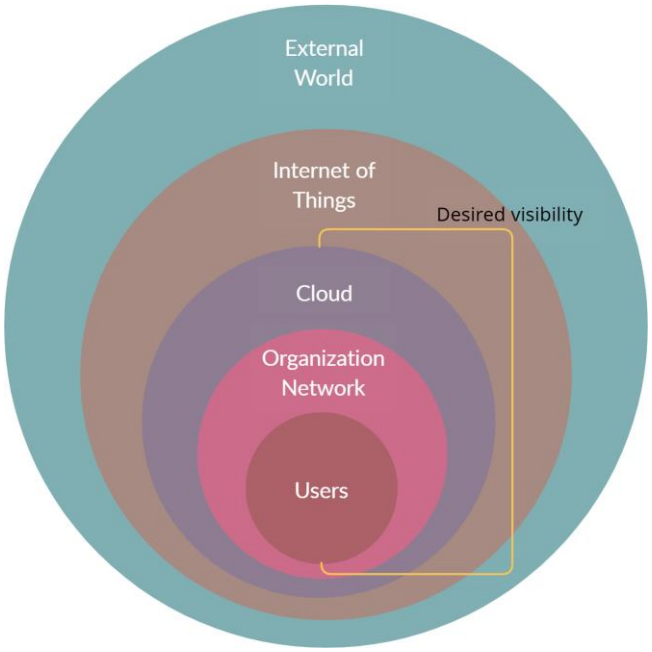

Image 11: Contemporary attack surface in critical infrastructures [43]

The exploitation of the opportunities presented by the aforementioned channels gives rise to cybersecurity threats. Therefore, it is crucial to identify and comprehend these threats to formulate effective cybersecurity strategies and minimize overall risks.

5.2 Discerning the Dimensions of Cyber Threats

The literature extensively covers the investigation of cyber threats, as the cybersecurity of critical infrastructures can be approached from various dimensions due to its multi-factorial nature. Understanding and visualizing all the elements and their interdependencies that constitute the entire system is the first and fundamental step towards achieving cybersecurity. To this end, the following categorization [133] is adopted as a reference point:

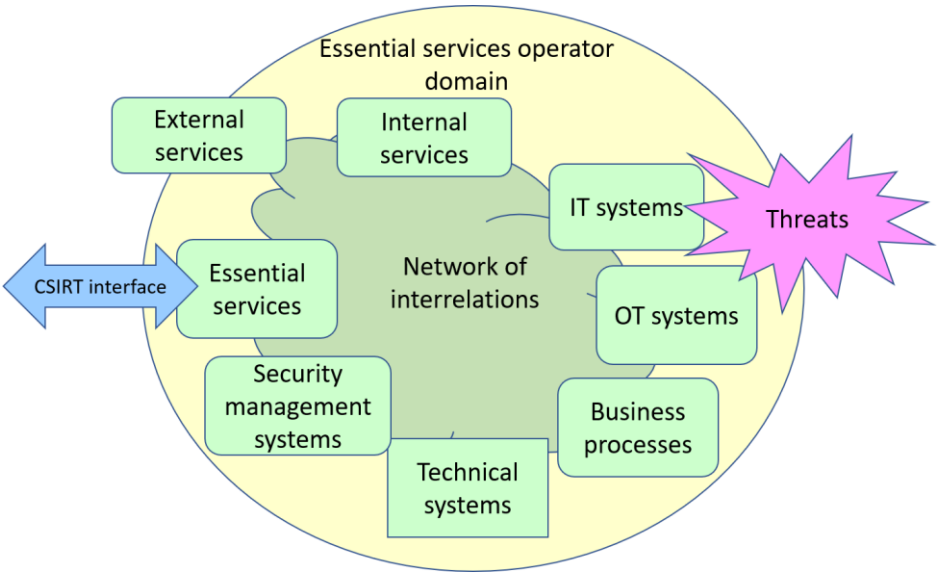

Image 12: The cyberspace of critical infrastructures [133]

Based on the aforementioned distinction, the cyberspace of critical infrastructures is comprised of a complex interwoven fabric of activities, processes, and services, which includes the following elements:

- The essential services provided by the critical infrastructure operator, such as electricity or water.
- External services offered to the operator by other critical infrastructure entities.
- The internal services furnished by the operator to support its operations, such as local transportation.
- The operational processes executed by the operator to achieve business objectives, such as customer service.
- All technological systems, including IT and OT systems, employed across the spectrum of the operator's activities.
- Security systems supporting the critical infrastructures.
- The entire network of internal components and their interconnections.
- Interfacing external systems for incident reporting and management.

The classification of attack categories presented in the study [134] was deemed highly valuable, despite its focus on attacks within the IoT environment:

Table 5: Classification of attack categories.

Categorisation	Description
Attack Severity	Depended on severity of the attack or the threat level
Access Type	Depended on type of access used by the attack (Physical, Cyber)
Attack Type	Overall type of attack (e.g. DoS, MitM, Ransomware)
Attacker Position	Depended on the attackers position relative to the victim (Insiders, Outsiders)
Attacker Implication	Depeded on the level interaction between attacker and victim (Active, Passive)
Objective Oriented	Depeded on the overall goal of the specific attack
Network Layer Oriented	Depeded on the OSI layer where the attack resides (e.g. jamming for physical layer, DoS UDP flood on the transport layer, SQL Injection on the application layer)
Use-Case Specific	Depended on the specific use case (CPS, Wireless Ad-Hoc Networks, IoT, SDN)

As can be seen from the analysis above, it is evident that cybersecurity can be approached from various perspectives, such as those concerning threat actors, the effects of disruptions on the CIA triad [135], the methods of attack, the type of attack surface, and the attack vectors utilized, among others.

In order to formulate effective countermeasures, it is essential to consider the full spectrum of potential attack and threat vectors, regardless of their origin [118]. For this reason, a thorough investigation has been conducted on the methodologies utilized by other scholars in tackling this problem.

A previous survey conducted in the cybersecurity space in 2015 [136], which covered more than 15 million attacks on government agencies and key service providers, predicted increasing trends in cyber espionage, cyber warfare, and attacks on IoT devices. The survey revealed that cybersecurity incidents were partially attributed to the capabilities of attackers and the rest to human error and system vulnerabilities, with criminal activity accounting for less than half of the actual cause of incidents. Malware, malicious insiders, social engineering, stolen devices, and web-based attacks were found to be the most common modes of attack.

Similarly, in the research discussed in [123], it is noted that the means of attack may potentially target various aspects of the critical information infrastructure (CII), including its environment, hardware, software, and services, as well as the personnel responsible for operating and maintaining it, and the end-users who rely on its functions. The

means of attack may involve the exploitation of software, network or protocol vulnerabilities (e.g. malware, zero-day vulnerabilities), the use of botnets for DDoS attacks, electromagnetic interference, the use of special tools to breach the confidentiality of systems, the exploitation of users themselves, or even the prior installation and exploitation of hardware or software to gain unauthorized access.

The survey conducted by reference [82] scrutinized a dataset provided by Hackmagedon, which encompassed the critical infrastructures, containing timelines and statistics regarding cyber-attacks transpired within European nations during the period of 2017 to 2019. The principal threats have emerged to include malware attacks, targeted attacks, account hijacking, malicious code injection, distributed denial-of-service (DDoS) attacks, phishing attacks, and man-in-the-middle (MITM) attacks. The reason for attributing significant threat to malware attacks was the surge in the prevalence of ransomware attacks.

After a comprehensive analysis of 78 studies that included critical infrastructures such as smart grids, ICS, CPS, and others as targets, [21] identified the significant security vulnerabilities and their frequencies of occurrence. The top three key vulnerabilities identified were Denial-of-Service (DoS) attacks, malware attacks, and web-based phishing vulnerabilities (SQL injection, XSS attack).

The study [137] states that there is no universal solution for cybersecurity and emphasizes the issues arising from the unavoidable interaction of various technology ecosystems, including IT, OT, and IoT, as well as the digitalization of systems in conjuction with the sluggish progression of cybersecurity measures at all these levels.

According to [124], the primary cyber threats are categorized as follows: a) external threats, b) internal threats, c) supply chain threats, and d) threats arising from inadequate operational capabilities. The most prevalent attack methods include a) Denial-of-Service (DoS), b) Man-in-the-Middle (MitM), c) Malware, and d) Phishing.

In the wider social context, FBI statistics covering cyber offenses from 2015 to 2020 have led to the conclusion that the top five cyber crimes in 2021 were extortion, identity theft, personal data breach, non-payment, and phishing attacks [22].

According to [138], cyber threats can be classified into four abstract categories: internal, external, integration-based, and interconnectivity.

At a different level, [139] highlights the risks associated with the new work culture of remote work.

Finally, according to the ENISA 2022 report [8], there has been a notable increase in the use and impact of specific cyber threats in recent years, which distinguish them from others. Although the threats identified in this study are not solely directed towards critical infrastructures, they do represent a comprehensive set of the major threats to society as a whole. These threats include: a) Ransomware, b) Malware, c) Social engineering, d) Threats to data, e) Threats to availability: DoS, f) Threats to availability: Internet Threats, g) Misinformation, and h) Supply chain attacks.

Considering all the information presented above, and relying heavily on the classifications discussed in [133] and [134], this research endeavors to abstractly categorize the dimensions of cybersecurity of critical infrastructures and explore cyber threats by examining each aspect, as illustrated below:

- Categorized by critical infrastructure sector (e.g. electricity, water supply, health facilities). This categorization allows for a more targeted and specific approach to cybersecurity measures, as different types of infrastructure may have different vulnerabilities and risks.
- Categorized by attack surface dimensions (e.g. IT, OT, Cloud). This classification highlights the importance of understanding the different technological layers and their vulnerabilities, as well as the interconnections between them.
- Categorized by attack types (e.g. social engineering, human factor, supply chain, ransomware). This classification provides insight into the different strategies and techniques used by threat actors, which can help in developing appropriate defense mechanisms.
- Categorized by attack domains (e.g. network, applications, etc.). This classification provides a more detailed understanding of the specific areas that are vulnerable to cyber threats and can guide the development of targeted defense strategies. It should be noted that the vast size of this category necessitated an ad hoc investigation of the corresponding vulnerabilities, which only served to complement the findings of the other categories.

The aforementioned categorization is not definitive, but it is an initial step towards systematically researching this vast topic. Defining the subject's boundaries has been challenging, and a similar challenge has been encountered in approaching the threats and developing corresponding countermeasures to mitigate the issues. This is due to the fact

that threats are diverse and continuously evolving as the aforementioned factors remain in a state of flux.

6 Cyber Threats in the Context of Critical Infrastructure Sectors

Due to the fact that optimal outcomes are achieved when the attacker causes significant disruption to the victim over an extended duration, adversaries consider all sectors of critical infrastructures to be ideal targets. Consequently, a successful attack to such an operator would affect a considerable number of individuals as such an attack could create a lot of damage or require complicated and costly repairs [140].

While there are notable variations between critical infrastructure sectors, there exist important similarities in the crucial components that are essential for their efficient operation. These elements demonstrate a degree of repetition and overlap in their usage across diverse sectors. More specifically, they encompass personnel with varying areas of expertise, knowledge, and specializations; technological elements such as hardware and software for monitoring and controlling critical systems, which play a crucial role in maintaining the integrity and security of the infrastructure; sector-specific infrastructure designed to meet unique needs; and defined procedures and protocols that ensure system safety and reliability, such as emergency response plans, maintenance schedules, and quality control processes. By recognizing these commonalities, it is possible to design more efficient strategies for managing and safeguarding critical infrastructures across multiple sectors and mitigating the impact of cyber-attacks.

Particular challenges arise from several factors such as the risk stemming from infrastructure interdependencies, the increasing dependence of Industrial Control Systems (ICS) on internet-based technologies that may compromise air-gapped infrastructures and the proliferation of technologies that increase the number of attack vectors. Furthermore, the task of integrating security measures into aging infrastructures exacerbates the complexity of implementing a proactive defense. At the organizational level, managing security-oriented assets can be particularly challenging due to the abundance of assets and the lack of accurate information about them, including asset inventory

[19], while human factor is now regarded as a significant risk source with the potential to create a substantial vulnerability [8].

The subsequent sub-chapters provide a concise and illustrative analysis of the energy, water, and healthcare sectors and present the potential hazards stemming from the inter-dependencies of critical infrastructures.

6.1 Energy sector

Our modernity is rooted in a great part in the foundations of energy system. At the same time, digital technologies are assuming an increasingly prominent role in the automation of conventional energy technologies, as well as serving as a central feature in the realm of energy transition. The importance of computer control has become paramount, and is set to become even more significant in a world where distributed energy systems prevail. It is widely accepted that the increasing interdependence of OT and IT has created new challenges for commercial entities operating in the energy sector [19], as well as for other critical infrastructures.

The architecture of energy systems involves numerous interconnected ICS devices, whereby attacks may potentially target any of these, including SCADA, PLCs, control and monitoring devices [141]. The criticality of these components has as extension that a single point of failure could render the entire network unavailable [120]. Furthermore, it is important to consider not only the number of heterogeneous devices, but also their geographical distribution. These hardware, computational and communication devices are installed in various locations such as power plants, substations, energy control centers, company headquarters, regional operating offices, and significant load sites. Additionally, a diverse range of communication systems is deployed on the power grid to facilitate monitoring and control across numerous communication channels. These factors collectively contribute to the vulnerabilities of power systems, which are primarily comprised of three main components: computer systems, communication systems, and power systems [142].

A generalized classification of the methods of malicious attacks on power infrastructure can be as follows [141]:

- Attacks on the power system target the electricity infrastructure, causing outages that have negative effects on customers.

- Attacks by the power system use parts of the electricity infrastructure as a weapon to cause damage to the population.
- Attacks through the power system target the civil infrastructure, using the means provided by the power system to cause damage to other infrastructures such as computers.

The complicated nature of these infrastructures is considered also as a vulnerability as they cannot be easily upgraded similar to other information assets. Moreover, the security improvement of specialized hardware is usually neglected. This trend is exacerbated by the fact that operators of these devices frequently lack the technical expertise required to implement any security patches. This factor could be a contributing reason for the existence of firmware vulnerabilities in various types of equipment within the energy sector, which in turn makes it a prime target for cyber attacks [120].

A typical example of the complexity of such an attack at energy operator took place in December 2015, at Prykarpattya Oblenergo, in which an Ukrainian power distribution operator, suffered a well-coordinated cyber attack that caused interruptions to the operation of several power substations and left about 80,000 customers without power for several hours. The attack was composed of three elements: a malware attack, a denial of service attack on the call center infrastructure, and the opening of substation breakers. The attackers infected the main servers controlling the electricity distribution process with malware and issued a command to open breakers of various substations. The malware was spread through spear-phishing campaigns targeting IT staff and system administrators working for companies responsible for electricity distribution in Ukraine. After the power outage, denial of service attacks were launched to prevent service personnel from receiving error messages, which delayed the recovery of infrastructure operations [143], [137].

As observed, the aforementioned case represents a combination of various attack types from several dimensions studied in this research. Social engineering through spear phishing exploited the human factor weakness, while malicious malware resulted in vulnerabilities in the IT attack surface causing damage at the OT level. Furthermore, the inability to inform the public was compounded by the DoS attack, aggravating the social impact of this situation.

The study referenced as [3], which takes the previous attacks on Ukraine as a starting point to demonstrate the vulnerabilities of centralized power grids, highlights the view

that a decentralized system, incorporating greater on-site generation and microgrids capable of operating independently, could potentially enhance resilience against the impacts of a large-scale cyber-attack.

At [144] is proposed a cybersecurity strategy involving multiple defence strategies among many layers. The first layer is the physical layer which includes all hardware devices such as panels and areas where the CI is used. The second layer is the network security layer, which includes firewalls, packet tracers, IDS, IPS, and backup and redundant equipment. The third layer is the hardening layer, which involves firewall, patch management, virus protection, and detection. The fourth layer is the application layer, which provides additional security to the ICS core systems. The final layer of security for ICS involves change control, physical and logical access control.

Investing in staff training and competence, standardizing and harmonizing regulations, and increasing technical and organizational measures are necessary steps to improve cybersecurity. These measures may include upgrading the resilience of both IT and OT, promoting horizontal information sharing between agencies, and investing in research by both the state and the agencies themselves [19].

In its EU Security Union Strategy, the Commission emphasizes the importance of sector-specific initiatives to address the unique risks encountered by energy sector as it mention that "*due to the particular sensitivities and impact of the energy system, a dedicated initiative will support a stronger resilience of critical energy infrastructure against physical, cyber and hybrid threats, ensuring a level playing field for energy operators across border*" [145].

In this context, the Greek Government under the Gazette 4657/2022 [57] approved the "Risk Preparedness Plan for the Electricity Sector of Greece". This plan acknowledges cyber attacks as a significant threat and outlines two different scenarios for their consideration. The plan focuses extensively on cybersecurity and the proposed procedure aims to achieve timely detection, notification, and effective response to any cyber-attacks that could potentially compromise the security of the country's electricity supply. It involves the participation of relevant stakeholders, such as the National Cyber Security Authority, GR-CSIRT, and Personal Data Protection Authority. To achieve this goal, the procedure recommends implementing an integrated cybersecurity framework, conducting continuous monitoring and analysis of incidents, and collaborating with a security operations center. Furthermore, the procedure aims to enhance the role of cybersecurity by

appointing a CISO and a cybersecurity team and conducting cybersecurity maturity measurement exercises.

6.2 Water and Wastewater Sector

Over the last years, there has been a noticeable increase in the occurrence and complexity of severe cybersecurity incidents that have been linked to water infrastructure systems [146]. According to CISA, attacks [147] such as spear phishing, ransomware, and exploitation of outdated software are now widely used by threat actors to compromise IT and OT networks, systems, and devices. It is not a mere coincidence that the United States Department of Homeland Security (DHS) has identified the water and wastewater infrastructure system (WWIS) as one of the primary targets of cyber-attacks among the 16 infrastructure sectors [140].

Contemporary water systems consist of several subsystems and components of varying complexity. At strategic locations in the system, SCADA systems continuously monitor the infrastructure and water quality automatically transimitting the obtained data over computer networks. All these technological components introduce new risks to the particular sector [148] changing the previous situation in which the security could be enforced through their isolation and access restriction as IoT, SCADA, PLCs are prone to cyber-physical attacks [140]. The water sector must achieve a balance between the numerous benefits of its current digital evolution and the inherent risks associated with it. This can be accomplished by incorporating innovative cyber-physical concepts and tools into its strategic and tactical planning procedures [149].

Apart from the direct technological vulnerabilities, another conceivable attack scenario within this specific industry involves supply chain attacks, whereby perpetrators can attain persistent access to the infrastructure by providing fraudulent hardware components. Furthermore, the scenario involving malicious insiders in water sector has already been materialized when in the year 2000, a disgruntled ex-employee of a contractor that supplied control system technology hacked into the Maroochy Shire, Queensland waste management system. The individual had good knowledge of the SCADA system and the capability of wireless access, thus as a result, was able to repeatedly cause millions of liters of raw sewage to spill out into local parks and rivers [148].

The water industry currently lacks a shared understanding of the potential risks posed by cyber threats. The reason behind this is the absence of a systematic exchange of in-

formation on previous cyberattacks experienced by water utilities and their associated IT service providers. Such information sharing could aid in the assessment of the current state of cybersecurity in the water sector, thereby enhancing preparedness and the ability to safeguard the service [150].

Additionally, it was argued that the water sector may not require additional support and may not need to be included in the list of sectors in need of it. That misconception was based on the slower integration of Information and Communications Technology (ICT) in water facilities. This stance seemed to be supported by the industry, which until recently, had not recognized the necessity for sector-specific guidelines and standards to protect water entities from cyber threats. However, with the increasing digitalization of water services, this perspective is beginning to shift [145]. This perspective appears to be endorsed by the findings of [146], which suggest that the water industry and relevant policy-making bodies have prioritized cybersecurity through the implementation of awareness programs, training initiatives, and tools.

The review [140] emphasizes the criticality of managing security vulnerabilities and threats in SCADA water control systems. This entails upgrading the current water security architecture to address emerging risks. Furthermore, the review identifies a dearth of human resource development initiatives that focus specifically on security awareness and training for SCADA employees. Effectively addressing this gap is crucial to mitigate cyber threats [140], and is in accordance with [148], which emphasizes the promotion of cybersecurity awareness and training to personnel responsible for performing IT and OT security functions.

The water sector may necessitate the adoption of more stringent standards with respect to operational procedures and cybersecurity. The European Commission has also emphasized the significance of standardization in promoting interoperability of emerging technologies and to achieve this objective, the Commission has implemented its EU Rolling Plan for ICT Standardization since 2019. It highlights the requirement for the development of a standardized system that promotes the formation of a digital single market for water services [145].

A very interesting project about cybersecurity at water sector was the European Union-sponsored STOP-IT. This initiative was designed to promote knowledge, training, proficiency, and readiness regarding the subject of safeguarding water critical infrastructures from cyber-physical threats. One of its achievements was the development of a

distinctive software tool (RAET) that facilitates a methodical and comprehensive risk management process to aid water utilities in making strategic and tactical decisions against cyber-physical threats. By generating hypothetical attack scenarios and testing system performance, the RAET tool enables users to explore opportunities for enhancing preparedness by identifying preventive and mitigation measures. Additionally, users can evaluate the time available to respond in the event of an attack before the system's performance is significantly impaired [150]. More specifically, end-users have the ability to utilize a Fault Tree analysis, which assists in the visualization of the interactions, paths of failure, and domino effects between the cyber and physical domains within the complete urban water cycle [149].

CISA also provides recommendations [147] to address cybersecurity threats in the water and wastewater sector. These measures encompass preventive, detective, and responsive actions and entail technical and organizational controls implemented at four levels. The first level involves continuous monitoring of water and wastewater systems at the OT level. The second level includes remote access mitigation through the use of multi-factor authentication (MFA) and blocklists, conducting regular audits, and proper asset parametrization. The third level focuses on network mitigations, such as implementing network segmentation and DMZs for both IT and OT networks, using firewalls, and reducing the attack surface by removing unnecessary equipment. Finally, the fourth level encompasses planning and operational measures, such as creating an emergency response plan, a business continuity plan, and providing security training.

6.3 Healthcare Sector

The inclusion of the healthcare sector by NIS and CISA is indicative of the universally acknowledged of its critical nature. Some experts have claimed that healthcare data and infrastructure are as susceptible to cyber threats as, if not more than, financial and military data highlighting the need of safeguarding the healthcare sector due to its critical role in preserving human life [151]. Apart from that, the protection of personal and sensitive data belonging to individuals must also be taken into account. Any breach of such data poses a risk to the fundamental rights and freedoms of the affected individuals, and may result in regulatory penalties for the organization responsible [56] which is further aggravated by the increasingly utilization of digital technologies which create an ideal environment for potential data breaches [151]. The utilization of digital technologies in

the field of healthcare heavily relies on the use of ICTs for exchanging information and data related to health and its determinants [152]. In addition to specialized devices are required to provide the health services offered by health and care structures, information systems for storing personal and sensitive health data of patients are also required [143].

Given that healthcare systems are based on IT infrastructure, they inherently inherit the challenges associated with the confidentiality, integrity, and availability (CIA) triad. In case of an incident of misauthentication or identity theft, the confidentiality of sensitive information such as patient medical records may be compromised. Additionally, the use of malware, such as ransomware, can undermine the integrity and availability of services, leading to disruptive attacks and the complete interruption of healthcare services.

Healthcare settings are also considered cyber-physical environments because their IT systems are connected to specialized devices and automation that directly monitor physical individuals in real-time, meaning that any disruption to this physical equipment can have serious consequences. Furthermore, since healthcare personnel are dealing with medical equipment, where even the slightest mistake can jeopardize patients' lives, any cybersecurity threat in this area is extremely important [153].

The devastating effects of cyber attacks on healthcare were highlighted by the infamous WannaCry ransomware attack on the National Health Service (NHS), as detailed in reference [154]. The attack had a profound impact on numerous hospitals, including critical healthcare delivery systems like MRI scanners, resulting in the cancellation of thousands of appointments and financial losses totaling up to £35 million.

Healthcare organizations encounter a variety of cyber threats that can be broadly classified, as underscored in citation [155]. According to this study they can be categorized into three groups:

- Attacks aimed at disrupting service by targeting an organization's IT infrastructure (e.g. misconfigurations, DoS, SQL injection, eavesdropping).
- Attacks carried out for the purpose of personal financial gain (ransomware).
- Social engineering.

One plausible reason for the increase in cyberattacks and threats appears to be linked to insufficient monitoring of the maintenance and operation of medical devices throughout their entire life cycle. Moreover, the lack of designated positions within organizations, such as Chief Information Officer and Chief Security Information Officer, exacerbates

the situation. Human factor plays also a significant role in the cybersecurity of the healthcare sector, and it is crucial to implement awareness and training programs for healthcare professionals. This is consistent with the existing literature on organizational strategies that categorize them into technical solutions implemented to improve cyber resilience and human factor approaches utilized to promote cyber defense.

Study [156] highlights the importance of focusing equally on data privacy and security as part of a comprehensive cybersecurity strategy. Additionally, it recommends improving internal stakeholders' awareness and alignment with cybersecurity measures, as well as reducing endpoint complexity.

Healthcare organizations must prioritize the enforcement of their cybersecurity posture and resilience. ISO 27799:2016 [157] provides guidance for the establishment of information security management practices and standards within an organization. This includes recommendations for the selection, implementation, and management of controls, while taking into account the organization's risk environment regarding information security. These measures include regular backups, implementing firewalls, antivirus and malware protection, network segmentation, disabling unused physical ports, whitelisting permitted applications, adopting the least privilege principle, performing regular updates and patches, encrypting data at rest and in transit, implementing audit trails and logging, network monitoring and intrusion detection, secure system configurations, and protecting mobile devices for BYOD services.

6.4 The Risk of Interdependencies for Critical Infrastructures

In modern times, infrastructures have become crucially reliant on one another to provide vital services. Assessing potential disruptions in heterogeneous cyber-infrastructures is imperative to identify cascading disruption vectors and determine suitable interventions to mitigate the damaging impact [158]. This implies that any issue can spread between sectors and operators, potentially amplifying the impact [7], [159], [118], which could be perceived as a threat in its own right. Critical infrastructures should not be considered as self-contained single entities and their design should be approached strategically to encompass the entire chain of other infrastructures with which they are connected [14], [160].

Technical and security issues are related all aspects of the interdependencies and the infrastructure environment [5].

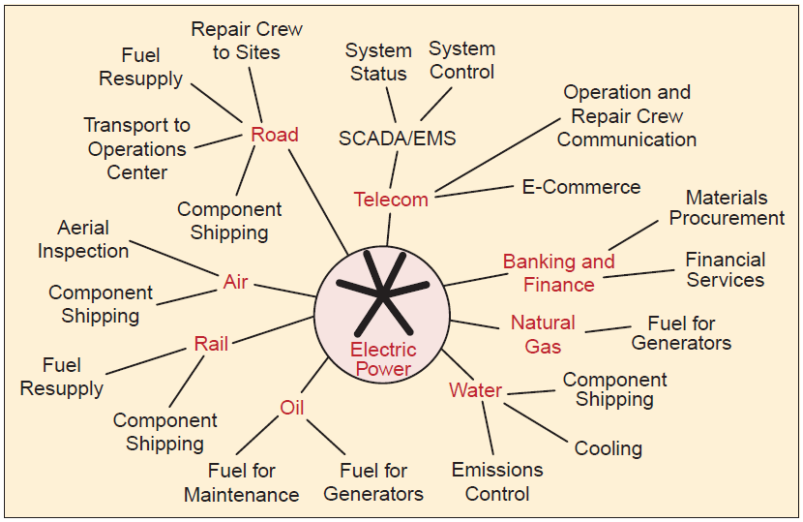

Image 13: Interdependence of critical infrastructures [7], [5]

The concept of interdependencies in critical infrastructures is differentiated based on various factors such as infrastructure characteristics, environment, type of failure, operational condition, and situations that lead to interdependency, as stated in [122]. Additionally, the interdependence of impacts on other infrastructures also affects the characterization of infrastructure criticality, as explained in [7]. As an illustration, it is worth noting that the proper operation of the electricity grid is crucial for many other critical infrastructure sectors. Without electricity, water and sewerage systems cannot provide water, the gas flow is disrupted, and telecommunication systems cannot function until back-up energy sources are implemented [126].

In 2001, an instance of chain reactions occurred in California, USA, where a widespread power outage caused successive disruptions of other essential services [14]. Another similar incident is the Rome outage in 2004, where the failure of SCADA systems in power infrastructure resulted in the unavailability of other critical infrastructures such as telecommunications and transport [158].

The aforementioned examples illustrate how the exploitation of vulnerabilities in one infrastructure can have an indirect impact on the activities of another, thereby expanding the overall attack surface.

Identifying and comprehending the interdependencies among different infrastructures is a necessary step towards assessing vulnerabilities and defining the appropriate measures to enhance safety and resilience [126]. In scenarios where the level of dependence is

significant and a particular component exhibits abnormal behavior, the possibility exists for the entire system and its services to be impacted, with the potential for the effects to spread to other critical infrastructures in a cascading fashion. Under such circumstances, it becomes crucial to consider four factors: the extent of the impact, its magnitude, the rate at which it spreads, and the methods of recovery [160].

It is necessary to conduct an analysis and categorization of each infrastructure based on the interdependency categories presented in the table below.

Table 6: Categories of interdependence between critical infrastructures [122], [7], [5].

Interdependence Category	Description
Physical	The condition of an infrastructure is dependent on the physical derivatives of another infrastructure.
Cyber	The condition of an infrastructure is contingent on the information conveyed by another infrastructure.
Geographic	The condition of an infrastructure is reliant on an environmental event occurring in a nearby infrastructure.
Logical	The state of an infrastructure is determined by the status of another infrastructure through control mechanisms, regulatory obligations, etc., that are not physical, informational, or geographical in nature.
Social	The state of an infrastructure is impacted by the outcomes of human behavior and activities that affect another infrastructure.

It is evident that cyber threats possess a universal scope and have the potential to target critical infrastructures at both vertical and horizontal levels. Assessing the risks associated with this issue is a challenging task and has been the subject of numerous studies.

Paper [158] presents a risk management framework aimed at mitigating threats and risks throughout the operational life cycle. The framework involves a quantitative assessment of safety and security risks in interconnected architectures, utilizing attack-fault trees to determine the probability and magnitude of the impact caused by service disruptions on complex infrastructures and their dependencies. Thus, the implementation of a multi-layered approach to security reinforces the concept of defense in depth, thereby enabling the selection of suitable response strategies and counter-measures in accordance with the prevailing circumstances.

Using a systematic approach and individual steps, [7] models the criticality calculation for interconnected infrastructures at the infrastructure, sector, and national levels. It also

identifies how potential threats and impacts can propagate to other multi-sector infrastructures and involves the assessment of risks associated with them.

In [14], a comprehensive model is proposed that identifies potentially hazardous chains of interdependent critical infrastructures and predicts the development of failures that endanger the system's stability. Simultaneously, the model prioritizes the importance of interdependent critical infrastructures to enable the appropriate targeting of protective measures to minimize the risk to the entire system.

In [161] is provided a definition and illustration of the cyber complexity of the essential services operator cyber environment, which includes interdependent services, business processes, systems, and IT infrastructure elements.

The outcome of the study at [133] is the proposal of a model that precisely depicts the intricate nature of the cyberspace utilized by essential services operators, and the identification of its components. This model utilizes predictions to estimate the likelihood and type of threat proliferation across interconnected services, business processes, software, and hardware infrastructure. Additionally, the model assesses the impact of these threats on the achievement of core strategic objectives.

Therefore, it is imperative to continuously assess and address the risks associated with cyber threats to critical infrastructures to ensure their resilience and reliability both at a national and operator level.

7 Cyber Threats Based on Attack Surface Type

This chapter provides an analysis of cyber threats within the context of the threat surface dimension of the entire technology ecosystem. This approach is considered essential in identifying the most significant and critical elements to be considered when developing a cybersecurity strategy and implementing necessary mitigation measures. The selection of the threat surface was based on the critical infrastructure elements and the trends and advancements in the overall environment. The overall threat environment was categorized into four specific areas:

- Information and Communication Technology (ICT): The elements to process, store, retrieve, and transmit data and information.
- Operational Technology (OT): Hardware, software and protocols used to monitor and control physical devices and operations in critical infrastructures.
- Internet of Things (IoT): Network of physical devices to exchange data with other devices and systems over the internet.
- Digital Transformation and Cloud: The concept to use digital technologies to fundamentally change and improve business operations, business models and strategies accompanying with the approach to use remote servers hosted on the internet to store, manage, and process data, and provide access to other applications and services.

It should be noted that due to the significant advancements in the Advanced Meter Infrastructure (AMI) sector in Greece, this area was further explored.

7.1 Information and Communication Technology Environment

Critical processes in most critical infrastructures are becoming increasingly dependent on information and communication technology, which requires advanced technological solutions to meet their specific demands. Additionally, the diverse usage patterns of

these systems further emphasize the importance of addressing cybersecurity risks [123]. As the process of digitalization continues in the OT environment of critical infrastructures, techniques from the Information and Communication Technology (ICT) sector such as cloud computing and software-defined networking (SDN) are becoming increasingly crucial [162].

Critical infrastructure operators rely on the use of classic ICT systems to support their daily operations. These systems encompass hardware, software and intangible components such as applications, databases, network devices, storage, servers, emails, information, frequencies, etc. which are essential for processing and transmitting organizational data [123], [163]. Additionally, the term "ICT systems" refers to the overall sum of computers and connections between them, including critical information flows that are transmitted through the network [7]. These systems include invoicing, procurement management, customer and personnel management, electronic document handling, communication, and more, which require corresponding software applications and hardware equipment for their operation. Apart from their individual use, software applications are also integrated with IT and telecommunication components as parts of other equipment (e.g. smart grids).

Given that critical infrastructures rely on a range of interconnected hardware and software components, any disruption or malfunction in one component may have ripple effects throughout the entire system, potentially resulting in significant consequences [138].

To be able to defend critical ICT assets first we need to classify the threats and vulnerabilities. Critical information infrastructure security breaches may occur [164] due to several factors, including but not limited to technology failure resulting in direct damage to operating equipment or dysfunctional systems, human error, natural disasters, and prolonged disruptions in the electricity supply.

A different approach is presented at [165], in which after conducting a literature review it classifies these two domains based on objects experiencing threats and vulnerabilitis into seven and four categories, respectively.

- Destruction of Information: An attacker deleting important files from a database.
- Corruption of Information: A virus changing the contents of a file.
- Loss of Information: A hard drive failure resulting in the loss of stored data.

- Illegal Use of Information: An employee using confidential customer data for personal gain.
- Disclosure of Information: An employee accidentally leaking sensitive information to the public.
- Denial of Use: A cyberattack that renders a website or service unavailable to users.
- Elevation of Privilege: An attacker gaining unauthorized access to an administrator-level account.

With regards to vulnerabilities, they are categorized as follows: a) computers, b) information, c) processes, d) people.

A very interesting approach to define the threat landscape, is presented at [13]. After conducting a thorough analysis of the security threat landscape it categorized cybersecurity into six general domains:

- Network-centric: It focuses on data transport and associated security issues, including DDoS protection, SDN, ad hoc networks, encrypted traffic analysis, 5G.
- System-centric: It centers around cloud and virtualized environments.
- IoT/Device-centric: It targets modern systems like IoT/edge devices, addressing middleware, secure OS, security by design, malware analysis, systems security validation, detection of zero-days, and recognizing service dependencies.
- Data-centric: It addresses management, analysis, protection, and visualization of data in Big Data environments.
- Application-centric: It focuses on the security of applications and their management.
- User-centric: It is related with privacy, social networks, fake news, and identity management.

This list presents an overview of the identified main cybersecurity threats about ICT and their respective domains [13]:

Table 7: ICT main threats.

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

Building upon the previous information, study [165] classifies security protection measures into seven distinct types.

Table 8: Security protection measures [165].

Security Measure	Description
Directive	Provide guidance and instructions in order to ensure compliance with security policies.
Deterrent	Discourage potential attackers.

Preventive	Proactively measures to reduce the likelihood of security incidents.
Compensatory	Mitigate the impact of security incidents.
Detective	Identify and alert for potential security incidents.
Corrective	Correct security incidents trying to restore the state of the assets as they were before the incident
Recovery	Restore the system back to normal after an incident

It is important to note that every new tool introduced into a system, although it may decrease the attack surface in some areas, also creates a new attack surface. Vulnerabilities within the tool can serve as a potential point of compromise for the system.

For the majority of organizations, the risk of IT security breaches continues to pose a significant threat to business continuity, necessitating the implementation of measures to prevent threats, expedite incident response, and facilitate prompt disaster recovery [166]. This concern is not unfounded, as there are a constant multitude of new cybersecurity incidents that occur in the area of critical infrastructures, which can potentially compromise the daily usage of informational elements by employees.

According to ENISA [8], there is a growing risk of ransomware attacks, phishing, malware, and DDoS attacks, which pose significant threats to critical information assets.

Cybersecurity trends [167] reveal a persistent incidence of attacks on web applications aimed at extracting data or disseminating malicious code. Malicious actors commonly disseminate their malevolent code through legitimate web servers that have been hacked, while the migration towards cloud computing has introduced new security risks, with traffic capable of circumventing traditional checkpoints. Moreover, mobile networks are highly susceptible to cyberattacks, representing a potential source of vulnerability given the fact that there are numerous devices that expand the attack surface. A plausible explanation for the aforementioned trends may be the increased reliance on information and communication technology (ICT) tools resulting from the COVID-19 pandemic, which in turn has led to a surge in cyber-attacks worldwide [138].

The typical motivation behind attacks in the enterprise ICT domain on critical infrastructures is often the acquisition of data making confidentiality the most important concern of CIA triad [168]. Particularly, databases and file servers are vulnerable to security breaches initiated by insiders [169]. This is not surprising since databases and file servers contain highly valuable and sensitive information, making them attractive tar-

gets for malicious insiders who wish to misuse, steal or corrupt such information. These insiders may abuse their access privileges to carry out attacks, such as data exfiltration or deleting important files. As a result, the challenge for cybersecurity is to find a balance between sharing information and protecting the privacy of individuals.

According to the study [136], over 20% of the stolen information consisted of data that the victim was unaware of being stored on the company's network meaning that there is a significant knowledge gap among both the personnel and the IT administrators with respect to the data stored on the company's network.

Shadow IT presents a similar risk, as it involves the use of information technology and assets within an organization without the approval or knowledge of the IT department. This lack of oversight and control results in reduced security, as threats and vulnerabilities cannot be safeguarded against if they are unknown to the IT department [170]. In addition to confidentiality concerns, the use of shadow IT also raises integrity issues, as the data in these systems may be inconsistent with data in authorized systems due to the absence of proper system interconnection. The significance of observing, monitoring, and analyzing the activities and behaviors of systems and networks (observability) has been also emphasized by [171] as it is placed on the same list as the CIA triad. Observability enhances situational awareness, allowing for efficient incident response and detection of threats.

There are several cybersecurity threats and vulnerabilities that are shared by both the enterprise IT and OT environments but interconnectivity between the enterprise IT and OT networks has introduced new risks [168]. Also the same study, an evaluation was conducted on the security capabilities of both enterprise IT and ICS based on selected frameworks, standards, and guidelines. The result proposed that critical infrastructure operators should acquire six additional capabilities, aside from those outlined by NIST, to attain a higher level of cybersecurity resilience. These capabilities include cloud security asset management, cloud security off-site activities, mobile computing device security, cryptography, audit assurance, and cybersecurity R&D.

[138] describes the basic cyber security aspects in ICT in general, according to the CIA triad. For instance, the security of confidentiality can be compromised by various attacks, including packet interception, side-channel attacks, sniffing, and eavesdropping. Techniques such as encryption, authentication, and randomization can be employed to prevent such breaches. Similarly, attacks such as false data injection, data modification,

and denial of service (DoS) can compromise the security of system integrity and availability. Security measures such as firewalls, antivirus software, intrusion detection and prevention systems (IDS/IPS), and tolerance mechanisms can be utilized to thwart such attacks.

Study [172] revealed that there was a deficiency in implementing two fundamental best practices in information security, namely patch management and incident handling.

In [123], is presented an analysis on the impact of ICT-related threats on the CIA triad, utilizing the classification system of the European VITA project while excluding threats that are not directly related to cybersecurity. The key findings were the following:

- Information is susceptible to threats resulting from human error, misconfiguration, malware, and unauthorized access.
- Hardware is exposed to threats in the supply chain, as it can be subject to malicious or counterfeit materials that could potentially provide unauthorized access or prove to be faulty in specific circumstances.
- Software vulnerabilities in a wide range of applications expose them to targeted attacks, enabling cyber criminals to create malware and gain unauthorized access to sensitive data.
- Intentional interference or burden in the communication of information can lead to a Denial of Service (DoS), resulting in the degradation of service performance.
- The human factor presents a significant risk in terms of cybersecurity, both due to unintentional misuse of information such as social engineering and human error, as well as intentional malicious use such as data leakage.

Study [167] proposes a range of specific countermeasures to address cybersecurity risks, including the implementation of an application firewall, traditional firewall, antivirus software, access control measures, password security protocols, data authentication mechanisms, malware scanners, and cybersecurity awareness training.

The research presented in reference [173] is focused on the utilization of cyber intelligence, cyberspace security strategies, and the establishment of a cyber security range to provide a practical operating environment so they can practice to evaluate new cyber security technologies. This controlled environment allows for the testing of new technologies before they be deployed in real-world scenarios. This enhanced the effective-

ness of designing appropriate counter measures and preparing personnel to better address potential cyberattacks.

Recommending countermeasures against cyber threats, [135] suggests the implementation IDS, IPS, firewalls, SOC and employee awareness campaigns. The study conducted supplements the previous findings concerning data exfiltration, emphasizing the importance of implementing continuous monitoring for data uploaded to cloud environments.

On a more abstract way, ENISA [8] emphasizes that it is necessary to implement a defense-in-depth approach, as state actors may attempt to exploit zero-day vulnerabilities. This is essential to ensure that any failures in one area do not result in the compromise of the entire system. Furthermore, widespread use of certain software can create a gateway for exploitation through a zero-day vulnerability, leading to a breach in multiple systems simultaneously, and even serve as a start for a supply chain attack.

In order to address ICT threats and risks it is recommended to adopt best security practices. This can be achieved through the adoption of various cybersecurity frameworks. One of them is ISO 27001:2022 [174] which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It includes policies, procedures, and controls for managing the confidentiality, integrity, and availability of information. It also provides guidelines for conducting risk assessments and developing a risk treatment plan.

7.2 Operational Technology Environment

In addition to the above established information elements, the backbone of many critical infrastructures such as the distribution and supply of electricity [175] and natural gas [176], water treatment and distribution units [177], sewage and wastewater treatment units [178], etc., rely on the broad use of Operational Technology (OT) [179]. These systems are accountable for ensuring the uninterrupted operation of crucial functions in such infrastructures. The continuous provision of services is dependent on the proper operation of industrial control systems, making their security of paramount importance. Cybersecurity incidents in this area can have the same devastating impact as natural disasters.

The convergence of IT and OT is challenging. The integration of logical and physical components entails that a cybersecurity breach in IT systems could be exploited to gain unauthorized access and control over critical physical systems [180]. Attacks that target sensors or actuators directly can result in significant issues due to the inherent nature of these devices [134].

An example of such an incident is the Triton cyber attack that occurred in 2017 at a petrochemical facility in Saudi Arabia that caused the shutdown of the industrial process and had the potential to impact the physical process [181]. It is possible that the attackers obtained access to the OT network almost a year prior to the attack by penetrating the IT network via a misconfigured firewall, and subsequently transitioning to the OT network reprogramming the Safety Instrumented System (SIS) controllers at the facility, causing them to fail [182]. The malware used in the attack had a unique capability to directly engage, remotely control [183], and compromised a safety system, which is a nearly unprecedented achievement.

These systems comprise remote control systems, Supervisory Control and Data Acquisition (SCADA), specialized sensors, and integrated management systems, aiming to automate and manage industrial processes. Their primary function is to gather data and oversee automation processes that are presented to system operators for informed decision-making [184].

The communication architectures integrated within these systems serve to link the control centers to remote substations that are positioned at the infrastructures under control, while the main components of SCADA systems are the control center, substations and a corporate network [160]. In order to establish wireless telemetry, remote terminal units (RTUs) are employed. Similarly, programmable logic controllers (PLCs) are utilized to perform logical operations via hardware [140]. The OT architecture for CI is predominantly centered around the control components, encompassing hardware, firmware, and software, as well as the network components, which include control networks, field networks, and network access points [168].

The integration of physical systems, computation, communication, and control has led to the emergence of a new field of study called Cyber-Physical Systems (CPS). CPS are primarily utilized in scenarios where their central deployments are unsupervised and unattended. Their purpose is to monitor and control systems based on specific physical attributes [138]. To ensure their efficacy, CPS must exhibit sufficient security and resil-

ience to confront potential adversaries. Additionally, their authorization capabilities for governing systems and infrastructures render them an intriguing target for attackers. Researchers are currently placing greater emphasis on cyber threats in CPS as opposed to physical threats. This is partly due to the limited accessibility that attackers have to physical components when compared to cyber components, which results in a higher level of cyber threats [138].

In the past, OT Systems were heavily dependent on mechanical or electrotechnical devices operating in isolated and segregated environments [162], [185], resulting in limited exposure to potential risks and hazards being disregarded [162], [21].

To aid in the understanding of the risks associated with OT systems, the Purdue Reference Model was selected to present the architecture of the Industrial Control and Automation System (ICAS). The ICAS includes both hardware and software for monitoring and controlling industrial processes, with components from both IT and OT systems. The Purdue model divides the core components of these systems into six zones to categorize their interconnections and interdependencies [163], [182].

Table 9: OT architecture per Purdue Reference Model.

Level 4/5	Also known as the Enterprise Zone, includes corporate IT infrastructure systems and applications.
IDMZ	The Industrial Demilitarized Zone includes security systems aimed at preventing unauthorized data transfer between IT and OT systems.
Level 3	It involves high-level monitoring and management of industrial operations.
Level 2	It encompasses a set of devices and applications that enable supervision, monitoring and control of the physical processes. It includes SCADA, Distributed Control Systems (DCS), and Human-Machine Interface (HMI)
Level 1	It controls input and output devices at Level 0 using PLCs and RTUs.
Level 0	It handles the physical measurement processes using sensors, pumps etc.

It is widely accepted that state actors will persist in targeting critical infrastructures with OT networks, investing considerable time and resources in gathering intelligence to execute successful attacks [8]. Vulnerabilities in OT systems can stem from various levels, including hardware, firmware, software, networks, and processes [163].

According to a survey [186] conducted on organizations utilizing Industrial Control Systems (ICSs), 56% of these operators encountered a breach in their OT systems. Fur-

thermore, the survey revealed that 97% of these breaches were attributed to the convergence of IT and OT.

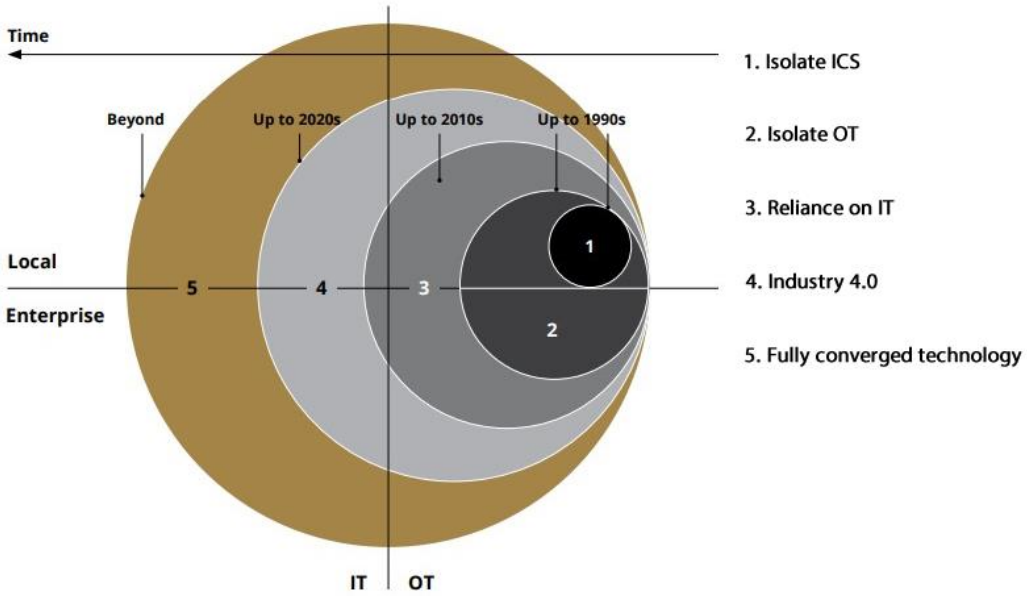

Image 14: Essential technology to deliver the industrial product or service [187]

The recent increased computerization and interconnectivity of OT systems have become indispensable in modern large-scale industrial activities [148]. The situation is aggrevated by the fact that ICS network architecture is typically flat, meaning that all devices on the network are connected at the same level and have similar access privileges thus the intruders has the potential to gain access to the whole unsgemented domain [148].

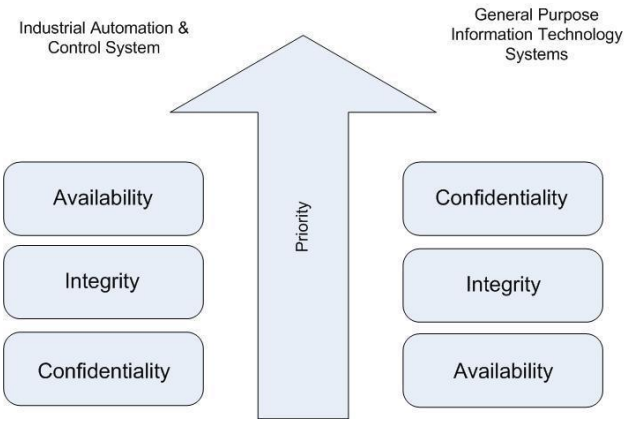

Image 15: ICT security goals in smart grids [73]

In contrast to traditional IT systems where the primary concern is to safeguard the confidentiality and integrity of information, the most significant priority in ICS systems is

to ensure availability and integrity, as they are responsible for the safety of individuals and network equipment, the environment, as well as the management of the systems themselves [73], [146]. A threat that compromises availability would render crucial control, performance, and informational resources inaccessible. In contrast, a threat to integrity would aim to manipulate critical hardware, software, or informational resources. Similarly, a threat to confidentiality would attempt to covertly intercept sensitive information [160]. Within the ICS domain, attacks are frequently motivated by the intention to destabilize the targeted system [168]. A SCADA system's compromised cybersecurity can have severe implications for a power system, particularly if the attack is capable of initiating disruptive switching actions that result in load loss or equipment damage. This is particularly concerning if the attack can infiltrate the control center network, which is linked to substations under the SCADA system [142].

In recent years, ICS systems have become a common target for attackers [188], and analysis of these events has revealed that many attacks exploit vulnerabilities stemming from their design philosophy, which prioritizes service availability over system security [184]. Due to the proprietary nature of SCADA protocols, it is challenging to utilize conventional security mechanisms for establishing zones.

The fact that these systems were developed much earlier, at a time when technology was not as advanced, adds to the problem [2] as many security mechanisms are incompatible with SCADA requirements and policies [160]. Implementation of security solutions such as Intrusion Detection Systems (IDS) in Industrial Control Systems (ICS) can be challenging due to the use of outdated operating systems. This was evident in the case of the National Health Service in the United Kingdom during the WannaCry Ransomware attack, where numerous systems were still running on outdated Windows XP operating systems [134]. Additionally, a significant number of cybersecurity systems that are considered outdated are not congruent with enhanced security systems such as intrusion detection devices and advanced encryption systems [140], [189], [146].

Another factor is that the deployment of security technologies to this type of systems is frequently challenging and complex, primarily due to the various types of devices utilized and their limited computing power capacity [162].

OT systems were not structurally designed to be permanently connected to the internet, which makes the situation more challenging at the modern days [162] were the trend is the migration to Cloud infrastructures. The migration to TCP/IP protocol for substation

communications has opened the door to relevant traditional threats and vulnerabilities [160]. The vulnerability of the network access interface to such attacks is feasible when accomplished through the internet resulting in unauthorized control of the systems compromising Authenticity [138].

Industrial environments, owing to their connectivity to the internet, are inherently vulnerable to an extensive array of security threats. These may include, but are not limited to, the duplication of assets, malicious replacement of assets, firmware substitution, theft of security parameters, interception of information, man-in-the-middle attacks, ransomware, routing attacks, and denial of service (DoS) attacks [162]. Also, SCADA systems are inherently vulnerable to a multitude of threats, which may arise from hardware or software malfunctions, operational errors, or deliberate and malicious actions [160]. The incorporation of wireless technologies also entails significant security concerns such as jamming, black hole attacks, wormhole attacks, DoS, eavesdropping. [160] also agrees to those findings underlying that the integration of ICT technologies into the control and operation of critical services has amplified many of the potential threats such as replay control messages, DoS attacks, eavesdrop, malicious command injection, parameter poison, unauthorized access, malware. Reference [138] expands upon this issue by indicating that a multitude of attacks are possible on controllers, including but not limited to logic manipulation, system command injection, memory corruption, firmware modification, and malicious code injection into firmware.

Previous study [138] has identified various risks, including but not limited to frequent system logins, lack of logging, absence of firewall and intrusion detection system (IDS), inadequate software maintenance, improper network configuration, and easy accessibility to the systems. Furthermore, component-interaction-wise attacks, such as disclosure, deception, and disruption attacks, can occur, which correspond to breaches of confidentiality, integrity, and availability, respectively. The study refers to many other possible attacks on ICS controllers such as logic manipulation, system command injection, memory corruption, firmware modification, and firmware malicious code injection.

SCADA protocols pose a significant source of security issues and risks due to their susceptibility to multiple vulnerabilities resulting from unsecured or vulnerable protocols [160], [138]. Common vulnerabilities in such protocols include (a) the opening of unnecessary ports during system startup, (b) unencrypted and insecure communication, (c) inadequate prevention strategies against DoS attacks, (d) device reengineering capabili-

ties, (e) improper configurations, (f) lack of proper authentication and authorization mechanisms, and (g) utilization of default keys, among others. To mitigate these vulnerabilities, it is essential to adopt secure communication mechanisms through encryption, authentication, and authorization. Additionally, packet filtration and blocking techniques can be employed to prevent DDoS attacks [138].

The realization of a secure and safe operation of ICS is reliant on numerous diverse factors of varying nature, including but not limited to administrative, regulatory, human-centered, technical, and environmental factors [190].

IT executives often mistakenly consider ICS elements as non-informational elements, leading to a lack of attention to their security considerations [123]. Therefore, it is strongly advised to establish separate yet integrated cybersecurity teams for enterprise IT and ICS within a single security operations center [168]. Effective personnel training is also crucial for conducting a comprehensive assessment of OT security risks. Insufficient familiarity of a power plant's SCADA system by a network administrator may lead to the compromise of the entire infrastructure [5]. For that reason efforts to converge IT security methods with OT should be undertaken to enhance the adaptability of security measures to the OT environment [179].

A crucial aspect to consider while assessing the security measures in an organization is the challenge of implementing interventions and controls within the infrastructures due to the need for continuous and uninterrupted operation of the OT systems [146]. An example of this is the necessity for continuous operation of SCADA operated pumping stations, as any interruption could result in an environmental hazard. A viable solution to this issue is to increase capacity and redundancy to ensure uninterrupted services in the event of a cybersecurity incident or necessary security system upgrades. A potential defense mechanism to counteract this risk is the integration of honeypots within the system perimeter. This approach ensures that the operational integrity of the systems is not compromised, while simultaneously impeding the progress of an attacker by misleading them into believing they have successfully infiltrated the system [191].

The Digital Twin approach is another potential solution [138] that can be adopted for enhancing the security of CPS. Digital twins are virtual replicas of physical objects that enable monitoring, visualization, and prediction of the states of CPS. By assessing the failure modes of the digital twin, it is possible to identify possible security flaws and evaluate whether the system fails safely and securely. Additionally, the system behavior

can be analyzed under attack, providing insights into potential vulnerabilities and enabling the development of effective mitigation strategies.

The study [142] presents a security framework for SCADA systems, which comprises four key components: real-time monitoring, anomaly detection, impact analysis, and mitigation strategies. Furthermore, the research underscores the importance of additional investigation in the following areas:

- Development of SCADA-specific real-time correlation and intrusion detection algorithms.
- Creation of online risk monitoring and mitigation algorithms that consider both cyber system vulnerabilities and their associated consequences.
- Use of advanced modeling techniques that accurately capture the dynamic behavior of attackers and the system.
- Advanced modeling that accounts for impacts such as load loss, equipment damage, and economic loss. Moreover, periodic vulnerability assessments can be conducted to ensure system security.

To ensure the security of these resources, technical measures can be implemented, such as external access must be fortified with firewalls, demilitarized zones (DMZs), intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and anti-virus software. Furthermore, access must be enabled for the corporate network that facilitates business operations, while the utilization of cloud computing infrastructure can offer significant operational benefits, such as data redundancy, data availability, and survivability [160]. Employing digital encryption standards is a widely adopted strategy for protecting ICS systems from potential cyber threats.

Modern technologies such as AI and machine learning can also be beneficial in addressing OT security issues. Reference [138] introduces a security framework that utilizes machine learning models to enhance system security. The framework considers approaches for improving performance, achieving optimal performance, and reducing computational requirements, as well as strategies for resilience against adversaries. To enhance system performance, the framework utilizes Hyper-parameter Optimization to optimize performance and reduce computational requirements by reducing complexity, training time, and overfitting.

A classification among defense strategies against cyber attacks can be categorized into prevention, resilience, and detection and mitigation mechanisms. Prevention mechanisms aim to delay the onset of an attack, while resilience mechanisms focus on minimizing the impact of an attack and preserving the system's normal functioning as much as possible. Detection and isolation mechanisms identify the source of the attack, isolate affected sub-components, and aim to restore the normal state of the system as quickly as possible. The deployment of a security solution in CPS must adhere to domain-specific constraints and provide robust security against both known and unknown attacks, including zero-day attacks [138].

The work presented in [163] proposes a holistic approach to secure OT systems against cyber attacks by protecting all components that constitute the entire threat surface, including physical assets, networks, devices, software, human factors, and processes. The proposed strategy includes the implementation of technical measures such as Intrusion Detection System, network segmentation, system hardening, and endpoint security. Additionally, physical security needs to be enhanced, and cybersecurity awareness and training must be provided. The conduct of a risk assessment is also recommended to identify, categorize, prioritize, and mitigate potential risks.

NIST has provided extensive guidelines through its publication of the Special Publication (SP) 800-82 Rev. 2 [192], aimed at fortifying Industrial Control Systems against cyber threats. This guide comprehensively addresses the selection, implementation, and management of security controls for ICS, while offering in-depth insights into the detection, response, and recovery from cyber incidents that may occur. The publication provides a comprehensive approach for maintaining the security of ICS, which is crucial in ensuring the continued operation of critical infrastructures in the face of emerging cyber threats.

7.3 Internet of Things

In recent times, the emergence of Internet of Things (IoT) technology and its associated capabilities have fundamentally transformed the implementation of wireless communications. By facilitating the inclusion of non-traditional physical objects within a network and allowing remote accessibility to such devices, IoT has brought about a paradigm shift in the domain. One may posit a definition of IoT as an overarching framework that interconnects objects with the Internet, enabling communication between dif-

ferent entities, including people, objects and distinct ecosystems. IoT systems are involved in various aspects of human life, encompassing daily activities, industry, self-driving cars, retail, healthcare, smart grids, business, farming, and more [193].

The integration of IoT has significantly contributed towards bridging together the traditionally distinct realms of IT and OT [194], [195], [185], fulfilling emerging requirements and contemporary management needs. However, this integration has resulted in new requirements for the convergence and interaction between these spheres [188].

The use of IoT is prominent to critical infrastructures. They can be found in smart grids, healthcare, industry, at transportations part of smart cities etc [193]. It is more than obvious that IoT is associated with human well-being as evidenced by practical applications of IoT in critical infrastructures like this one in the UK where providers of wastewater and drinking water services rely on a combination of Industrial Internet of Things (IIoT) sensors, real-time data, and analytics to identify and predict equipment failures, as well as to respond rapidly to emergency situations such as water leaks [185]. As it is easily understood, any security risks posed by the lack of security in IoT may lead to incidents which can potentially endanger human lives, something that it is underscored at study [189] drawing on two case studies of critical infrastructures - one on energy management and the other on smart transportation.

The functionality of IoT is accomplished through the utilization of various technology devices that communicate via applications using a diverse range of protocols and natural frequencies. This considerably increases the potential targets for attackers as the vast majority of objects and applications implemented in IoT systems are not engineered to prevent or handle intrusions, resulting in an enlarged surface area and attack vectors that could potentially exploit this type of infrastructure making them a vulnerable target for cybercriminals, providing an easy point of entry for attacks on critical infrastructures [196].

Cybersecurity in IoT systems differs from that in conventional ICT-only systems in various aspects, such as complex cybersecurity deployment landscapes, cyber-attacks on physical systems, and physical attacks on and physics-based mitigation for cyber systems [180]. Although this is the case, it is worth highlighting that despite their groundbreaking impact on the technological landscape, contemporary IoT devices are plagued with security issues that are common to traditional IT systems [197]. Attack surfaces in IoT systems can be diverse and may include the device firmware, various interfaces

such as web, administrative, and physical interfaces, hardware components, device memory, system applications, and network services [189]. The same study proposes a threat architecture that encompasses the same three architecture IoT layers namely, (i) perception layer that perceives the data from the surroundings, (ii) network layer that forwards the data, and (iii) application layer that provides an interface to the end user [189]. Attacks according to [184] can be differentiated on those that target backend devices used in critical infrastructures, and those aimed at end-user IoT devices. These devices are classified based on their connection to critical infrastructures, either directly or indirectly. Additionally, IoT vulnerabilities are categorized into embedded and network vulnerabilities. The study in [184] aims to differentiate various types of attacks in IoT environments. In healthcare facilities, the attacks are categorized as computational, listening, and broadcasting, based on their ability to modify, intercept, or disseminate data, respectively. On the other hand, in 5G cellular infrastructures, attacks are classified into privacy, integrity, availability, and authentication categories.

A significant amount of research has demonstrated the presence of security and privacy vulnerabilities in systems enabled by IoT technology. These vulnerabilities include issues related to authentication, authorization, DoS attacks, and information leakage, among others [193]. In the subsequent discussion, we aim to illuminate the various factors that give rise to this phenomenon based on the review of existing literature.

The frequency of IoT device breaches has surged due to the convenience of exploiting security weaknesses resulting from the devices' limited resources, lack of security software, and the diversity of interfaces and protocols employed [134].

The network is a common vector for many IoT vulnerabilities [189]. Vulnerabilities that exist in IoT systems are apparent not only to basic IoT devices but also industrial safety systems, leading to incidents such as large-scale DDoS attacks resulting in significant consequences [198]. In recent years, there has been a substantial surge in the frequency, magnitude, and diversity of distributed denial-of-service (DDoS) attacks [195], [196]. The primary objective of these attacks is to render services inaccessible by inundating the target destination with an overwhelming volume of packets from multiple sources, eventually leading to unresponsiveness or network saturation, thereby impeding the seamless operation of the infrastructure [196].

Privacy concerns arise as well as end-users are responsible for safeguarding their device data, which is compounded by the inability to implement conventional authentication

practices due to the sheer quantity of devices connected to the network [179]. Insecure interfaces, such as the lack of device authentication/identification and insufficient encryption, are also deemed to be a critical vulnerability. Moreover, default credentials represent another prevalent challenge, for which manufacturers have yet to offer a satisfactory solution [197]. Vulnerabilities related to cryptographic mechanisms have been identified as the most commonly exploited ones [189]. The lack of a comprehensive security and/or privacy-protecting framework exacerbates the problems [193].

Also, the limited computational resources of IoT devices prevent them from utilizing security solutions like intrusion detection systems (IDS) or antivirus software, which increases their susceptibility to security breaches [179], [134].

End users are also contributors to this negative phenomenon as human-related factors also significantly bolster these breaches [134]. A lower level of security awareness is prevalent among IoT stakeholders and users, providing adversaries with a larger landscape of potential threats [189]. Among the most significant cybersecurity threats in the IoT sector is inadequate parameterization, which arises from limited awareness of cybersecurity concerns or insufficient knowledge, leaving the devices vulnerable and susceptible to access from the internet [197].

The integration of IoT devices into OT infrastructures, in particular, renders them susceptible to external exposure [179]. Notably, the Zoomeye search engine has amassed data on over a billion IoT devices, highlighting the scale of the issue [179]. A highly enlightening study [197] revealed that N-day vulnerabilities continue to pose a significant threat, with 28,25% (385.060) of the devices studied being found to have at least one such vulnerability, and 2.669 of these devices having already been infected by botnets. Significantly, since N-day vulnerabilities are publicly known, they represent a potential time bomb for the security of unpatched devices.

The study presented in [194] delves into the security risks associated with the IoT landscape in healthcare institutions, with particular focus on the perception, network, and application layers.

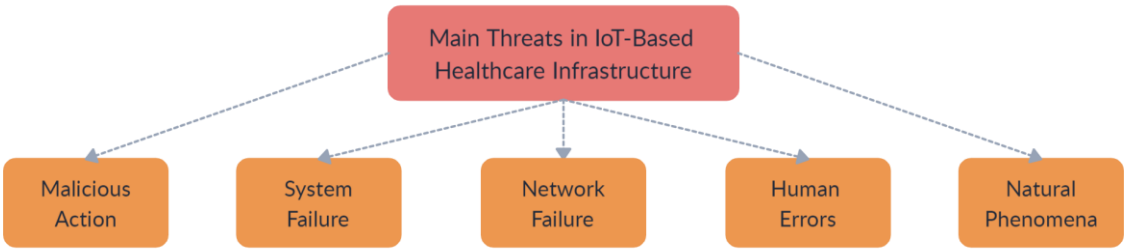

Image 16: Healthcare IoT main threats [194]

Session hacking, Ransomware, and DoS attacks [196], as well as vulnerabilities related to RFID systems, are identified as the key technical assaults. The research findings presented in [197] are of particular significance, as they reveal the inclusion of IoT devices in both ICS infrastructures and medical devices. This suggests that any security breach could result not only in the disruption of critical infrastructures but also pose a threat to human life.

The study [193] summarizes the key security requirements, threats, and potential solutions in the IoT application use cases.

Table 10: Summary of the key security requirements in the IoT application use cases [193].

	Key requirements						
Use Case	Confidentiality	Integrity	Availability	Authentication	Authorization	Non-repudiation	Privacy
Smart grids	x	x	x				
Smart Healthcare	x	x		x	x	x	x
ITSs	x	x	x	x		x	
Industrial IoT	x	x	x	x			
Threats	Password-pilfering, Traffic analysis, Eavesdropping, Unauthorized access, False data injection, Password theft, Data tampering, Wormhole, Spoofing, Mitm, Masquerading, Jamming, DoS, Buffer overflow, Malware						
Solutions	Data encryption, Authentication encryption mechanism and protocols, Cryptography, Security gateways, End-to-end-encryption, Traffic filtering, Anomaly detection, Air gapping, Anti-jamming, Access control, Security of cloud computing, Monitoring, Digital signatures and certificates.						

It highlights three significant challenges. A significant limitation of many IoT devices is their constrained processing and storage capabilities, which may prevent the implementation of resource-intensive security techniques such as anti-malware and advanced se-

curity protocols. Also, IoT security approaches mostly focus on defending against remote adversaries and assume that the devices are not physically accessible to the adversaries. However, this assumption does not hold true for large-scale IoT networks, which consist of numerous dispersed devices. The third challenge relates to the extended duration of sessions, as it provides an increased opportunity for attackers to interfere with the system [193]. Mitigating cybersecurity risks in IoT environments is vital to ensure the safety and security of critical systems.

According to the same study the key security requirements of the IoT application layer including authorization, confidentiality, integirty, availability, authentication, non-repudiation, and privacy. Multiple strategies can be employed to secure Industrial Internet of Things (IIoT) applications, such as safeguarding data confidentiality, implementing network segmentation, detecting and preventing attacks, ensuring the integrity of cyber-physical systems, and providing employee training [185].

Machine learning models are frequently utilized in IoT networks to address a variety of security concerns, such as identifying and detecting attacks and malware, detecting malicious code, identifying and responding to DDoS attacks, and performing facial recognition and authentication [193].

An example of this strategy in order to alleviate the impact of DoS attacks is presented at [196]. This study suggests an architecture that employs a machine learning (ML) model to differentiate between legitimate and malevolent network traffic. The goal is to attain a supervised, self-organized, and regulated operation of the micro-level IoT components and then control the processes that emerge from the macro-level operations.

[199] sheds light on diverse solutions utilizing Blockchain technologies to enhance security, privacy, and confidentiality in IoT. Additionally, these solutions promote the principle of security-by-design in IoT, as remote patching can be accomplished more securely. Furthermore, [200] presents a proof of concept for the implementation of Blockchain-based solutions in industrial IoT use cases, such as the transmission of data from smart meters and toll infrastructures.

The emerging technique of cyber deception aims to impede an attacker who successfully penetrates the front lines of defense by infiltrating the digital perimeter. This is achieved by deploying decoys or traps that imitate the behavior of virtual assets, redirecting the attacker's attention away from actual targets. This strategy allows defenders

to buy time, increase the probability of intruder discovery, and mitigate the potential impact of the attack [201].

In [179], the utilization of opacity techniques in IoT systems is suggested as a means to prevent attackers from obtaining accurate knowledge of the system's state, even if the communication channels are insecure. Representing the control system of the OT environment as a Discrete Event System, driven solely by physical events, creates a more secure interface between IoT and OT.

Study [198] highlights the importance of the consideration of security standards and certification schemes on IoT industry in order to assess cybersecurity risks.

NIST at its special Publication [180] for Cyber-Physical Systems and Internet of Things underline that effective cybersecurity strategies for CPS/IoT should consider the ongoing development of operating systems, threat landscapes, and IT capabilities for long-lifecycle CPS/IoT systems with components that may remain in use for the long term. Additionally, proposes that cybersecurity must be addressed in systems that operate in physical time as opposed to logical time. The implementation of resilience features such as fail-safe and fail-operational provisions, as well as authentication solutions that can handle the large scale and high speed of interacting CPS/IoT systems, should also be considered.

The implementation of cybersecurity by design has been recognized as a crucial necessity for all Internet of Things (IoT) devices. The Cybersecurity Strategy explicitly mentions that “All Internet-connected things in the EU, whether automated cars, industrial control systems or home appliances, and the whole supply chains which make them available, need to be secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered” [145]. In addition to cybersecurity by design, it has been noted that smart metering systems must also adhere to the principles of privacy by design and by default.

7.4 Advanced Metering Infrastructure and Smart Metering

In recent years, a growing number of utilities that are part of national critical infrastructures have been implementing a digital transformation strategy involving the gradual replacement of old meters with smart ones as part of their Digital Transformation plans. This trend is becoming increasingly prevalent globally [202]. In Greece, at water sector,

EYDAP has included in its investment program [203] the replacement of older meter technology to transition to the smart network by installing up to 2.5 million smart meters [204]. Similarly, EYATH has plans to install up to 200,000 smart meters in the next seven years [205]. Simultaneously, the electricity sector is currently engaged in integrating its distribution system with communication networks and control techniques to form a bidirectional infrastructure of power and information flow, commonly known as the smart grid [206]. HEDNO has announced its plans to transition to smart meters and is currently implementing a pilot program worth 41 million euros [207].

Smart meters are distinguished from conventional meters by their ability to facilitate two-way communication [202], [160]. In addition, they can be controlled remotely or locally, and are capable of performing various control commands, including shutting down the provision [208]. The implementation of smart meters will enable utilities to develop improved pricing plans featuring multi-scale and time-zone charges, detect leaks at an early stage, remotely manage operations, reduce costs, and prevent theft, among other benefits [202], [209], [210].

To illustrate, Advanced Metering Infrastructure (AMI) primarily comprises of various components such as: a) smart meters for collecting and transmitting data, b) the Gateway acting as an intermediary between the customer and the infrastructure, c) the communication network for managing the flow of information, and d) the information management system that integrates the AMI with external systems [211], [206], while the Meter Data Management System (MDMS) plays a pivotal role in analyzing and forecasting based on AMI data [212].

In addition to the undeniable advantages, the utilization of smart meters also presents potential risks to both the infrastructure and consumers. Smart meter security priorities are comparable to those of conventional ICT environments [73], which expose them to the complete spectrum of threats posed by the CIA triad.

The remote control of smart meters by malicious actors in an AMI infrastructure poses a one of the most severe scenarios, potentially resulting in the disconnection of a large number of users from essential services. Since data transmission occurs wirelessly, the transmission medium is accessible to anyone [211]. This vulnerability makes the AMI a potential entry point for the smart grid network. The consequences of such an attack could be catastrophic, ranging from noncompliance with regulatory standards to ecological disasters (e.g., failure of a smart electricity meter at a pumping station) or even loss

of life (e.g., disabling a smart water meter of a hospital). The aforementioned security risks have been recognized by various authorities and have resulted in actions to mitigate these threats. For instance, in the Netherlands, the authorities have disabled the remote disconnection feature of smart meters due to security concerns [213].

An additional layer of concern arises with smart meters, as interference and data integrity violations may not be immediately detectable, unlike the destruction of a traditional meter [211]. In 2009, a vulnerability was demonstrated in a specific type of smart meter that could allow an attacker to remotely control the meters, potentially affecting up to 15.000 homes within 24 hours [73].

Denial of Service attacks can affect both the gateway and the end-user in a smart metering system, resulting in a decrease in the quality of measurement services and hindering the proper operation of the measurement system [214].

Similar concerns also arise regarding the confidentiality and privacy of consumer data, which can ultimately impact their personal lives.

The collection of meter readings is now being acknowledged as personal data as they can disclose information about an individual's routine. Therefore, for energy services that add value to end-users, the Confidentiality-Integrity-Availability (CIA) strategy is preferable to the Availability-Integrity-Confidentiality (AIC) approach [73]. In terms of prioritization, as previously stated, availability and integrity are given priority in the smart grid [73], [206].

Smart meter usage may result in privacy issues primarily due to the gathering of detailed data (load profiles) for particular, distinct, and brief intervals [215], [211], [145]. Despite encryption, data transmission patterns can reveal the actions and behavior of residents [216], while consumption data may disclose information about individuals' economic status [215]. Furthermore, the eavesdropping technique can be employed to determine whether individuals are present in their residence, which poses significant privacy and security risks (known as a Presence Privacy Attack - PPA) [216].

Differences in data transmission times may exist across different countries [215] while, discussions at the European level are taking place regarding the implementation of 15-minute interval measurements for energy meters [145].

Table 11: Smart meter time interval data gathering [215].

Country	Time Interval
France	30 minutes
Netherlands	Once a month
Norway	30 minutes
UK	As often as 30 minutes
Canada	15 minutes
US	Varies (California is hourly for residential use, 15 min for commercial use)

The aforementioned issues raise concerns about the regulatory compliance of organizations with the fundamental principles of the GDPR, including consent, purpose limitation, data minimization, the right to limit the use of data, and the right to access, rectify, and erase personal data [215], [56]. Moreover, consumers may avoid adopting smart meters due to concerns about potential leaks of their personal data.

The use of a large number of smart meters poses a challenge for security solutions, as traditional solutions such as adopting a Public Key Infrastructure (PKI) are not scalable due to the need for digitally signing and verifying each message [206].

One of the potential risks associated with smart meters is the unauthorized acquisition of sensitive information or disruption of network services, as demonstrated in a black hole attack targeting communication between a meter and an access point [217]. To address this issue, it has been proposed to establish a dedicated path between the meter and the access point during the network discovery phase as a preventive measure against such attacks.

Regarding technical vulnerabilities, there appear to be several issues with AMI systems such as weak authentication control and protocols, poor software quality [208], [218], errors handling, and improper session management [208]. A comprehensive list of potential attacks on smart meters is presented in [214].

Table 12 : Smart meter potential attack list [214].

Security Attacks	
Local Attacks	Remote Attacks
Session Hijacking	Wormhole Attack
Snooping	Black hole Attack
Denial of Service	Byzantine Attack
Device Tampering	Resource Consumption Attack

Impersonation	Routing Attack
Packet Replay	Network Manipulation
Repudiation	

The implementation of advanced measurement infrastructures involves numerous technologies, resulting in a considerable attack surface, making it challenging to design and maintain a scalable and reliable solution.

To ensure the security of the AMI network, it is essential to design the network with built-in security mechanisms that prevent unauthorized access and interaction between consumer meters. This is particularly important to prevent situations where one consumer may gain access to another consumer's sensitive data [211]. Additionally, all existing interfaces, processes (e.g., firmware updates, etc.), and devices themselves must be considered to ensure secure solutions [73]. Failure to take all elements into account in advanced measurement infrastructures could potentially expose them to risks where attackers can compromise the confidentiality and integrity of data, manipulate account adjustments, modify functionalities in the data center, and more.

To mitigate DoS attacks, it is recommended to use different predefined frequency channels over time, as stated in [214]. In addition, to mitigate network interference and packet flooding, it is recommended to design a resilient AMI with built-in mechanisms to switch to alternate frequency channels if the default channel is unavailable for a certain period. Another approach is to implement network traffic filtering to prevent ping requests that flood the network and cause it to become unavailable to legitimate users [219]. Additionally, [220] suggests a new authentication approach based on Physically Uncloneable Functions (PUFs), which improves communication security, anonymity, session keys, and is robust against impersonation, replay, man-in-the-middle, and DoS attacks.

The Integrated Authentication and Confidentiality (IAC) protocol offers an effective and secure solution caused by the large number of smart meters and PKI inefficiency. The protocol involves mutual authentication between a neighboring smart meter acting as an authenticator and a remote server located in the local management office. Through this authentication, secure encryption keys are obtained for subsequent secure data communication [206].

To address the eavesdropping attack discussed in [216], the Change and Transmit (CAT) technique is proposed, which involves the use of spoofed data to mislead attack-

ers who are monitoring packets, thus preventing them from verifying the presence of tenants in the building. Additionally, in [218], it is suggested to equip smart meters with a Privacy Preserving Jammer (PPJ) that continuously monitors channels and emits jamming signals upon detecting packets transmitted by the targeted meter to prevent eavesdropping.

Several solutions have been proposed to address the confidentiality and privacy issues associated with smart meter technology. One such solution is the adoption of the "opt-out" principle [56], which allows individuals whose personal data is at risk to choose to retain an analog meter or restrict the data collection capabilities of smart meters [215]. A potential solution to address this particular issue is the use of aliased data, which involves converting the original data set into an alias or destroying the data after use if deemed necessary [212]. This can provide an added layer of privacy and prevent the exposure of sensitive information, even in the event of a data breach or unauthorized access.

It is crucial to ensure that communication between different AMI nodes is encrypted, as noted in [211] and [219]. Encryption mechanisms such as RSA should be incorporated at both the application and transport layers. Verifying the source of the data accurately is crucial for authenticating the consumer with the AMI they are communicating with and for the AMI to validate the authenticity of legitimate consumers.

A privacy-enhanced cryptography system proposed in [221] presents a solution to prevent insiders from obtaining information about the consumption of specific consumers. This is achieved by introducing factors into the data, which allow insiders to only receive the total electricity consumption of a group of users, without knowing the electricity consumption of each individual user.

Another proposed solution to protect privacy is presented in [222], which suggests placing a device with a battery and a control system between the smart meter and the circuit breaker. This device identifies peaks and dips in power usage and removes information that could reveal specific device usage, thus enhancing privacy.

In terms of organizational and regulatory standards and directions, the European Union has introduced Directive (EU) 2019/944 [223]. This is a noteworthy piece of legislation that encourages Member States to advance the development of smart metering systems while also prescribing minimum functional and technical requirements that smart meters must meet to comply with the Directive's provisions. This is the first legislative ini-

tiative that explicitly highlights the necessity for ensuring a high level of cybersecurity protection for smart metering systems in EU law. In the water sector, the regulation of smart meters is still in its nascent stages, and in some cases, nonexistent [145]. Despite the lack of technical specifics within the Regulation, it emphasizes the importance of incorporating security considerations and implementing the most effective available practices to achieve optimal levels of cybersecurity. It also underscores the need to balance associated costs and the principle of proportionality.

7.5 Digital Transformation and the Migration to Cloud Infrastructures

The emergence of new technologies has resulted in the phenomenon of "digital disruption" [43], which led organizations to pursue digital transformation to maximize efficiency. This concept is multidisciplinary in nature, encompassing changes across various domains such as strategy, organization, information technology, supply chains, and marketing [224]. The widespread availability of large amounts of data, along with the emergence of new digital technologies like artificial intelligence, blockchain, the Internet of Things, and robotics, is expected to have significant and wide-ranging impacts on business [224]. The mindset is gradually shifting from the need to know to the need to share knowledge [13].

The need to shift service delivery from traditional interaction channels to digital channels is one of the guidelines of the Digital Transformation Bible [225], establishing them as the default and default mode of service delivery. This has meant changing the way organizations operate and moving many of their business processes into the digital world with all the attendant disadvantages and advantages.

Processes that have over time been performed in manual ways are now being radically transformed thus improving the effectiveness and efficiency of organizations thereby significantly increasing the service to citizens. The encoding of analog information into a digital format (digitization) and the alteration of existing business processes with the use of digital technologies (digitalization) results in the emergence of new business models (digital transformation) [224]. With the advent of IoT and edge/fog computing, production processes have undergone complete digitization [201]. Processes such as information storage, document production and exchange, authentication and identification processes and citizen/customer/consumer communication are now being trans-

formed and implemented in digital form, transferring the associated risks of the digital world to the new processes at all levels of the CIA triad.

In this context, the prevailing trend is the migration of systems to the Cloud [226]. Cloud computing offers significant benefits such as cost and resource allocation among users, improved collaboration, scaling, as well as providing access to information services regardless of their geographical location allowing remote working [227]. It provides several services through three main models [228], [229], [230]:

- Infrastructure as a Service (IaaS) offers various computational resources like network, virtualization, virtual machines, firewalls, and storage.
- Platform as a Service (PaaS) typically includes all the previous plus software development programs and tools.
- Software as a Service (SaaS) model enables users to run applications on the cloud.

Large IaaS and PaaS services that provide services to other IT vendors are considered the most critical services in cloud computing [231].

Furthermore, based on their visibility, clouds are categorized into private, public, hybrid, and community [227]:

- The public cloud is a cloud infrastructure that is publicly available on the internet and can be accessed by anyone.
- A private cloud is an IT infrastructure that combines the services and resources of an organization and is not accessible to external entities.
- The hybrid cloud is a combination of private and public cloud infrastructure and allows organizations to utilize the benefits of both models.
- A community cloud is a shared infrastructure among several organizations that have a shared interest and allows them to share resources while maintaining a certain level of privacy and security.

In the context of a cloud service, the interaction typically involves three parties: the service user, the service provider, and the cloud provider. The resulting threat landscape arises from the combination of these parties. The Service-to-User and User-to-Service surfaces are considered the most vulnerable because of the web-based interaction between them, which exposes a wide range of possible attacks [139].

With the increasing adoption of cloud-based services to support business operations, the Greek government has begun to migrate public services [232] to the government cloud, while critical infrastructures have been also integrated their systems under this regulatory context [233]. However, this action may pose security risks, as the transfer of outdated systems outside the perimeter of the organization's network significantly increases the total attack surface and overall risk as cybercriminals tend to follow technological developments and cloud is not an exception to this [8]. This is particularly concerning given that the security of critical infrastructure systems was not a major priority in the past, as they were often air-gapped. The Stuxnet incident revealed that even fully isolated infrastructures are vulnerable to attack [234].

Furthermore, the use of specific Cloud hosting platforms such as Microsoft Azure, Google Cloud, and Amazon Web Services, whose procurement tender specifications are publicly available, creates potential security risks. Attackers can easily obtain knowledge of the hosting infrastructure's characteristics and vulnerabilities, rendering them vulnerable to zero-day attacks. SolarWinds incident revealed that hackers may have utilized US cloud services to conceal themselves and take advantage of the results of their initial hack [111].

The integration of Greek critical infrastructures [235], [233] into the wider interoperability of public sector entities [232] for electronic identification and authentication of individuals for the provision of digital public services appears to be a positive development. However, a more thorough analysis reveals potential risks. At the time of writing this study, the authentication process via Taxis, the Greek government's central identity management system, does not fully support multifactor authentication (MFA), which may create vulnerabilities depending on the nature of the services for which it will be utilized.

The official access guidelines for the G-Cloud [236] and the Interoperability Center of the Ministry of Digital Governance [237] platforms do not appear to incorporate MFA either. This implies that if the passwords of the employees responsible for handling requests are compromised, attackers could potentially disrupt the online services of critical infrastructures. Moreover, it is worth noting that the common practice of disclosing Taxis codes to accounting firms may result in granting access to systems that the user may not be aware of.

Similarily, Signle Sign-On (SSO) authentication carries potential cybersecurity risks including compromised credentials, lack of control over third-party applications, and single point of failure. If a user's SSO credentials are compromised, the attacker can gain access to all linked accounts, which can lead to a significant data breach. Moreover, SSO enables third-party applications to access user information, which increases the risk of unauthorized access and data breaches. Thus, a successful phishing attack can grant an attacker direct access to all systems.

The adoption of the "once-only" principle [225] in the digital transformation process has resulted in the creation of information repositories that eliminate the persistent issues of repetitive information updating. However, these repositories are considered high-value targets for attackers. Moreover, the multi-channel and omni-channel communication capabilities, which provide direct means of interaction between stakeholders and organizations [224], also introduce significant cybersecurity risks, particularly through mobile devices. These vulnerabilities are further amplified by the lack of cybersecurity awareness and culture among users, especially in cases where Bring Your Own Device (BYOD) policies are in place [238].

Additionally, it is important to consider regulatory issues related to the General Data Protection Regulation (GDPR), particularly with regards to the storage of personal data in a country outside of the European Union. In such cases, it is imperative to ensure that the country in question provides rules that are deemed adequate by the EU [55]. Failure to comply with these regulations could have significant impacts, particularly for critical infrastructures like healthcare sector.

The use of cloud technology has facilitated rapid and extensive data sharing. Nevertheless, the sharing of data through cloud-based systems exposes it to various types of malicious attacks [239]. Due to users' inadequate knowledge, it is not uncommon to inadvertently grant access to shared files to unintended parties across multiple platforms. This type of error can have significant consequences in terms of data confidentiality and integrity, as unauthorized parties may be able to gain access to sensitive information, causing potential harm to the organization.

Given their broader attack surface compared to wired links, wireless communications have made many potentially critical facilities accessible even via the World Wide Web [148]. A significant proportion of data breaches during the pandemic were related to cloud assets [139].

Similar challenges arise with remote work, particularly with the Remote Desktop Protocol (RDP) which is a crucial protocol in this context. It serves as a vital network protocol for establishing connectivity with corporate networks through the internet. Regrettably, cybercriminals have identified RDP as a prime target to illicitly gain entry into corporate networks. The exploitation of RDP by malevolent actors enables them to execute code from a remote location, thereby conferring access to either the target machine or the entire corporate network. This places organizations at grave risk of significant compromise [139].

As previously discussed, the Infrastructure as a Service (IaaS) model is employed by some of the largest technology companies such as Microsoft Azure, Google Cloud, and Amazon Web Services. A study [197] discovered that 64,309 MQTT servers were hosted primarily on one of the aforementioned platforms and were accessible via the internet. Shockingly, 88% of these servers were unprotected, allowing for direct connection and access to the hosted data.

Table 13: Unsecured MQTT servers [197].

Platforms	Total	Unsecured Servers	%
Amazon Web Services	4.070	3.314	81,4%
Alibaba Cloud	6.936	6.420	92,6%
Google Cloud	999	874	87.5%
Microsoft Azure	1.226	1.030	84,0%
Tencent Cloud	1.246	1.102	88,4%
Total	**14.477**	**12.740**	**88,0%**

The utilization of the MQTT protocol for machine-to-machine (M2M) communication significantly elevates the significance of this discovery.

As stated at [139], the adoption of cloud technology also includes the potential risk of distributed denial-of-service (DDoS) attacks. Botnets may target an organization's infrastructure leading to depletion of the system's resources, ultimately resulting in a denial of service. A potential mitigation strategy involves distinguishing between requests from an attacker and those from legitimate users, using network equipment such as a Web Application Firewall (WAF) or a cloud-based security service. Elasticity is also an effective mitigation measure for managing load and minimizing the risk of overload or

DDoS attacks in cloud computing [231]. However, it is important to note that it also carries the risk of potential financial costs due to the auto-scaling mode.

Another cloud related threat that targets confidentiality is the Man-in-the-Middle Attack (MiTM), for which a possible countermeasure is the utilization of end-to-end-encryption such as digital certificates.

The aforementioned highlights the crucial nature of implementing digital transformation and the utilization of cloud infrastructures with a well-planned and structured approach that takes into consideration the aspects of cybersecurity. A successful model for digital transformation should be grounded in the best practices in developing IT capabilities and providing services, with a focus on governance and management, technology, and human capital [240].

To safeguard sensitive data at rest and in motion in a cloud environment, appropriate security and privacy mechanisms must be implemented. These mechanisms include cryptographic schemes, authentication and identity management, access control and accounting, as well as trust management, governance, policies, and regulations. In addition, data redundancy in the cloud must be carefully evaluated along with effective intrusion detection, alarms, and incident handling mechanisms [160].

According to ENISA perspective on cloud computing services [231], a comprehensive approach to cloud cybersecurity consists of three key steps: conducting a thorough risk assessment, implementing appropriate security measures, and establishing a reliable incident reporting system.

Another useful guideline to cloud service providers and customers is the Cloud Controls Matrix (CCM) [241] which is a security framework developed by the Cloud Security Alliance (CSA). CCM is organized into 17 domains, covering areas such as compliance, data security, and application security. Each domain contains a set of control objectives and associated controls that are intended to mitigate risks in that area. The controls are divided into the categories administrative, technical, and legal.

8 Contemporary Attack Types of Cyber Threats

The investigation has identified distinct cyber threats that have emerged in the contemporary cybersecurity landscape aiming to undermine or target critical infrastructure services from various angles, thereby increasing the risk of causing disruptions to them.

The selection of specific threats was made with careful consideration given to their impact, frequency of occurrence, available mitigation techniques, and potential management strategies. All aspects of the CIA triad were taken under consideration as well as the triad of organization, technology, and human resources.

Those attack types are the following:

- Human factor.
- Social engineering and phishing.
- Insider threats.
- Bring Your Own Device (BYOD).
- Supply chain attacks.
- Ransomware attacks.
- Denial of Service (DoS) attacks.

8.1 Human Factors as a Cybersecurity Threat

The implementation of automated systems in critical infrastructures has resulted in the delegation of day-to-day tasks to non-IT personnel. Despite the continuous introduction of new technological security systems to prevent unauthorized access, the human factor in cybersecurity is often neglected [242].

It is common for staff to lack a culture of cybersecurity and understanding of security issues, as revealed by a survey conducted in an energy sector organization [243], situation that results in the compromise of the organization's security, leading to unintentional insider threats. Moreover, organizations may employ or collaborate with individuals

who, due to various reasons, may not always have good intentions and may attempt to cause harm through diverse methods, such as the misuse of information systems.

8.1.1 Tactics and Implications of Social Engineering

The vulnerability caused by the human factor, compounded by the malicious actions of attackers and the lack of awareness of workers, creates a significant security gap that is often exploited through social engineering, an identified key cyber threat to critical infrastructures [244].

Social engineering techniques are those that involve manipulating the human factor and are designed to trick individuals into divulging confidential information or performing actions on behalf of others for illegal purposes [245], [244]. Attackers employ various tactics to deceive or manipulate users, such as enticing them to open emails or files, visit websites, or disclose sensitive information, ultimately granting unauthorized access to the organization's systems. Social engineering attacks have become increasingly prevalent and constitute a major contributing factor to cybersecurity incidents, as evidenced by sources such as [8], [188], and [246]. It is recognized that social engineering attacks pose a significant threat to the security of information, and this serves as an important driving force for organizations to implement measures to protect and secure this information [155].

The increasing reliance on technology has prompted attackers to employ techniques, such as social engineering, in which users are unwittingly used as Trojan horses for successful cyber attacks [247]. These attacks can result in theft of credentials, transfer of funds, extraction of confidential information, destruction of data, and disruption of critical information systems and infrastructure. It is distinctive from other types of cyber threats as it aims to target individuals rather than infrastructure [244].

The frequency, complexity, and sophistication of these attacks targeting critical infrastructures through social engineering are increasing. A notable example is the 2015 Ukrainian network attack, where a widespread blackout resulted from a malicious email [248]. Similarly, in 2014, a steel production plant in Germany was compromised through a personalized approach that led to the installation of malware, providing access to both IT and industrial systems [119], [249]. This attack is considered significant as it resulted in physical destruction, in addition to its impact on the cyber realm.

These attacks exhibit a common pattern, characterized by the initial deception of users, which serves as the primary step of the attack. Subsequently, the attacker gains access to the victim's computer system through a second attack. The attacker then utilizes the victim's computer to target the organization's infrastructure, bypassing any security measures in the wider perimeter and executing the final attack [119].

Irrespective of the methods employed, attackers appear to adhere to a particular four-phase model [250].

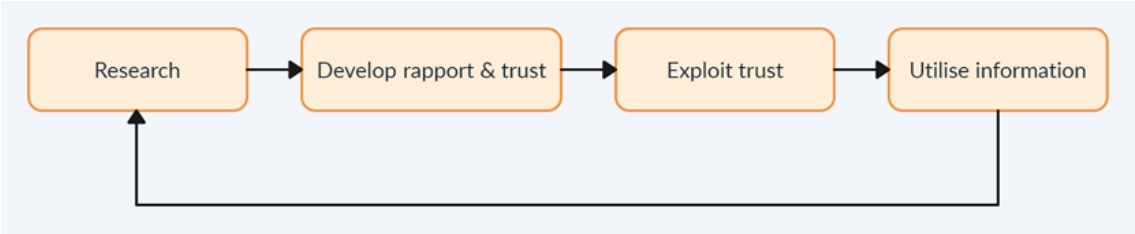

Image 17: Social engineering attack cycle [250]

In the initial phase, known as the reconnaissance phase, attackers collect essential information about their target, ranging from basic information like email addresses and full names to more specific data regarding the target's position and responsibilities within the organization. The attacker then gains the target's trust and proceeds with the deception in the following phase [250], [246]. In the final phase, the attacker leverages the acquired information for their intended purposes, such as installing malware or obtaining credentials.

Attackers have a multitude of tactics available to deceive their victims, enabling them to achieve their objectives. On an abstract level, they utilize tactics such as psychological manipulation, employees' inclination to obey authority, and the lack of knowledge and understanding of technology users in similar situations [242].

Social engineering encompasses both passive and active reconnaissance. Passive reconnaissance involves the collection of information through non-invasive methods, such as the examination of social media profiles, company websites, or public records identifying employees within large online communities. While social engineering often utilizes passive reconnaissance as a means of information gathering in preparation for an attack, it can also incorporate active reconnaissance, such as phishing emails or phone calls [250], [244].

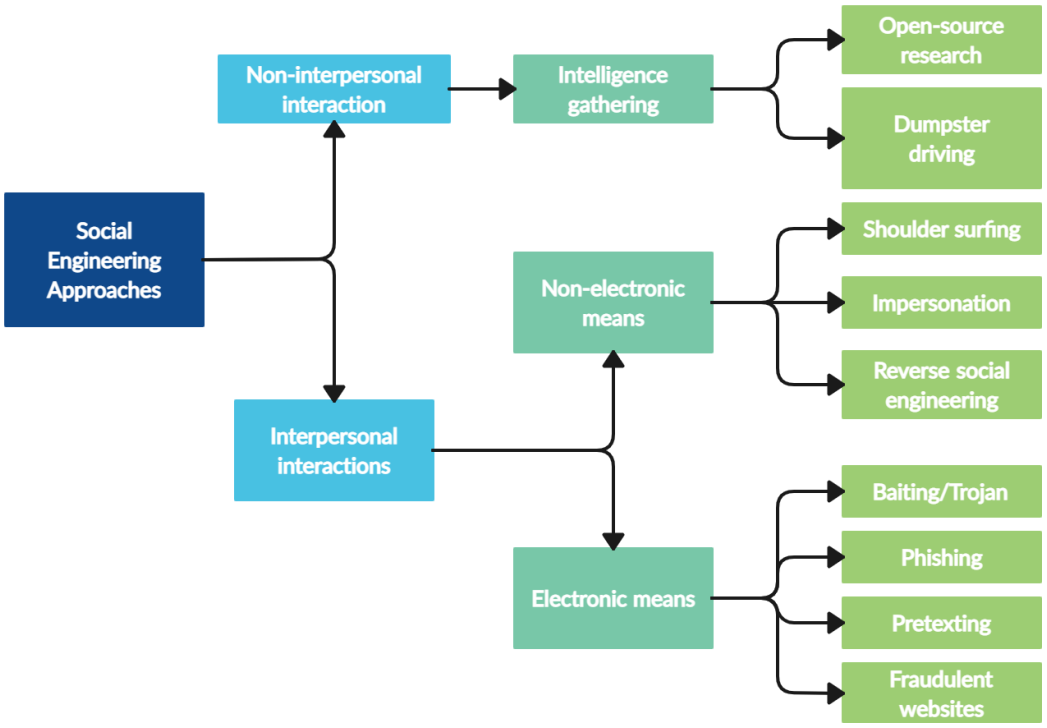

Image 18: Social engineering attack taxonomy [246]

In order to gain access to an organization or obtain ample information on an individual, successful attackers may utilize a combination of human and technical strategies [247].

Most social engineering attackers tend to avoid personal interactions with their targets, opting instead to exploit human behavior through electronic means, such as email, the internet, or other digital media, to deceive and manipulate the victim and accomplish their objectives [246]. Direct human engagement occurs when an attacker acquires personal information about a victim and establishes a relationship with them. Technical attacks are often executed through software programs, email attachments, pop-up windows, and websites, and are relatively straightforward in their approach. One particularly effective tactic is to prompt users to input their account usernames and passwords through pop-up windows [247].

In addition to psychological manipulation, attackers also have access to technological tools for large-scale information gathering, including OSINT and the use of bot or fake accounts to send virtual friend requests to targets in order to obtain more information [244], [155]. A study [244] conducted on employees of critical infrastructure organizations (such as those involved in energy, water, and gas) demonstrated that with only the

URL of the critical infrastructure website, attackers could initiate the collection of important information, providing them with essential tools to tailor phishing attacks.

The potential for online social media to function as a communication platform for the cyber community also creates opportunities for cyberwarfare and cybercrime heightening the risks to critical infrastructures, particularly with regards to information theft, cyber attacks, and cyber crime [251]. As highlighted in [155], the most successful cyber attacks target healthcare professionals through social engineering methods, taking advantage of personal data shared on social media platforms which is an indication of the evolving nature of the cyber attacks.

8.1.2 Phishing

Phishing, which is presented in the ENISA 2022 report as the most common threat vector [8], is a significant social engineering technique that pertains to cybersecurity in the relevant field [119], [73]. This technique involves a blend of social engineering tactics and techniques aimed at tricking victims into divulging sensitive information or inadvertently installing malware on an organization's systems.

Phishing typically involves the dissemination of deceptive messages that are designed to appear as if they originate from a genuine source (spoofing), and the most common method of delivery is through email, due to its cost-effectiveness and scalability for perpetrators [252]. Upon clicking on the links or opening the attachments, a surreptitious program infiltrates the laptops or devices without raising an alarm for the victims. This provides the hackers with the ability to manipulate or pilfer data from the compromised devices. Alternatively, the hackers may convince the victims to divulge their sensitive information, which can then be exploited to gain access to the victims' bank accounts or other online resources [253].

Within the realm of phishing, there exists a subcategory known as spear phishing that specifically targets employees deemed critical to infrastructure management. This form of phishing can serve as a preliminary stage in an Advanced Persistent Threat campaign aimed at gaining initial access to the infrastructure [119]. Commonly, attackers take advantage of user susceptibilities such as curiosity about interesting information, shopping, regular notifications, or general interest events (such as Covid or mail parcels) [254]. Also, as state before, attackers may leverage an individual's social network to more effectively target their attacks.

Image 19: Spear phishing email [255]

The issue of misleading emails is compounded by the fact that a significant portion of these emails bypass filters and reach their intended recipients. Additionally, individuals are more likely to open infected attachments if they believe the sender is trustworthy [254]. This problem is further intensified by the use of Internationalized Domain Names, which can be used to create domain names that visually resemble those of legitimate critical infrastructure websites (homographs). Similarly, the technique of typosquatting involves registering domains that are similar to legitimate domains, making it difficult to distinguish between the two URLs [256], [257]. A commonly utilized version of this attack [258] involves utilizing fragments of a genuine URL to construct a new domain name, as exemplified below.

Table 14: Typosquatted domains [258]

Original Domain	Typosqatted Domain	Homograph Domain
login.example.com	login-example.com	login.exạmple.com
		Actual interpretation by Google Chrome: login.xn--exmple-xc8b.com

It is evident that attackers could easily obtain user account credentials from a careless user. A study [259] illustrates that almost 20% of surveyed users were deceived into submitting their credentials on a spoofed website. Therefore, educating and training critical infrastructure personnel is deemed as the most effective approach to prevent social

engineering attacks [242]. It is imperative for organizations to encourage their employees to adopt cyber hygiene practices when accessing social media platforms, which serve as an ideal platform for attackers to gain insight into the lives of potential targets [155].

A key strategy for preventing phishing attacks is to prevent them at their early stages.

The successful prevention of phishing attacks is accomplished through the proper recognition of such attempts by the intended recipients, followed by appropriate handling and response to the identified cases. Education is of capital importance and can significantly help in preventing and mitigating the impact of phishing attacks [155]. There is a notable correlation between the resilience of users to phishing attacks and their prior exposure to phishing email training. It is also found that individuals where the most likely to be open to learning when they have just fallen victim to a phishing attack using concise and user-friendly training materials that demonstrate the identification of phishing attacks [259].

As a countermeasure to this threat, the following mitigation strategies are generally proposed [244]:

- Security awareness training can serve as a means to emphasize the significance of information monitoring and assist employees in comprehending the rationale behind fostering a culture of security. It is noteworthy that user training should be consistent and conducted through a well-structured program, while training for new employees joining the organization should not be overlooked.
- Revised security policies and practices aimed at promoting a culture of security.
- Implementation of network restrictions to minimize employee exposure to potential threats within the work environment.
- Performing a review of the company website to identify and remove any unnecessary public information that may be valuable to attackers, in order to reduce the risk of potential cyber threats.
- Conducting a social engineering penetration test can help strengthen the security culture within an organization.
- Use of an automated vulnerability scanner for social engineering that organizations can utilize to assess their susceptibility to possible social engineering attacks originating from open-source information sources.

According to reference [246], it is also recommended to periodically perform simulation tests as part of continuous cybersecurity posture assessment, in addition to training and awareness-raising efforts.

Integrating educational strategies into a comprehensive cybersecurity approach, primarily through training, is crucial. However, it is insufficient to solely raise awareness among employees. It is equally important to educate technical personnel in the proper use of security mechanisms and tools [188]. This training can be facilitated through computer-based methods, which offer affordability, flexibility, and easy accessibility, or in-person training with trainers to provide personalized interactivity and enhanced learning experiences [242].

In addition to organizational measures considering social engineering, more specific technical measures are proposed such as the implementation of DMZ, and the use of IDS, IPS, firewall, web filters and VPN [247].

Other anti-phishing measures are the use of advance security and password management, prevent users from visiting spoofed sites, MFA and email blocking [260].

The use of content-based filters can automatically distinguish between phishing and legitimate email messages. Numerous studies have focused on content-based email classification, utilizing advanced machine learning algorithms, decision trees, topic classification, and more [261].

In order to effectively secure email it is needed the adoption of MFA and SMTP security extensions like STARTTLS, SPF, DKIM, and DMARC. However, despite the availability of these technologies, the global adoption rates of these measures were only 35%, with DMARC being implemented by a mere 1.1% of email services [256].

Also, at the operator and national level is very important the adoption of adequate legal solutions and legislations [260].

8.2 Insider Threats

As previously stated in a preceding chapter the misuse of information assets or deliberate attacks carried out by individuals who have gained legitimate access to an organization's information systems or information is one of the categories of the internal threat. This type of threat is characterized by individuals who have the opportunities and capabilities to cause harm but lack hostile intent until their motivations change [69]. Disgruntled employees, those with psychological issues, and unauthorized intruders can

employ a broad spectrum of physical and operational threats to impair the uninterrupted operation of critical infrastructures [123].

It is a prevalent threat in modern times, as many employees possess the technical capabilities to unlawfully acquire data using internal systems [262]. As a consequence of the broad access granted to an organization's systems, the impact of malicious or negligent behavior by internal actors may be more consequential than that of external threat actors. The routine activities of employees can potentially pose a threat to sensitive data and critical systems, and the improper use of business applications can result in significant risks [118]. The operational continuity of critical infrastructures is susceptible to significant disruption due to threats posed to operators and engineers who fail to execute their responsibilities appropriately [123]. Therefore any user who fails to adhere to cyber security policies may constitute an internal threat [127].

Malicious attacks by individuals are typically motivated by personal reasons, such as revenge, career advancement, or financial gain, and may manifest in the form of digital violence, threatening or abusive behavior, espionage, sabotage, and theft of money or intellectual property [117]. A general classification based on the incentives of malicious insiders includes two categories, namely a) digital, and b) behavioral. The former refers to an insider who intends to gain unauthorized access to information for malicious purposes, whereas the latter aims to violate the system with the intention of disrupting or harming business operations [139]. The outcomes of both types of malicious insiders could potentially result in catastrophic consequences.

These attackers are often former or current employees, outsiders who have access to the organization's systems, or external vendors providing services to the organization having access to critical data [263], [118]. The dimensions typically considered for insider threats are [7]:

- Risk to infrastructure or society as a whole focusing on the potential impact.
- Type of access or role in the system as this can determine the extent of damage it can cause.
- Target, intent, or cause that examines the reasons behind the insider threat, such as financial gain, revenge, or sabotage.
- Level of technical skill which can influence the methods and tools they use to carry out the threat.

- Impact on infrastructure that evaluates the extent of damage or disruption to critical infrastructure.
- Type of attacker. This can be masquerader, malicious, or naïve and classifies the insider threat based on their level of malicious intent and their ability to hide their actions.

In contrast to external attackers, internal threat actors have distinct advantages, as they possess direct access to and extensive knowledge of an organization's systems. Such actors include employees with specialized knowledge, as well as those who are willing to facilitate unauthorized access to internal systems without subsequent involvement. It is estimated that cybercriminals are highly probable to engage in the recruitment of insiders within victim organizations to carry out exfiltration of data or deployment of malware [8]. In 2020, an instance of such activity occurred when individuals from Russia attempted to bribe Tesla employees with a substantial amount of money in exchange for installing malware designed to extract data from the company's network [9]. Another illustrative example of this occurred in 2013 when a systems administrator gained direct physical access to the primary data and server room space of a medical data management center, and subsequently intercepted sensitive personal data via a simple external hard drive [264].

Regrettably, organizations tend to place undue emphasis on perimeter security, thereby impeding the identification and mitigation of insider threats. The Snowden case is a notable example, wherein a system administrator for the US Intelligence Community intercepted and leaked approximately 1.7 million confidential documents to Russia [88].

To assess the potential insider threat to critical infrastructures, it is necessary to consider the following factors [7]:

- The scope and severity of potential impact.
- The variety of actions that could compromise the infrastructure.
- The characteristics and motives of the potential attackers.
- Strategies for responding to insider threats.

Every organization should endeavor to minimize the risks of insider threats by implementing consistent and robust security policies and controls for securing the organization's information systems and physical assets. However, it is not realistic to completely eliminate insider threats [243].

One approach to address this issue is to focus on detecting internal threats. Study [118] proposes a proactive approach to detecting internal threats involves conducting a risk assessment of users and creating their profile based on their daily activities and behavior. Additionally, analyzing the flow of information within the organization can identify sensitive information that requires heightened security measures.

Countermeasures proposed in [136] include: a) conducting continuous risk assessments to identify necessary security measures, threats, vulnerabilities, and risks; b) enhancing hardware and software security through necessary patches and contracts with respective suppliers; c) increasing the level of authentication in organizational systems (e.g. MFA); d) strengthening security procedures, policies, and awareness at all organizational levels; e) improving control over access to information; f) implementing detailed regulations for data retention; and g) implementing general preventive measures (e.g. access control), threat detection measures, and remediation measures (e.g. business recovery).

At [243] emphasis is placed on strengthening security awareness by conducting training programs for the entire workforce of the organization. These training programs should help employees recognize the risks associated with insider threats and their impact, as well as increase their motivation to protect their organization and themselves from such risks. Adequate and continuous training will also enable employees to upskill and reskill in cybersecurity, enhancing their ability to recognize and respond to cyber risks, and promoting adherence to the organization's policies and guidelines [243].

ENISA proposes various technical and organizational measures that cover the whole Identify, Protect, Detect, Respond and Recover cycle [169].

Table 15: Insider threats countermeasures [169].

Insider threats countermeasures	
Technical	**Organizational**
Threat hunting	Security policy
Network security	Personnel security
Endpoint security	Physical security
Data security	Security awareness
Penetration tests	Incident management
Vulnerability scanning	
Identity and access management	
Digital forensics	

Utilization of AI	

Examples of technical countermeasures related to internal threats may include DLP, IDS, IPS, HIPS, antivirus, DAM, firewall, SIEM.

8.3 Bring Your Own Device

The contemporary technology landscape is marked by a now common trend referred to as “Bring Your Own Device (BYOD)”. This trend has become particularly prevalent due to the COVID-19 pandemic, with many organizations having implemented extensive remote work practices and now transitioning to enduring and strategic teleworking structures [265].

This practice enables employees to use their personal devices to complete work tasks by connecting to the network and corporate resources. This provides the employees with the ability to access and complete work-related tasks from any location, increasing their comfort and productivity, while also providing cost savings to companies by reducing the need to purchase and maintain a large number of devices for their personnel [238], [266]. This approach is frequently employed in the implementation of remote work arrangements and this possibility is now provided by the greek law stipulated in legislation 4808/2021 [267].

Alongside the advantages, the adoption of BYOD policies presents significant challenges. The most prominent challenge faced by organizations implementing BYOD is the increased risk of security breaches [266].

As is readily understood the primary concern is related to the lack of control over personal devices and the potential privacy and confidentiality risks associated with the sensitive data stored on these devices. As it is easy to understand, storing data on employees' personal devices raises serious issues, as in case of loss or theft of the device it is very likely that this data will be compromised. A similar example is when repair or maintenance work is required on the devices where even if users believe that the data is protected by using a password this is not the case since with the use of specialized tools the data can be easily retrieved [268].

More precisely, the use of personal devices poses significant risks to the privacy and confidentiality of data, which can arise from lost or stolen devices, unauthorized access, and connection to unsecured networks. Additionally, the risk of malware is heightened

[238]. This issue is compounded by the fact that personal devices may not adhere to the same security standards as company-owned devices, rendering them susceptible to attacks and unable to mitigate data breaches. Furthermore, a common concern is the lack of awareness, guidance, and cybersecurity skills amongst users [269]. Another non-security related side effect is that the use of personal devices for work purposes may blur the lines between personal and professional use, leading to issues related to privacy and data protection for the individual. One must take into account that in the event of a lost device, employees may be hesitant to report it due to potential consequences, creating further issues in terms of non-compliance.

It is important for organizations to carefully consider the potential risks and implement appropriate security measures to mitigate them.

HDPA has published some exemplary security measures [270] such as segmentation of the personal device for professional purposes; enforcing robust user authentication mechanisms for remote access; establishing encryption measures for information transmission (e.g., VPN, TLS); implementing a procedure for device recovery in the event of loss or damage; requiring adherence to fundamental security measures, such as using strong passwords and up-to-date antivirus software; promoting user awareness of potential risks; seeking prior approval from the network administrator and/or employer before utilizing personal equipment; and articulating everyone's responsibilities and the necessary precautions in a binding charter.

Study [269] proposes a combination of counter measures according to the people, policy, technology model (PPT).

Table 16: BYOD solutions [269].

Dimensions	Solutions	Description
People	Security Culture	Employee Awareness and Training and skills improvement.
Policy	BYOD policy	Establishing procedures for regulatory compliance and determining the acceptable use of devices and data.
Technology	Strong authentication passwords	Multifactor authentication, strong passwords.
	Mobile Device Management (MDM)	Central management of devices within the organization.
	Containerization	Logical separation of organizational and personal data.
	Virtual Desktop Infrastructure	Eliminating the necessity to store data on personal devices of employees.

	Identity and Access Management	Ensure appropriate access using access control mechanisms.
	Endpoint Security Tools	Antivirus, antimalware, antispyware, or antiphishing tools.

ENISA at its report [271] identifies similar mitigation strategies, policies and controls for the risks identified in this area, while the guidelines provided by CISA for executive leaders, IT professionals, and teleworkers follow similar fundamental principles [265].

8.4 Supply Chain Attacks

The supply chain is the foundation of modern economies and plays a crucial role in enabling the flow of goods, services, and information between producers, distributors, retailers, and ultimately consumers. It extends beyond the mere movement of physical goods and materials and it encompasses the exchange of critical information, delivery of essential services, and the transfer of financial resources throughout the entire supply network characterized by its interconnectedness among all its dimensions [239].

The growing complexity and interdependence of global supply chains has resulted in the increase of the risk of supply chain cyber threats in recent years [114], [272]. It is practically infeasible to guarantee the product supply chain process due to the widespread production of software and hardware products globally [124]. As businesses and governments rely more on a network of suppliers and vendors to obtain necessary goods and services, ensuring the security of each link in the supply chain becomes increasingly challenging. These links can include a variety of components, such as data, software, hardware, networks, legal entities, and infrastructures [273]. Supply chain attacks can have a detrimental impact on key components and directly target critical technologies and systems that are vital for organizational operations, such as the IT and OT stacks [274]. This trend is underscored by a substantial increase in the proportion of intrusions attributed to third-party incidents, which rose from less than 1% in 2020 to 17% in 2021 [8].

The intricacy of the supply chain and the participation of several entities can pose difficulties in the monitoring and control of every aspect of the process. This is attributed to the fact that vulnerabilities can be introduced at any phase of the product life cycle, namely design, development, production, distribution, acquisition and deployment, maintenance and disposal [275]. The situation can become even more complex if one

considers the potential for conflicting national interests, especially when companies that are based in these countries simultaneously serve as both suppliers and customers within the supply chain. As previously stated, state actors play a significant role and must be considered within the cybersecurity ecosystem, something that raises concerns particularly given China's significant control over the global supply chain and the absence of reliable security assurances from the country [273]. It is evident that periods of geopolitical tensions and conflicts, such as the ongoing conflict between Russia and Ukraine, serve to highlight the vulnerability of supply chains to cyber attacks. An example of the criticality of supply chain security is Operation Warp Speed (OWS), in which the CISA focused on safeguarding the supply chain for the secure manufacture and distribution of vaccines to the general public [4].

In recent times, there have been multiple documented incidents of supply chain attacks on critical infrastructures, which have resulted in particularly severe consequences. At 2017 NotPetya malware attack, which started in Ukraine was evidently targeted towards infecting its critical national infrastructures, including its energy companies, power grid, transport sector, and banks [111]. The attack was launched through a software update from a Ukrainian accounting software provider and affected many organizations that used that software including international shipping, financial services, and healthcare [276]. The 2018 attack on the British Airways website and mobile app also demonstrated the risks of supply chain attacks, as hackers were able to insert malicious code into the company's third-party payment processing system, which allowed them to steal customers' payment card information [273]. The devastating SolarWinds cyber attack involved hackers infecting SolarWinds' Orion software and using a routine security update in March 2020 to install malicious software in the company's clients' networks. The attack evaded clients' cyber-security defenses by hiding within that security update and affected approximately 18,000 of SolarWinds' clients. A notable observation was that 30% of the victims identified in the hack had no direct affiliation with SolarWinds, the company whose software was used as a vector for the attack [111].

Based on the findings of ENISA at [114], it has been determined that malware has become the most common method of attack, and APT groups have been identified as the primary culprits. Furthermore, the danger of malicious external suppliers has also been recognized, while code has been identified as a key attack vector for supply chain attacks, as it is utilized to further compromise the targeted customers.

A supply chain attack can be considered an indirect attack, as its attack surface encompasses various components, including suppliers, customers, and their respective assets, and involves a two-step process. The initial step involves targeting a supplier to compromise an asset, followed by a second step targeting the final customer or another supplier [114]. Therefore, it is necessary for an organization to consider the possibility of threats originating from both outside and within the conventional limits of a corporate network [277]. The trust relationships that Cloud Service Providers (CSPs), Managed Services Providers (MSPs), and IT services organizations establish with their customers also makes them a common vector for the initiation of cyber attacks [114].

Attackers may target software solution providers and hardware products by exploiting backdoors and inserting malware [273], using combination of techniques such hijacking updates (e.g. NotPetya case), undermining code signing, and compromising open-source code [278]. Interconnected IT systems create an extended attack surface with each system possessing unique vulnerabilities, resulting in the entire ecosystem being vulnerable to any potential point of failure [239]. It is predicted by ENISA [279] that the increased demand for swift software product delivery, code reuse, and the adoption of open-source solutions will persist, leading to the elevation of this threat to become the primary cybersecurity concern by 2030.

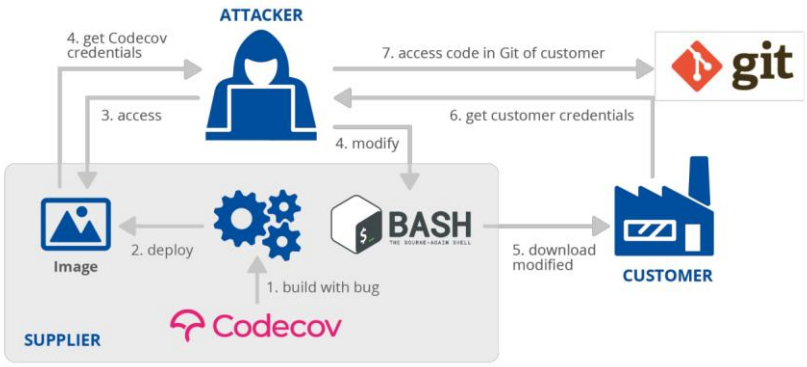

Image 20: Codecov supply chain attack [114]

Any software or hardware that necessitates third-party updates to guarantee reliable operation presents a potential source of attack [244]. Organizations and vendors often perceive software security measures as merely a feature rather than an essential necessity. The intangible nature of software as well as distribution, change management, and interdependencies with other software can all contribute to potential threats [239].

Organizations employ various types of software, including both proprietary and open-source systems. Proprietary software may pose security risks, as the code is not accessible for review. Conversely, open-source software and reused software are subject to visibility by multiple parties, thereby increasing the potential for security breaches. Additionally, open-source software repositories are also vulnerable to attacks [257]. A noticeable example that shows the scale of this issue occurred in 2018, when the official PHP Git repository [280] was compromised by attackers who added a malicious backdoor to the source code. The attackers impersonated the PHP project founder Rasmus Lerdorf and Nikita Popov. The backdoor was designed to allow remote code execution on servers running PHP. It was discovered and removed within hours, but the incident highlighted the risk of supply chain attacks even in widely used and trusted open source software. Another example of a similar nature was demonstrated in dissertation [281], where typosquatting in programming packages and libraries resulted in the execution of arbitrary code on thousands of servers, including military ones.

For software or hardware products that are readily available in the commercial market (Commercial Off-The-Shelf - COTS), it is recommended to follow a well-thought-out process that includes the identification of assets and security requirements. Only after performing a tradeoff analysis, final product specifications should be developed [257]. The utilization of reverse engineering can be considered a possible approach to mitigate the impact of cyber attacks, as it can uncover any hidden malicious code that could otherwise remain undetected [282].

Another major concern regarding supply chain is counterfeits. Critical infrastructures is highly vulnerable against this threat. One only has to consider the impact of the use of a counterfeit component in SCADA water quality control infrastructures can have severe consequences, whether as a result of a malicious attack or due to the absence of appropriate procedures and technical measures to control the final product. A proposed solution in [239] to counteract counterfeiting is the use of Physical Unclonable Functions (PUFs). PUFs are hardware-based digital signatures that serve as unique identifiers for each device and are almost immune to forgery. Another potential solution is the use of blockchain technology, which provides traceability, transparency, and a tamper-proof record of transactions due to its decentralized and distributed nature.

Achieving trust in a supply chain is a fundamental but a complex problem that is difficult to quantify and attain given the numerous partners and products.

Given the characteristics of a supply chain and the significant number of ICT components involved, a suitable and diverse multi-level assessment framework is necessary to effectively manage an organization's cybersecurity posture instilling trust and confidence in commercial relationships to all partners and the broader society [162].

The study [277] suggests that assuming there should be no trust in the supply chain and implementing continuous monitoring may be a solution to this complex problem of trust. This approach requires a detailed inventory of all assets (Software Bill of Materials - SBOM) and adoption of principles outlined in related frameworks such as NIST standard 800-207, Microsoft's Zero Trust Guidance Center, and the Zero Trust Maturity Model. These principles include continuous monitoring of all assets, strengthening authentication, continuous information gathering, and securing processes through automation techniques. A gap analysis will reveal the necessary measures to address any discrepancies.

Supply chain risk management (SCCRM) is a crucial factor in reducing vulnerabilities and preventing service and product disruptions. Typically, the process involves identifying, assessing, controlling, and monitoring risks. The use of external data sources can be beneficial in identifying and assessing these risks. A framework for SCCRM, presented in [272], utilizes data from a threat intelligence system in conjunction with attack vectors, company and supplier security postures, and environments. This framework generates forecasts of emerging risks and supplier rankings, which can be useful in negotiating Service Level Agreements (SLAs).

The study presented in [111] advocating for the reinforcement of an international strategy that incorporates both retaliatory and de-escalatory measures to deter potential aggressors [273] proposes a similar approach in which it is crucial to address the risk at higher levels by strengthening international legislation to enforce regulatory and deterrence mechanisms against supply chain attacks. Moreover, investment in collaboration between industry players and manufacturers to promote security standards and monitoring of associated risk is deemed important. In order to address the potential security risks associated with third-party vendors, it is necessary to establish and enforce rigorous procedures while the use of modern technologies like Cloud Computing, Big Data Analytics, Supply Chain Digitalization, and Blockchain can play a crucial role in countering the threats [239].

The study presented in [283] proposes the implementation of a Zero Trust framework to mitigate the threat of supply chain attacks, primarily by minimizing the organization's exposure in case of a breach. The study also emphasizes the importance of reducing the attack surface by eliminating unnecessary assets, improving process security, hardening assets, continuously monitoring the perimeter, and enhancing incident response capabilities. Furthermore, any software modifications should be meticulously scrutinized to prevent changes that could result in malfunction or inadequate function. These proposals are in alignment with NIST's recommendations for cyber posture across internal, interagency, international, and industry sectors [274].

In conclusion, ENISA [114] provides high-level recommendations for organizations to evaluate the cybersecurity maturity of their suppliers and assess the level of risk associated with the customer-supplier relationship. It is suggested that suppliers should implement measures to secure the development of products and services using best practices and through vulnerability management.

8.5 Ransomware

As already previously discussed in this text, there has been a surge in ransomware attacks on critical infrastructures in recent times. Instances include the WannaCry [154] attack on the healthcare sector in the UK, the NotPetya [111] attack on Ukraine's energy companies, electricity grid, transport sector, and banks, as well as an attack on Greek postal services [31], among others. In fact, there has been an increase in the targeting of ICS by ransomware, likely due to the critical nature of the operations involved in these industries. One sector that is particularly vulnerable to these types of cyber threats is the energy sector [284].

Based on these cases, it is evident that ransomware has become a significantly destructive form of cyber attack. In fact, over the past ten years, has inflicted damage on organizations of all sizes across the globe [285], [8]. The impact of this kind of malware is so significant that the US Department of Homeland Security considers it to be an equal national security threat to terrorism [286]. Critical infrastructures are not exempt from being targeted by ransomware, on the contrary, they are persistently under the threat of it. This situation can be attributed to multiple factors, each to varying degrees.

The outbreak of COVID-19 pandemic has significantly increased the risk of ransomware attacks due to the sudden shift to remote work and reliance on digital communica-

tion, leaving them vulnerable to cyber threats something that resulted in a dramatic increase in the number of attacks [8]. The escalation of the war in Ukraine has also heightened the risk of cyber-attacks, and particularly ransomware, notably on high-value targets such as critical infrastructures [287] in which a minor disruption to essential services can lead to a considerable impact.

The transformation of the cybercrime model into an as-a-service model has also facilitated and accelerated the use and the spread of ransomware. As a result, the development and distribution of this kind of malware can now be outsourced, usually using the pay-per-purchase business model [288], resulting in ransomware attacks to become more accessible to individuals, including low level threat actors (e.g. script kiddies) with basic technical skills.

Another factor that significantly impacted the field of ransomware is the use of cryptocurrencies. One possible explanation for this resides to the anonymity provided by this kind of transactions, as these payments are not traceable allowing attackers to conceal their identities and avoid detection. It is worth noting that some attackers have even created QR codes with Bitcoin wallet addresses to make easier the ransom payments [289]. The demanded ransom is influenced generally by two factors: the value of the affected data and the scope of the victims, which is related to how easily the ransomware spreads through the targeted area [284].

As illustrated by the etymology of the term itself, "ransomware," that derived from the fusion of "ransom" and "malware," it represents a form of malware which demands a payment in exchange for a stolen functionality. In fact, ransomware can be considered a type of digital blackmail that exploits the vulnerabilities of the victim's assets in the new digital environment [290]. The 2022 edition of ENISA's Threat Landscape report [285] on ransomware attacks provided a more formal definition of ransomware as an attack in which malicious actors seize control of a target's assets and demand payment in exchange for restoring access to those assets.

Ransomware threat actors have adopted a tactic known as "triple extortion," [287] which involves threatening victims in multiple ways after disrupting their services. This tactic involves the threat of publicly releasing sensitive information that has been stolen, disrupting the victim's internet access, and/or informing the victim's partners, shareholders, or suppliers about the incident. This tactics seems to be proven fruitful as a study [291] suggests that a very large percentage of the organizations that fell victim to

ransomware attacks entered into negotiations with the attackers and potentially even paid the demanded ransom. It is important to note that compliance with attackers' demands and payment of ransom does not offer any assurance that they will fulfill their promises to restore data or services to their prior state or refrain from disclosing the attack to the public. According to unofficial reports [292], it appears that even the Colonial Pipeline company may have agreed to pay a substantial ransom amount.

Moving on to the analysis of technical characteristics ransomware is a specific form of malware [293] that is designed to restrict access to informational assets typically is installed using a trojan or worm that is distributed typically through phishing or by visiting a compromised website. Ransomware has the ability to carry out four main actions compromising assets, referred to as LEDS, which stand for Lock, Encrypt, Delete, and Steal [285]. The prevalent type of ransomware is the one that encrypts data on the victim's device and withholds it until the ransom is paid. On the other hand, locker ransomware infects the system and restricts user access to the data without affecting the stored files [284]. For example, WannaCry [154] case was a typical encrypt attack targeting patient records and disrupting hospital operations.

The typical phases of a ransomware attack involve an engagement between the attacker and the victim [285], [290].

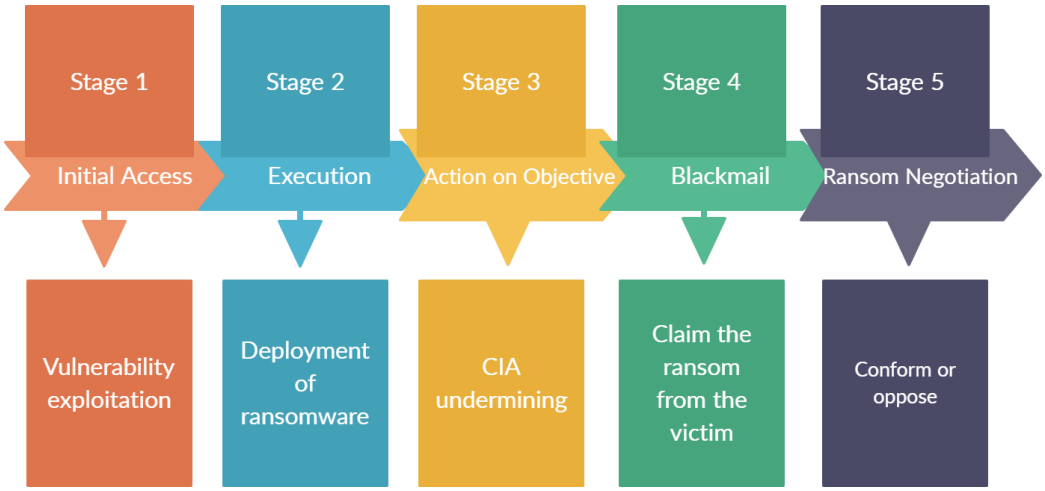

Image 21: Ransomware attack life cycle [285], [290]

- Initial Access: Ransomware utilizes similar attack vectors as other forms of cyberattacks, such as exploiting software vulnerabilities, gaining access through stolen credentials, phishing, etc.

- Execution: Following initial access, threat actors may spend a considerable amount of time investigating the target and utilizing various attack techniques to discover additional assets that can be exploited.
- Action on objectives: After deployment, the ransomware executes a series of actions to compromise the CIA properties of the targeted assets.
- Blackmail: In addition to demanding a ransom in exchange for the return of the compromised assets, the threat actor may take other actions to pressure the victim, such as publicly communicating about the attack or leaking sensitive data.
- Ransom negotiation: At this point, the victim can either comply with the attacker's demands or refuse. However, there is no guarantee that paying the ransom will result in the return of the stolen data or services.

In ICS environments, the steps are similar. The scenario typically involves infecting a PLC on the corporate network level, which in order to maximize profit and impact then it spreads to more PLCs and harvests credentials and access control lists/resources [284]. As previously mentioned, critical infrastructures prioritize availability over the other dimensions of the CIA triad as ICS impacts essential functions that can affect a large population and may jeopardize human life with potential consequences on human life and safety [284]. For this reason ransomware infections are a significant challenge for industrial network administrators, because of their destructive consequences as ransomware often employs scatter mechanisms that flood automation networks, leading to service disruptions and affecting availability. This can lead to block access to supervisory stations, destroy supervisory controls, encrypt historical databases and block access to utility systems [294]. IoT devices are equally or even more vulnerable to ransomware attacks than ICS because of their inherent limitations, which prevent them from implementing basic security measures [295], [296].

The effects of ransomware on traditional IT assets should not be overlooked. Various devices such as servers, databases, desktops, laptops, and mobile devices are all susceptible to such attacks. For example, in Greece, there are utility companies that are considered critical infrastructures and have a customer data stored in a database, which means that a ransomware attack on this database could lead to compliance and regulatory issues and substantial financial losses.

To manage and combat ransomware attacks organizations can choose various strategies or a combination of them, including proactive, reactive, and preventive approaches.

Proactive prevention involves stopping the malware's execution, while a proactive framework consists of policies, procedures, control and management, exposure analysis and reporting, as well as awareness and education. Reactive prevention aims to mitigate the impact of the attack by restoring extorted files from backup [284].

Generally, implementing policies that address ransom payment strategies, such as setting a "cybersecurity poverty line" to ensure a minimum level of security measures is maintained, is recommended over a "plan to pay" approach and can help reduce the overall threat posed by ransomware [286].

It has been discovered that certain key elements have emerged during the investigation of ransomware incidents. One very significant finding was that ransomware was mostly delivered through web and email channels using social engineering, phishing [297], [284], [298], and stolen RDP credentials [287]. To prevent this, spam filters can be set up, and attachments can be inspected in a sandbox or quarantined. Threat intelligence can also be proven useful, as well as exploit execution prevention modules. This involves also the continuous monitoring of deep, and dark web for newly leaked or stolen data while services that encompasses PwnedLists like “haveibeenpwned” are quite useful for the detection any compromised account.

To block ransomware during encryption, administrators should define trust boundaries to block access to shared folders, and HIPS can be deployed. Furthermore, detecting traffic to the Tor network through traffic monitoring is crucial as it can indicate a highly suspicious activity [297]. The supply chain also plays a role, as ransomware can infiltrate through third-party vendors and managed service providers so it is essential to conduct thorough screening of suppliers and partners to minimize the risk of such attacks [298], [287].

At the case of enterprise machines and endpoints such as servers, cybercriminals tend to develop more complex forms of ransomware rather than relying on malicious URLs or spam emails [284].

As for IIoT systems the entry point is usually the edge gateway due to its critical functionality as the bridge between the physical and cyber worlds, and its location which makes it a critical point of failure. Being the entry point for any threat vector, it is often the first line of defense and the first to be attacked because by compromising it attackers can gain control over the entire IIoT system. Countermeasures that can be taken specifically in IIoT sectors include deploying a next-generation firewall, implementing net-

work segmentation and monitoring, establishing backup plans, enforcing physical security policies, and providing cybersecurity training [296].

Finally, at its antiransomware guide [298], CISA proposes various countermeasures such as implementing MFA for all services to the extent possible, applying the principle of least privilege to all systems and services, leveraging best practices and enabling security settings, creating a comprehensive network diagram, using logical or physical means of network segmentation, adopting an asset management approach, and securing domain controllers.

8.6 Denial of Service

Denial of Service (DoS) attacks are not something new in the realm of cybersecurity, as they have existed for many years. Nevertheless, they persist as one of the most common risks in cyberspace [299], critical infrastructures, and modern way of life in general [8]. Simply considering the aftermath of an attack on a telecommunication provider or a power grid suffices to highlight its severity. An instance like this could have apocalyptic proportions, considering that nuclear power plants are also classified as critical infrastructures. The Stuxnet cyber-attack on the Iranian nuclear power plant, even if not a typical availability attack, serves as a real-world example of the previous scenario. While the attack did not result in any environmental damage, it is easy to imagine the incalculable environmental disaster in the event of radioactive release.

Similar to the situation with ransomware, the rise in attacks of this nature can be attributed in part to the influence of geopolitical factors and the COVID-19 pandemic. Notably, in addition to the rise in the frequency of attacks during this period, there has been an increase in their complexity and sophistication [8].

In brief, DoS attacks are deliberate efforts by unauthorized users to disrupt or prevent access to resources for legitimate users [300], [293] by specifically targeting a particular source in order to deplete the resources of the targeted system [301]. For example, email services could experience delays or failures, websites may become inaccessible and IoT devices may be negatively impacted.

To effectively defend against DoS attacks, it is crucial to have a comprehensive understanding of the nature and mechanics of such attacks. While there are numerous types of DoS attacks, the most prevalent ones can be classified according where they focus.

- Network resource overload refers to the depletion of all accessible network hardware, software, or bandwidth of the target.
- Protocol resource overload targets the available session or connection resources.
- Application resource overload focuses on the consumption of available compute or storage resources [301].

According to [302] DoS attacks can affect all Open Systems Interconnection (OSI) layers.

Table 17: DoS attacks examples per OSI layer [302].

OSI layer	Example of DoS layer
7 Application	Denical of access to database.
6 Presentation	Data injection so that information becomes useless.
5 Session	Use session identifier of another user.
4 Transport	SYN flood attacks
3 Network	Teardrop attacks depleting target resources to reassemble the packets
2 Link (data)	ARP spoofing to pose as a gateway causing degradation at message delivery
1 Physical	Unplubbing of the network cable

A common generally acceptable categorization of the DoS attacks is the following:

Distributed Denial-of-service (DDoS): This attack happens upon overloading traffic originates from multiple attacking machines operating in unison. DDoS attackers frequently exploit a botnet to execute their attacks [301], [293], [302] and this form of attack is becoming more focused on mobile networks and IoT devices, and are particularly cost-effective against vulnerable sites. Nowadays is commonly used by hacktivists as a primary means of attack [303].

DDoS attacks can be based on web-based attacks that are frequently disseminated through web applications, and employ the cloud as a primary attack vector. Evidence shows that it gets progressively more advanced as attackers use more techniques such as DDoS-for-Hire services and botnets [8]. The first approach involves employing individuals to carry out DDoS attacks on behalf of the hiring party. The second type involves the utilization of malware-infected devices, which are remotely controlled and coordinated by a threat actor [293], [301].

The Mirai botnet was an example DDoS attack that occurred in 2016 and has been responsible for multiple large-scale DDoS attacks since then. This botnet was able to

propagate and infect IoT devices by exploiting weak security measures, such as default or easily guessable usernames and passwords, through brute force attacks [189], [304]. As a result, the Mirai botnet was able to compromise IoT devices and turn them into bots that performed DDoS attacks. This attack highlights the significant risks posed by IoT devices to the Internet and it is considered a turning point in the history of IoT security, exposing the vulnerabilities and weaknesses in IoT devices and highlighting the urgent need for better security measures to be implemented [304]. Given the security vulnerabilities inherent in IoT devices and their vast numbers, it is not difficult to imagine that even a small fraction of contaminated devices could contribute to the creation of a botnet capable of generating massive DDoS attacks [305].

It is easy to envision the significant impact that any such scenario involving smart meters could have on critical infrastructures [306]. As reported in a study [307], two simulation scenarios were performed to assess the impact of Denial of Service (DoS) attacks on Advanced Metering Infrastructure (AMI) and smart meters, confirming the potential threat to critical infrastructures in which the communication between the control center and 89.7% of the total Smart Meters was successfully compromised.

Similar problems suggests the study [306] where it states that an attacker could carry out a DoS attack on a Power Generation System, resulting in a relay malfunction or even unauthorized modification of relay settings, leading to inadvertent faults. At a scenario like the successful delay in message transmission could cause severe damage to power equipment.

Similar results can be seen in the telecommunication system in which the core of internet connectivity can be endangered at national level due to targeting and disabling a DNS server, something that can result unavailability to domain name resolving [308]. As it can easily someone imagine the interconnectedness of critical infrastructures can result in cascading effects to other sectors as well.

According to [302] there are four generic categories of DoS. Those are a) depletion of resources, b) exploitation of programming errors, c) attack on routing and DNS, and d) disruption of network access through flooding traffic that consumes available bandwidth. Nevertheless, other conventional names there can be used for DoS attacks:

- Smurf attack is a network layer DoS attack [309], [310] that involves flooding a target node or group of nodes with a large volume of ICMP packets containing a spoofed source IP address. These packets are sent to the victim using an IP

broadcast address which the victim nodes in response to the ICMP requests, generate other ICMP responses, resulting in a large amount of traffic in the targeted network.

- Attacks on routing and DNS such as TCP flooding, also known as ping flooding, is a form of DoS attack that targets the transport layer in which the attacker sends an enormous amount of ping requests with the intention of overwhelming the targeted system [309], [310], [293].
- A crash attack is a form of cyber attack that is designed to make a system or network unavailable by sending deliberately malformed or specifically engineered data packets to a targeted system or network, resulting in it becoming unresponsive or crashing [293], [302].

The incorporation of wireless technologies in both IT and the OT environments exacerbates the security risks. As the transmission medium is shared, attackers can disrupt its availability or misuse it for malicious purposes. Here the risk lies in the wireless availability which implies that the authorized users are indeed capable of accessing a wireless network anytime and anywhere upon request. An illustration of the potential risks posed by wireless technologies is the fact that an unauthorized node could launch a denial-of-service (DoS) attack at the physical layer. This could be achieved by generating interferences with the goal of disrupting the desired communications between legitimate users, also known as a jamming attack. Such an attack can interfere with either the transmission or the reception (or both) of legitimate wireless communications, creating significant disruption to the network [309].

The management and security of a large, diverse network of devices like IoT present significant challenges. As proposed in [305], Software-Defined Networking (SDN) can aid in monitoring network flows and providing centralized control of network devices. This approach demonstrates a detect-and-mitigate strategy for DDoS attacks originating from IoT devices.

The utilization of a cloud environment also presents significant challenges for the services provided by critical infrastructures. In order to combat DDoS attacks within a cloud environment or any other computing architecture, it is crucial to distinguish between legitimate and illegitimate packets. Security firewalls installed within the network of a cloud computing environment are insufficient in blocking such packets, as are in-

trusion prevention systems (IPS), while the scalability of the cloud itself, however, can offer a partial solution [229].

To defend against DDoS attacks at the application layer, measures such as implementing CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) and AYAHs (Are You A Human) can be utilized to restrict automated requests from accessing the system. DDoS attacks can be detected through monitoring, tracking, and analyzing requests. Additionally, resource monitoring can also be an effective strategy to detect DDoS attacks at an early stage, as recommended by [308]. The same study proposes proper validation and sanitization of data should be implemented to filter out any malformed packets or data for many subtypes of this attack.

A recommended solution [309] to defend against the Smurf attack is to utilize firewalls that can reject malicious packets arriving from forged source IP addresses.

In order to counteract the effects of jamming attacks at OT devices of critical infrastructures, current wireless systems commonly employ spread spectrum techniques such as direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS), or employ methods to detect the presence of jammers or conceal the activity of authorized users to prevent jammers from knowing when to interfere with legitimate wireless communications [309].

CISA’s guidelines [301] recommend several measures to prevent and mitigate the impact of DDoS attacks. These include conducting a risk assessment and asset evaluation to identify vulnerabilities and potential attack vectors. Network bottlenecks should also be identified and addressed, such as by implementing load balancing and colocation designs to distribute traffic and prevent single points of failure. A dedicated DDoS protection service can also be used to monitor and filter traffic, while High-Availability designs can ensure that critical services remain available even during an attack. In addition, a response plan and business continuity plan should be developed to minimize the impact of an attack and quickly recover from any disruptions.

9 The Significance of a Cyber-security Strategy

This chapter intends to provide concise recommendations for the cybersecurity strategy that ought to be adopted by critical infrastructures. Given the multi-faceted nature of this undertaking, the viewpoints of other scholars will be referred to, and subsequently, various components discussed in previous chapters will be incorporated.

Generally, the advancement of cybersecurity demands an initial step of utilizing existing knowledge to enhance cybersecurity, followed by the subsequent step of acquiring new knowledge in the realm of cybersecurity [22]. The implementation of globally recognized security standards and certification schemes can facilitate the achievement of this goal [198]. Cybersecurity challenges require [148] greater integration and perhaps partnerships of the private and public sectors by standardization, licensing, and auditing, as well as local and national governments, rather than relying on a centralized top-down approach. Coordinated efforts at national, regional, and international levels are necessary for enhancing cybersecurity and protecting critical infrastructures [161]. A noteworthy deficiency identified is the tendency for many of framework approaches to prioritize technical risk management over other aspects such as social and human dimensions of cybersecurity. All these dimensions are mutually reliant and equally indispensable for achieving optimal project outcomes [311] and understanding of how attackers operate important to develop an effective plan of action against cyber threats.

To ensure the efficient and reliable operation of critical infrastructures, it is essential to meet certain prerequisites, including the use of robust and dependable ICT systems. In order for this objective to be achieved, it is imperative that the technology employed possesses specific features such as performability, interoperability, scalability, extensibility, availability, reliability, resilience, safety criticality, autonomy, and self-healing, usability, trust, and collaboration between disparate entities to confront aberrant and menacing situations while sustaining fault tolerance and security [160].

Critical infrastructures must prioritize [312] adopting a heightened state of awareness and engaging in proactive threat hunting to enhance their resilience and minimize the risk of compromise or significant business degradation. To achieve this they should:

- Be prepared minimizing personnel security gaps in IT/OT and following a cybersecurity plan.
- Enhance their cybersecurity posture following best practices.
- Increase organizational vigilance.

A "protection pyramid" for managing cybersecurity of critical infrastructures is proposed in the study [160].

- Governance and security management using organizational and operational subcontrols.
- Secure network architectures.
- Self-healing in order to achieve fault tolerance.
- Model and simulation in order to analyze and enhance resilience.
- Wide-area situational awareness to prevent, detect and respond in time.
- Forensics and learning to analyze incidents and develop countermeasures.
- Promote overall trust management and privacy.

It is worth noting the existence of the Self-Assessment Tool for Cybersecurity Critical Infrastructure Operators [313] created by the National Cybersecurity Authority, which the reader is encouraged to review.

In the context of cyber security countermeasures can be categorized into two types: proactive which is the first line of defence and reactive measures which serve as an additional defense line in the event of failure. The first includes security awareness, security-by-design processes, patch management processes, threat intelligence, penetration testing, and other tools such as firewalls and intrusion prevention systems. The latter include attacks/anomalies detection and reaction systems, security auditing, digital forensics, and incident response [172]. When implementing those measures it is crucial to develop techniques and protocols for fast identification, isolation, and remediation of faults [118].

A bit more technically, critical infrastructures operators should put in place measures to detect, delay, and respond to physical and cyberattacks such as establishing security of-

ficials; creating barriers and access control measures; implementing intrusion detection capabilities; and developing incident reporting, response and investigation programs for both physical and cyberattacks, among other measures [4].

A compelling framework for enhancing cybersecurity in critical infrastructures what is worth noting is proposed at [184]. This framework, referred to as the Lifecycle of Cybersecurity, comprises four distinct phases.

- The Prediction phase involves intelligence gathering (cyber threat intelligence) and risk management.
- The Protection phase is concerned with implementing measures to achieve security objectives based on the risk assessment.
- The Detection phase entails the implementation of monitoring mechanisms, intrusion detection, and identification of anomalous or malicious behavior in systems using potential threat detection tools.
- The Response phase involves the implementation of incident notification and management procedures, along with appropriate mitigation, recovery, and business continuity plans.

Critical infrastructure protection can be categorized into two major domains: cybersecurity measures and cyber threat intelligence.

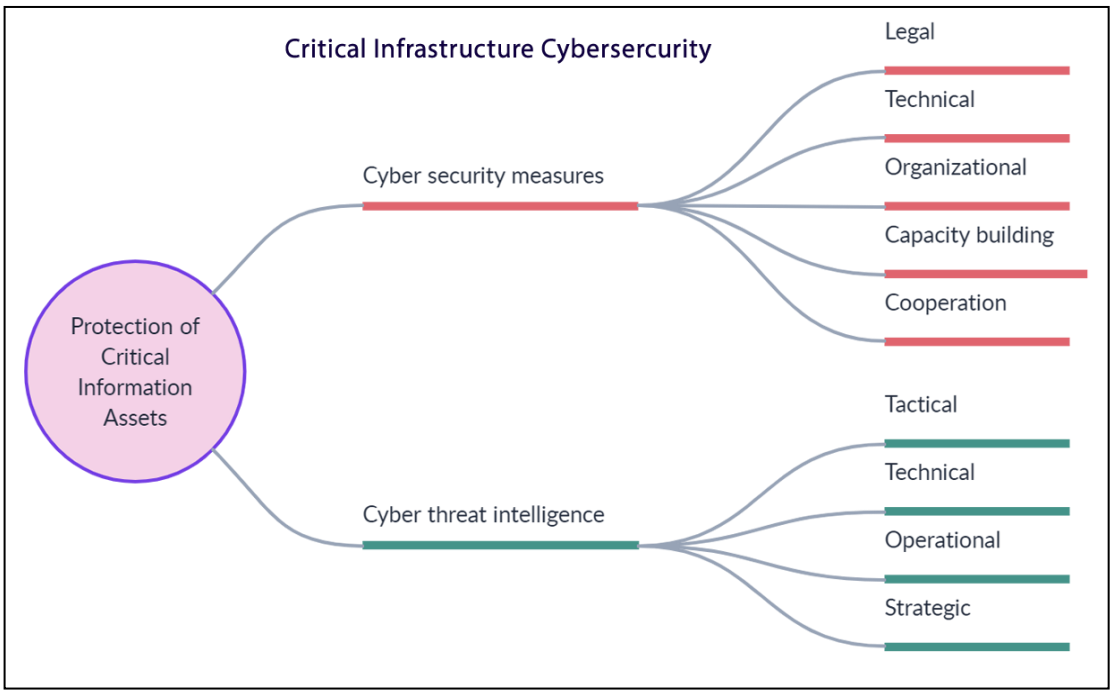

Image 22: Critical infrastructure protection measures [184]

Critical infrastructure protection can be achieved through various measures:

- Legal instruments involve legislation, regulatory frameworks and the adoption of good practices (e.g. ISO 27001).
- Technical means consist of hardware and software procurement and usage software of assets to prevent, detect, mitigate and respond to cyber-attacks (e.g. firewall, IDS, IPS, antivirus, antimalware, forensics).
- Organizational measures include the adoption of a cybersecurity strategy and participation in cybersecurity exercises.
- Capacity building involves increasing staff knowledge and awareness.
- Collaborative means include information sharing and research to increase the resilience of organizations against cyber threats.

Within the same study [184], there is also an acknowledgment of the significance attributed to cyber threat intelligence. This concept encompasses proactive security measures characterized by the pre-emptive collection of information preceding an attack. The purpose of this information gathering is to enhance comprehension of the wider threat landscape and facilitate the implementation of preventive measures. The proposed classification of threat intelligence can be outlined as follows:

- Tactical: The provided information is derived from actively monitoring systems in real-time allowing defenders to ensure that their incident response systems and investigations are adequately equipped to handle the tactics employed by these adversaries.
- Technical: The aforementioned data is acquired and processed using technical methods serving as a valuable resource for defenders, enabling them to proactively take preventive measures like blocking suspected IP addresses.
- Operational: The provided data offers specific information regarding incoming attacks providing valuable insights that can inform and assist in responding to specific incidents, as well as aid in assessing the organization's capability to identify and address future cyber threats.
- Strategic: The presented data constitutes valuable high-level information and serves as a timely warning regarding cyber threats. It is primarily utilized by individuals at the board level or other senior decision-makers within the organization.

Finally, the NIST framework [314] plays a pivotal role as a foundational element within the strategic cybersecurity strategy specifically tailored for critical infrastructures. It stands as an influential and extensively acknowledged guideline that has been meticulously developed by the esteemed National Institute of Standards and Technology (NIST) in the United States. It provides a comprehensive and structured approach for organizations to assess, manage, and enhance their cybersecurity posture. The framework is designed to assist organizations in effectively addressing and mitigating cybersecurity risks, regardless of their size, sector, or technological complexity. By offering a common language, the NIST framework facilitates consistent and effective communication among stakeholders, enabling a shared understanding of cybersecurity objectives, processes, and outcomes.

The Framework provides a versatile approach to tackle cybersecurity concerns, encompassing the impact of cybersecurity on physical, cyber, and human dimensions. It is applicable to organizations relying on technology, regardless of whether their cybersecurity efforts primarily revolve around information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or interconnected devices such as the Internet of Things (IoT). The Framework serves as a valuable tool for organizations to address cybersecurity matters concerning the privacy of customers, employees, and other stakeholders. Furthermore, the outcomes outlined in the Framework serve as benchmarks for guiding workforce development and fostering continuous improvement endeavors.

The NIST framework encourages a proactive and adaptive approach to cybersecurity. By encompassing five core functions—Identify, Protect, Detect, Respond, and Recover—the framework covers the entire cybersecurity lifecycle. It enables organizations to not only establish preventive measures but also develop robust detection and response capabilities.

Image 23: NIST framework core functions [314]

- The "Identify" function involves understanding and managing cybersecurity risks by establishing an organizational baseline and conducting continuous asset and risk management.
- The "Protect" function emphasizes the implementation of appropriate safeguards to protect against potential threats. This includes activities such as access control, security awareness training, and data encryption.
- The "Detect" function aims to develop and deploy mechanisms for timely identification of cybersecurity events. This involves implementing monitoring systems, conducting anomaly detection, and establishing incident response procedures.
- The "Respond" function encompasses the ability to effectively respond to and mitigate detected cybersecurity incidents. It involves incident management, communication, and mitigation activities.
- Lastly, the "Recover" function focuses on restoring normal operations and services following a cybersecurity incident. This includes developing and implementing recovery plans, conducting post-incident analysis, and improving future response capabilities.

The significance of the NIST framework lies in its ability to align cybersecurity practices with business objectives. By incorporating a risk-based approach, the framework enables organizations to prioritize their efforts and allocate resources efficiently. It assists in identifying and understanding cybersecurity risks specific to an organization, taking into account its unique operating environment, assets, and threats. This tailored approach enhances decision-making processes and ensures that cybersecurity efforts are aligned with the organization's broader goals.

10 Conclusions

The realm of cybersecurity in critical infrastructures presents both compelling and arduous challenges. The threat landscape undergoes constant evolution, driven by both technological advances and hostile adversaries. Furthermore, the shifting geopolitical landscape has rendered state actors as key threats to the security of critical infrastructures. Concurrently, the allure of cybercrime has grown substantially, empowered by increasingly potent damage infliction capabilities and the ability to elude repercussions. Additionally, the lack of security awareness among end-users makes them vulnerable to potential attacks, while other critical infrastructures can turn into liabilities during such events.

The integration of novel technologies with legacy systems yields a challenging amalgamation that encompasses the cybersecurity issues of both elements. Meanwhile, modern technological advancements continue to exacerbate existing insecurities.

The presence of risks permeates every level of critical infrastructures, encompassing operational environments, as well as new threats, attack vectors and technologies. Within the domains of IT, OT, IoT, and Cloud, all environments are susceptible to significant contemporary threats, including insider threats, social engineering, phishing attacks, supply chain attacks, ransomware, and Denial-of-Service (DoS) attacks. Scenarios such as telecommuting and the implementation of BYOD policies further exacerbate the circumstances and introduce new emerging threats.

We have to keep in mind that an additional challenge in securing critical infrastructures, including those in Greece, is that several of them are either partially or entirely owned by private entities. Consequently, owners of these infrastructures tend to prioritize security measures that maintain their profitability, rather than implementing comprehensive security protocols and frameworks.

It is crucial to acknowledge that there is no such thing as absolute security when adopting any security strategy. The critical question is how quickly we can detect, respond, and recover from a cyberattack.

The foremost priority of any cybersecurity strategy designed for critical infrastructures is the safeguarding of human life, citizens' rights, the environment, and national sovereignty. In this context, all possible organizational and technical measures must be taken, while adhering to existing legislation and regulations and within the context of proportionality. The threat landscape needs to be constantly monitored, and all cyber threats and actors that could potentially jeopardize essential service providers should be identified, documented and monitored.

In order to achieve a successful cybersecurity strategy, it is imperative to incorporate complementary concepts such as Security by Design, Defense in Depth, Zero Trust, and Isolation. In addition, it is crucial to engage in a multifaceted protection network with other governmental agencies, organizations, and consortia.

This scholarly work aimed to provide an all-encompassing analysis of the subject under scrutiny. However, due to the broad scope of the topic, it was not practically feasible to present a complete examination within the limitations of this dissertation. Thus, this research area may hold great promise for further exploration at the doctoral level.

We hold the belief that the most crucial factors pertaining to contemporary cybersecurity threats have been comprehensively covered, as a range of elements has been diligently selected to counteract risks that relate to the entirety of the CIA triad while also considering the triad of organizational, technological, and human resources.

Concluding this study, we maintain that this dissertation may serve as a valuable resource and a solid foundational reference for readers seeking to expand their knowledge on the subject of cybersecurity in critical infrastructures.

11 Bibliography

The most recent access of every link occurred at April 3, 2023.

[1]	Law 4577, Government Gazette 199/2018, "Incorporation into Greek legislation of Directive 2016/1148/EU of the European Parliament and of the Council on measures for a high common level of security of network and information systems across the Union and other provisions".
[2]	M. Plachkinova and A. Vo (2022) "A Taxonomy of Cyberattacks against Critical Infrastructure," Journal of Cybersecurity Education, Research and Practice, vol. 2021, no. 2 , article 3, Feb 2022.
[3]	J. E. Sullivan and D. Kamensky, “How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid,” The Electricity Journal, vol. 30, no. 3. Elsevier BV, pp. 30–35, Apr. 2017. doi: 10.1016/j.tej.2017.02.006.
[4]	Cybersecurity and Infrastructure Security Agency, “CISA Strategic Plan 2023-2025,” Sep. 2022.
[5]	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.
[6]	European Commission. Joint Research Centre et al., “Cybersecurity, our digital anchor: a European perspective”, LU: Publications Office, 2020. doi: 10.2760/352218.
[7]	M. Theoharidou, "Risk Assessment of Critical Information and Communication (ICT) Infrastructures," Ph.D. Thesis, Department of Informatics, Athens University of Economics and Business, May 2010
[8]	European Union Agency for Cybersecurity, ENISA threat landscape 2022: July 2021 to July 2022. LU: Publications Office, 2022. doi: 10.2824/764318.
[9]	European Union Agency for Cybersecurity., ENISA threat landscape 2021: April 2020 to mid July 2021. LU: Publications Office, 2021. doi: 10.2824/324797.
[10]	European Union Agency for Cybersecurity., NIS investments: November 2022. LU: Publications Office, 2021. doi: 10.2824/433214.
[11]	European Union Agency for Cybersecurity., Foresight challenges. LU: Publications Office, 2021. doi: 10.2824/187824.
[12]	G. Desarnaud, "Cyber Attacks and Energy Infrastructures: Anticipating Risks," Etudes de l'Ifri, Jan. 2017
[13]	M. Anisetti et al., "Security Threat Landscape," White Paper Security Threats, Jul. 2020.
[14]	G. Stergiopoulos, "Securing Critical Infrastructures at software and interdependency levels," Ph.D. Thesis, Department of Informatics, Athens University of Economics and Business, Nov. 2015.
[15]	S. Argyropoulou, "Risk Assessment in Critical and Dependent Communication and Information Infrastructures," MSc thesis, University of Piraeus, Feb. 2013.
[16]	A. Nikolopoulou, "The Directive on security of network and information systems (NIS Directive) from a practical view – Challenges for the Aviation Industry," MSc thesis, International Hellenic University, Dec. 2018.
[17]	K. Geers, “The Cyber Threat to National Critical Infrastructures: Beyond Theory,” The Information Security Journal: A Global Perspective, vol. 18, no. 1, pp. 1-7, 2009.
[18]	National Institute of Standards and Technology, “Guide for Conducting Risk Assessments,” NIST Special Publication 800-30, Sep. 2012.
[19]	P. Sanders, C. Bronk, and M. D. Bazilian, “Critical energy infrastructure and the evolution

	of cybersecurity," The Electricity Journal, vol. 35, no. 10. Elsevier BV, p. 107224, Dec. 2022. doi: 10.1016/j.tej.2022.107224.
[20]	https://www.independent.co.uk/news/long_reads/cyber-warfare-saudi-arabia-petrochemical-security-america-a8258636.html
[21]	M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," Arabian Journal for Science and Engineering, vol. 45, no. 4. Springer Science and Business Media LLC, pp. 3171–3189, Jan. 06, 2020. doi: 10.1007/s13369-019-04319-2.
[22]	Md Haris Uddin Sharif and Mehmood Ali Mohammed, "A literature review of financial losses statistics for cyber security and future trend," World Journal of Advanced Research and Reviews, vol. 15, no. 1. GSC Online Press, pp. 138–156, Jul. 30, 2022. doi: 10.30574/wjarr.2022.15.1.0573.
[23]	https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/
[24]	https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
[25]	https://www.eett.gr/opencms/export/sites/default/EETT_EN/Journalists/MarketAnalysis/MarketReview/PDFs/2019.pdf
[26]	https://www.dpa.gr/sites/default/files/2022-01/4_2022%20anonym%20%282%29_0.pdf
[27]	https://elstat-outsourcers.statistics.gr/Census2022_GR.pdf
[28]	https://kede.gr/diarroi-prosopikon-dedomenon-apo-ta-systimata-tou-dimou-thessalonikis/
[29]	https://thessaloniki.gr/%ce%ba-%ce%b6%ce%ad%cf%81%ce%b2%ce%b1%cf%82-%cf%83%ce%b5-%ce%bb%ce%b5%ce%b9%cf%84%ce%bf%cf%85%cf%81%ce%b3%ce%af%ce%b1-%cf%8c%ce%bb%ce%b5%cf%82-%ce%bf%ce%b9-%ce%b4%ce%b7%ce%bc%ce%bf%cf%84%ce%b9%ce%ba/
[30]	https://diavgeia.gov.gr/doc/6%CE%9F%CE%A7%CE%9B%CE%A9%CE%A15-%CE%A07%CE%A7?inline=true
[31]	https://elta.gr/singleblog/deltia-tupou/press-release-21032022-cyberattack-against-the-hellenic-post
[32]	https://elta.gr/singleblog/deltia-tupou/epanafora-kai-gia-to-teleutaio-sustima-ton-elta-pliris-i-epanafora-ton-upiresion
[33]	https://diavgeia.gov.gr/search?advanced&query=q:%22%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B5%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7%22&page=0&fq=organizationUid:%2250039%22&sort=relative
[34]	https://www.desfa.gr/press-center/press-releases/anakoinwsh
[35]	Center for Strategic & International Studies, "Significant Cyber Incidents since 2006," www.csis.org
[36]	https://www.cisa.gov/uscert/sites/default/files/Annual_Reports/Year_in_Review_FY2010_Final_S508C.pdf
[37]	S. Al-Rabiaah, "The "Stuxnet" Virus of 2010 As an Example of A "APT" and Its "Re-cent" Variances," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 2018, pp. 1-5, doi: 10.1109/NCG.2018.8593143.
[38]	https://www.cisa.gov/uscert/sites/default/files/publications/AA21-042A_Joint_Cybersecurity_Advisory_Compromise_of_U.S._Drinking_Treatment_Facility.pdf
[39]	https://www.energy.gov/ceser/colonial-pipeline-cyber-incident
[40]	https://www.fmcsa.dot.gov/emergency/esc-ssc-wsc-regional-emergency-declaration-2021-002-05-09-2021
[41]	https://www.cisa.gov/uscert/ncas/alerts/aa20-352a
[42]	https://composite-indicators.jrc.ec.europa.eu/explorer/explorer/indices/GCI/global-cyber-security-index
[43]	Deloitte, "Cybersecurity," Digital Transformation Observatory HFE, Jul. 2020.
[44]	Council of Europe, "Convention on Cybercrime," European Treaty Series - No. 185 ETS

	185, Budapest, 23.XI.2001.
[45]	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
[46]	Decision No. 1027, Government Gazette 3739/2019, "Issues of implementation and procedures of Law no. 4577/2018 (A΄ 199)".
[47]	https://www.cisa.gov/critical-infrastructure-sectors
[48]	https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en
[49]	https://www.eeas.europa.eu/eeas/towards-more-secure-global-and-open-cyberspace-eu-presents-its-new-cybersecurity-strategy_en
[50]	https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[51]	European Commission, Joint Communication to the European Parliament and the Council, "The EU's Cybersecurity Strategy for the Digital Decade," JOIN (2020) 18 final, Brussels, Dec., 2020.
[52]	https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/
[53]	Ministry of Digital Governance, National Cybersecurity Authority, National Cybersecurity Strategy 2020 -2025, Dec. 2020
[54]	European Parliament and the Council of the European Union, "REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)", Official Journal of the European Union, 2019.
[55]	European Parliament and the Council of the European Union, "Regulation (EU) 2018/1725 of The European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC", Official Journal of the European Union, 2018.
[56]	Law 4624, Government Gazette 137/2019, "Hellenic Data Protection Authority, measures implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and transposing into national law Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 and other provisions".
[57]	Act of Legislative Content 671/2022, Government Gazette 4657/2022, "Approval of the Risk Preparedness Plan, in accordance with Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk preparedness in the electricity sector and repealing Directive 2005/89/EC".
[58]	M. Weiss and F. Biermann, "Cyberspace and the protection of critical national infrastructure," Journal of Economic Policy Reform. Informa UK Limited, pp. 1–18, Apr. 05, 2021. doi: 10.1080/17487870.2021.1905530.
[59]	https://www.nis.gr/downloads/national-cert/RFC2350-GR.pdf
[60]	National Intelligence Service, RFC2350 - Operation of the National CERT, Version 1.1 - 2022.07.05.
[61]	European Parliament and the Council of the European Union, "Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency", 2004.
[62]	Law 2472/1997, Government Gazette A' 50/10.04.1997, "Protection of Individuals from the Processing of Personal Data"
[63]	Presidential decree 178, Government Gazette 281/2014, "Organization of Greek Police Services".

[64]	Law 4070, Government Gazette 82/2012, "Regulation of Electronic Communications, Transport, Public Works and other provisions".
[65]	Law 3115, Government Gazette 47/2003, "Hellenic Authority for Communication Security and Privacy".
[66]	Law 3387, Government Gazette 224/2005, "Center for Security Studies and other provisions".
[67]	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-15.pdf
[68]	R. S. Ross, M. Winstead and M. McEvilley, “Engineering Trustworthy Secure Systems,” National Institute of Standards and Technology, 2022. doi: 10.6028/nist.sp.800-160v1r1.
[69]	P. D. Gasper and J. Rodriguez, "Understanding the Value of a Computer Emergency Response Capability for Nuclear Security". The International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange. Vienna, Austria. June 2015.
[70]	Defence Science Board Washington DC, “Resilient Military Systems and the Advanced Cyber Threat,” Task Force Report. Accession No ADA5699752013, Jan. 2013.
[71]	J. P. Brashear, “Managing Risk to Critical Infrastructures, Their Interdependencies, and the Region They Serve: A Risk Management Process,” Optimizing Community Infrastructure. Elsevier, pp. 41–67, 2020. doi: 10.1016/b978-0-12-816240-8.00003-3.
[72]	ISO 27001
[73]	European Network and Information Security Agency, "Smart Grid Security," Annex 2 to the ENISA study ‘Smart Grid Security: Recommendations for Europe and Member States, Jun. 2012.
[74]	G. Weimann, "Cyberterrorism: How Real Is the Threat?", United States Institute of Peace, Special Report 119, May 13, 2004.
[75]	https://www.microsoft.com/en-us/security/blog/2022/10/21/securing-iot-devices-against-attacks-that-target-critical-infrastructure/
[76]	R. Das and M. Z. Gündüz, "Analysis of cyber-attacks in IoT-based critical infrastructures", International Journal of Information Security Science, vol. 8, no. 4, pp. 122-133, Dec. 2019
[77]	https://www.tepco.co.jp/news/2014/1238798_5918.html
[78]	B. Sándor and D. J. Fehér, "Examining the Relationship between the Bitcoin and Cybercrime," 2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 2019, pp. 121-126, doi: 10.1109/SACI46893.2019.9111568.
[79]	S. Cordey, “The Evolving Cyber Threat Landscape during the Coronavirus Crisis,” ETH Zurich, 2020. doi: 10.3929/ETHZ-B-000458221.
[80]	Cyberwatching.eu, "Covid-19 Pandemic - A New Crisis in Privacy," 2021.
[81]	https://blog.shodan.io/trends-in-internet-exposure/
[82]	S. Wass, S. Pournouri, and G. Ibbotson, “Prediction of Cyber Attacks During Coronavirus Pandemic by Classification Techniques and Open Source Intelligence,” Cybersecurity, Privacy and Freedom Protection in the Connected World. Springer International Publishing, pp. 67–100, 2021. doi: 10.1007/978-3-030-68534-8_6.
[83]	Las 4807, Government Gazette 96/2021, "Institutional framework for teleworking, provisions on human resources in the public sector and other urgent regulations".
[84]	Hellenic Data Protection Authority, “Guideline 1/2021 on the application of personal data protection rules in the context of teleworking", Athens, 4/8/2021.
[85]	IBM Corporation, Cost of a Data Breach Report 2022.
[86]	Identity Theft Resource Center, "Identify Compromisers: From the Era of Identity Theft to the Age of Identity Fraud," ITRC Annual Data Breach Report, 2022.
[87]	S. Mabunda, "Cryptocurrency: The New Face of Cyber Money Laundering," 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 2018, pp. 1-6, doi: 10.1109/ICABCD.2018.8465467.
[88]	H. Loiseau, D. Ventre, and H. Aden, Eds., Cybersecurity in Humanities and Social Sci-

	ences. Wiley, 2020. doi: 10.1002/9781119777588.
[89]	https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html
[90]	https://securelist.com/initial-access-data-price-on-the-dark-web/106740/
[91]	R. Koch, “Hidden in the Shadow: The Dark Web - A Growing Risk for Military Operations?,” 2019 11th International Conference on Cyber Conflict (CyCon). IEEE, May 2019. doi: 10.23919/cycon.2019.8756708.
[92]	Z. Yunos and S. Hafidz Suid, "Protection of Critical National Information Infrastructure (CNII) against cyber terrorism: Development of strategy and policy framework," 2010 IEEE International Conference on Intelligence and Security Informatics, Vancouver, BC, Canada, 2010, pp. 169-169, doi: 10.1109/ISI.2010.5484748.
[93]	S. S. Sin, L. A. Blackerby, E. Asiamah and R. Washburn, "Determining extremist organisations' likelihood of conducting cyber attacks," 2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2016, pp. 81-98, doi: 10.1109/CYCON.2016.7529428.
[94]	https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions#terror
[95]	Council of the EU, " Council Conclusions on shaping the European Union's cyber stance," 9364/22, Brussels, May 23, 2022
[96]	European Parliament and the Council of the European Union, "EU cyber defence policy framework," Brussels, November 19, 2018.
[97]	A. Tanchev, "The strategic dimensions of cyber-security – an interdisciplinary approach," FOKUS 7/2018, Austria Institut für Europa-und Sicherheitspolitik.
[98]	https://ec.europa.eu/newsroom/cipr/newsletter-archives/40013
[99]	European Commission, "Critical Infrastructure Resilience: News, Updates and Events," ISSN 2600-3570, Jul 2022.
[100]	https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
[101]	Cybersecurity and Infrastructure Security Agency, “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure,” Apr. 2022.
[102]	https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf
[103]	Informal meeting of the Heads of State or Government, Versailles Declaration, Mar. 2022.
[104]	M. Libicki, "The coming of cyber espionage norms," 2017 9th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2017, pp. 1-17, doi: 10.23919/CYCON.2017.8240325.
[105]	Microsoft, "Illuminating the threat landscape and empowering a digital defense," Microsoft Digital Defense Report 2022.
[106]	D. J. Bodeau, C. D. McCollum and D. B. Fox, “Cyber Threat Modeling: Survey, Assessment, and Representative Framework,” Homeland Security Systems Engineering Development Institute, DHS reference no. 16-J-00184-01, Apr. 2018.
[107]	https://www.reuters.com/article/us-cyberattacks-china-idUSBRE98G0M720130917
[108]	https://www.smh.com.au/technology/australian-spies-buying-computer-bugs-sources-20120307-1ujlb.html
[109]	United States of America, Plaintiff, v. Dmitry Dokuchaev, Igor Sushchin, Alexsey Belan, Karim Baratov, Defendant, United States District Court, Northern District of California, San Francisco Division, Feb. 28, 2017.
[110]	L. Y. Connolly and D. S. Wall, “The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures,” Computers & Security, vol. 87. Elsevier BV, p. 101568, Nov. 2019. doi: 10.1016/j.cose.2019.101568.
[111]	M. Willett, “Lessons of the SolarWinds Hack,” Survival, vol. 63, no. 2. Informa UK Limited, pp. 7–26, Mar. 04, 2021. doi: 10.1080/00396338.2021.1906001.
[112]	https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions#hack

[113]	https://www.cfr.org/cyber-operations/ukrainian-it-army
[114]	European Union Agency for Cybersecurity., ENISA threat landscape for supply chain attacks. LU: Publications Office, 2021. doi: 10.2824/168593.
[115]	https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/advanced_persistent_threat_incident_handling_handbook
[116]	https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
[117]	https://www.cisa.gov/defining-insider-threats
[118]	I. Gaidarski and Z. Minchev, "Insider Threats to IT Security of Critical Infrastructures," Studies in Big Data. Springer International Publishing, pp. 381–394, 2021. doi: 10.1007/978-3-030-65722-2_24.
[119]	H. A. Aldawood and G. Skinner, "A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications," 2018 26th International Conference on Systems Engineering (ICSEng). IEEE, Dec. 2018. doi: 10.1109/icseng.2018.8638166.
[120]	S. K. Venkatachary, A. Alagappan, and L. J. B. Andrews, "Cybersecurity challenges in energy sector (virtual power plants) - can edge computing principles be applied to enhance security?," Energy Informatics, vol. 4, no. 1. Springer Science and Business Media LLC, Mar. 31, 2021. doi: 10.1186/s42162-021-00139-7.
[121]	R. Setola, E. Luiijf, and M. Theocharidou, "Critical Infrastructures, Protection and Resilience," Managing the Complexity of Critical Infrastructures. Springer International Publishing, pp. 1–18, 2016. doi: 10.1007/978-3-319-51043-9_1.
[122]	R. Setola and M. Theocharidou, "Modelling Dependencies Between Critical Infrastructures," Managing the Complexity of Critical Infrastructures. Springer International Publishing, pp. 19–41, 2016. doi: 10.1007/978-3-319-51043-9_2.
[123]	E. Luiijf, "Understanding Cyber Threats and Vulnerabilities," Critical Infrastructure Protection. Springer Berlin Heidelberg, pp. 52–67, 2012. doi: 10.1007/978-3-642-28920-0_4.
[124]	Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7. Elsevier BV, pp. 8176–8186, Nov. 2021. doi: 10.1016/j.egyr.2021.08.126.
[125]	https://encyclopedia.kaspersky.com/glossary/attack-vector/
[126]	Randori, an IBM Company, "The State of Attack Surface Management 2022".
[127]	Joint Chiefs of Staff, "Cyberspace Operations," Joint Publication 3-12, Jun. 2018.
[128]	https://www.ibm.com/topics/attack-surface
[129]	https://www.crowdstrike.com/cybersecurity-101/attack-surface/
[130]	https://www.fortinet.com/resources/cyberglossary/attack-surface
[131]	https://www.upguard.com/blog/attack-surface
[132]	https://nordvpn.com/blog/attack-surface/
[133]	M. Amanowicz and M. Kamola, "Building Security Awareness of Interdependent Services, Business Processes, and Systems in Cyberspace," Electronics, vol. 11, no. 22. MDPI AG, p. 3835, Nov. 21, 2022. doi: 10.3390/electronics11223835.
[134]	E. Staddon, V. Loscri, and N. Mitton, "Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey," Applied Sciences, vol. 11, no. 16. MDPI AG, p. 7228, Aug. 05, 2021. doi: 10.3390/app11167228.
[135]	A. Adel, D. Sarwar, and A. Hosseinian-Far, "Transformation of Cybersecurity Posture in IT Telecommunication: A Case Study of a Telecom Operator," Cybersecurity, Privacy and Freedom Protection in the Connected World. Springer International Publishing, pp. 441–457, 2021. doi: 10.1007/978-3-030-68534-8_28.
[136]	A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," Procedia Economics and Finance, vol. 28. Elsevier BV, pp. 24–31, 2015. doi: 10.1016/s2212-5671(15)01077-1.

[137]	T. Plėta, M. Tvaronavičienė, S. D. Casa, and K. Agafonov, “Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases,” Insights into Regional Development, vol. 2, no. 3. Entrepreneurship and Sustainability Center, pp. 703–715, Sep. 01, 2020. doi: 10.9770/ird.2020.2.3(7).
[138]	Z. A. Sheikh, Y. Singh, P. K. Singh, and K. Z. Ghafoor, “Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope,” Computer Communications, vol. 193. Elsevier BV, pp. 302–331, Sep. 2022. doi: 10.1016/j.comcom.2022.07.007.
[139]	U. J. Butt, W. Richardson, A. Nouman, H.-M. Agbo, C. Eghan, and F. Hashmi, “Cloud and Its Security Impacts on Managing a Workforce Remotely: A Reflection to Cover Remote Working Challenges,” Cybersecurity, Privacy and Freedom Protection in the Connected World. Springer International Publishing, pp. 285–311, 2021. doi: 10.1007/978-3-030-68534-8_18.
[140]	A. Bello, S. Jahan, F. Farid, and F. Ahamed, “A Systemic Review of the Cybersecurity Challenges in Australian Water Infrastructure Management,” Water, vol. 15, no. 1. MDPI AG, p. 168, Dec. 31, 2022. doi: 10.3390/w15010168.
[141]	M. Amin, "Security challenges for the electricity infrastructure," in Computer, vol. 35, no. 4, pp. supl8-supl10, April 2002, doi: 10.1109/MC.2002.1012423.
[142]	C.-W. Ten, G. Manimaran, and C.-C. Liu, “Cybersecurity for Critical Infrastructures: Attack and Defense Modeling,” IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 40, no. 4. Institute of Electrical and Electronics Engineers (IEEE), pp. 853–865, Jul. 2010. doi: 10.1109/tsmca.2010.2048028.
[143]	M. Chorąś, R. Kozik, A. Flizikowski, W. Hołubowicz, and R. Renk, “Cyber Threats Impacting Critical Infrastructures,” Managing the Complexity of Critical Infrastructures. Springer International Publishing, pp. 139–161, 2016. doi: 10.1007/978-3-319-51043-9_7.
[144]	S. K. Venkatachary, J. Prasad, and R. Samikannu, “Cybersecurity and cyber terrorism - in energy sector – a review,” Journal of Cyber Security Technology, vol. 2, no. 3–4. Informa UK Limited, pp. 111–130, Oct. 02, 2018. doi: 10.1080/23742917.2018.1518057.
[145]	D. Markopoulou, “Tackling cybersecurity challenges in the energy and water sectors in the context of the cybersecurity and sectoral regulatory frameworks: the case of smart metering systems in the new digitalised environment,” International Review of Law, Computers & Technology. Informa UK Limited, pp. 1–26, 07-Jul-2022.
[146]	A. Hassanzadeh et al., “A Review of Cybersecurity Incidents in the Water Sector,” Journal of Environmental Engineering, vol. 146, no. 5. American Society of Civil Engineers (ASCE), May 2020. doi: 10.1061/(asce)ee.1943-7870.0001686.
[147]	https://www.cisa.gov/sites/default/files/publications/AA21-287A-Ongoing_Cyber_Threats_to_U.S._Water_and_Wastewater_Systems.pdf
[148]	L. Tabansky, “Cyber Security Challenges: The Israeli Water Sector Example,” Cyber-Physical Security. Springer International Publishing, pp. 205–219, Aug. 11, 2016. doi: 10.1007/978-3-319-32824-9_10.
[149]	Executive Agency for Small and Medium sized Enterprises, “ICT4WATER cluster: vision and showcases”, LU: Publications Office, 2021.
[150]	C. Bosco, G. S. Raspati, K. Tefera, H. Rishovd, and R. Ugarelli, “Protection of Water Distribution Networks against Cyber and Physical Threats: The STOP-IT Approach Demonstrated in a Case Study,” Water, vol. 14, no. 23. MDPI AG, p. 3895, Nov. 30, 2022. doi: 10.3390/w14233895.
[151]	E. D. Perakslis, “Cybersecurity in Health Care,” New England Journal of Medicine, vol. 371, no. 5. Massachusetts Medical Society, pp. 395–397, Jul. 31, 2014. doi: 10.1056/nejmp1404358.
[152]	H. Alami, M.-P. Gagnon, M. A. Ag Ahmed, and J.-P. Fortin, “Digital health: Cybersecurity is a value creation lever, not only a source of expenditure,” Health Policy and Technology, vol. 8, no. 4. Elsevier BV, pp. 319–321, Dec. 2019. doi: 10.1016/j.hlpt.2019.09.002.
[153]	D. I. Dogaru and I. Dumitrache, "Cyber security in healthcare networks," 2017 E-Health and Bioengineering Conference (EHB), Sinaia, Romania, 2017, pp. 414-417, doi:

	10.1109/EHB.2017.7995449.
[154]	[S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin, “A retrospective impact analysis of the WannaCry cyberattack on the NHS,” npj Digital Medicine, vol. 2, no. 1. Springer Science and Business Media LLC, Oct. 02, 2019. doi: 10.1038/s41746-019-0161-6.
[155]	S. Nifakos et al., “Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review,” Sensors, vol. 21, no. 15. MDPI AG, p. 5119, Jul. 28, 2021. doi: 10.3390/s21155119.
[156]	M. S. Jalali and J. P. Kaiser, “Cybersecurity in Hospitals: A Systematic, Organizational Perspective,” Journal of Medical Internet Research, vol. 20, no. 5. JMIR Publications Inc., p. e10059, May 28, 2018. doi: 10.2196/10059.
[157]	https://www.iso.org/standard/62777.html
[158]	R. Kumar, “Quantitative safety-security risk analysis of interconnected cyber-infrastructures,” 2022 IEEE 10th Region 10 Humanitarian Technology Conference (R10-HTC). IEEE, Sep. 16, 2022. doi: 10.1109/r10-htc54060.2022.9929906.
[159]	F. Petit, D. et al., "Analysis of Critical Infrastructure Dependencies and Interdependencies," Argonne National Laboratory, Report ANL/GSS-15/4, Jun. 2015.
[160]	C. Alcaraz and S. Zeadally, “Critical infrastructure protection: Requirements and challenges for the 21st century,” International Journal of Critical Infrastructure Protection, vol. 8. Elsevier BV, pp. 53–66, Jan. 2015. doi: 10.1016/j.ijcip.2014.12.002.
[161]	G. Sharkov, “Assessing the Maturity of National Cybersecurity and Resilience,” Connections: The Quarterly Journal, vol. 19, no. 4. Procon, Ltd., pp. 5–24, 2020. doi: 10.11610/connections.19.4.01.
[162]	A. da S. Oliveira and H. Santos, “Continuous Industrial Sector Cybersecurity Assessment Paradigm: Proposed Model of Cybersecurity Certification,” 2022 18th International Conference on the Design of Reliable Communication Networks (DRCN). IEEE, Mar. 28, 2022. doi: 10.1109/drcn53993.2022.9758022.
[163]	A. Ocaka, D. O. Briain, S. Davy, and K. Barrett, “Cybersecurity Threats, Vulnerabilities, Mitigation Measures in Industrial Control and Automation Systems: A Technical Review,” 2022 Cyber Research Conference - Ireland (Cyber-RCI). IEEE, Apr. 25, 2022. doi: 10.1109/cyber-rci55324.2022.10032665.
[164]	Š. Kavan and M. Z. Freitinger Skalická, "Security of critical information infrastructure and possible disruption as a crisis," 2022 11th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2022, pp. 1-5, doi: 10.1109/MECO55406.2022.9797175.
[165]	P. A. Wibowo Putro and D. I. Sensuse, "Threats, Vulnerabilities and Security Functions in Critical Information Infrastructure," 2021 8th International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), Semarang, Indonesia, 2021, pp. 113-117, doi: 10.1109/ICITACEE53184.2021.9617515.
[166]	K. Abbasi, N. Petford, and A. Hosseinian-Far, “Centralised IT Structure and Cyber Risk Management,” Cybersecurity, Privacy and Freedom Protection in the Connected World. Springer International Publishing, pp. 357–366, 2021. doi: 10.1007/978-3-030-68534-8_22.
[167]	A. Hussien, “Cyber Security Crimes, Ethics and a Suggested Algorithm to Overcome Cyber-Physical Systems Problems (CybSec1)”, in Journal of Information Security, 12, 56-78, 2021.
[168]	M. Malatji, A. L. Marnewick, and S. Von Solms, “Cybersecurity capabilities for critical infrastructure resilience,” Information & Computer Security, vol. 30, no. 2. Emerald, pp. 255–279, Oct. 14, 2021. doi: 10.1108/ics-06-2021-0091.
[169]	M. Lourenco and L. Marinos . ENISA Threat Landscape 2019/2020 - The year in review, 2020. Doi: 10.2824/552242.
[170]	J. Magunduni and W. Chigona, "Revisiting shadow IT research: What we already know, what we still need to know, and how do we get there?," 2018 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2018, pp. 1-6,

	doi: 10.1109/ICTAS.2018.8368735.
[171]	Y. Ulianovska, S. Florov, A. Hrebeniuk, T. Katkova, D. Prokopovich-Tkachenko and R. Gvozdov, "Formalized Designing Methodology of ISMS for Critical Infrastructure," 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2021, pp. 587-590, doi: 10.1109/PICST54195.2021.9772182.
[172]	Y. Fadlallah, M. Sbeiti, M. Hammoud, M. Nehme and A. Fadlallah, "On the Cyber Security of Lebanon: A Large Scale Empirical Study of Critical Vulnerabilities," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-6, doi: 10.1109/ISDFS49300.2020.9116446.
[173]	Z. Chen, L. Yan, Y. He, D. Bai, X. Liu and L. Li, "Reflections on the Construction of Cyber Security Range in Power Information System," 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2018, pp. 2093-2097, doi: 10.1109/IAEAC.2018.8577685.
[174]	https://www.iso.org/standard/82875.html
[175]	https://deddie.gr/el/stratigiki-eksugxronismos/eksugxronismos/susthmata-epopteias-diaxeirishs-thlexeirismpu-diktuou/nea-sistimata-scada/
[176]	https://www.desfa.gr/userfiles/consultations/diag-689_17-teuxos-se-dimosia-diavouleusi.pdf
[177]	https://www.eyath.gr/neo-exeligmeno-scada-stin-apocheteysi/
[178]	https://www.eydap.gr/TheCompany/DrainageAndSewerage/NetworkFuctionality/
[179]	R. Colelli, C. Foglietta, S. Panzieri and F. Pascucci, "An opacity approach for security exposure of IoT components in critical infrastructures," 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 2019, pp. 427-432, doi: 10.1109/SMC.2019.8914291.
[180]	C. Greer, M. Burns, D. Wollman, and E. Griffor, “Cyber-physical systems and internet of things,” National Institute of Standards and Technology, Mar. 2019. doi: 10.6028/nist.sp.1900-202.
[181]	https://scadahacker.com/library/Documents/Cyber_Events/Nozomi%20-%20TRITON%20-%20The%20First%20SIS%20Cyberattack.pdf
[182]	G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger and J. Benjamin, "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," in IEEE Access, vol. 9, pp. 165295-165325, 2021, doi: 10.1109/ACCESS.2021.3133348.
[183]	https://www.cisa.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
[184]	L. Maglaras, M. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, and S. Rallis, “Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures,” ICST Transactions on Security and Safety, vol. 5, no. 16. European Alliance for Innovation n.o., p. 155856, Dec. 11, 2018. doi: 10.4108/eai.15-10-2018.155856.
[185]	H. Yacoob Bhaiyat and S. P. Sithungu, "The Emergence of IIoT and its Cyber Security Issues in Critical Information Infrastructure," 21st European Conference on Cyber Warfare and Security, vol. 21, no. 1. 2022.
[186]	https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf
[187]	https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-deloitte-managing-the-successful-convergence-of-it-and-ot.pdf
[188]	L. Maglaras, I. Kantzavelou, and M. A. Ferrag, “Digital Transformation and Cybersecurity of Critical Infrastructures,” Applied Sciences, vol. 11, no. 18. MDPI AG, p. 8357, Sep. 09, 2021. doi: 10.3390/app11188357.
[189]	P. Anand, Y. Singh, A. Selwal, P. K. Singh, R. A. Felseghi, and M. S. Raboaca, “IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids,” Energies, vol. 13, no. 18. MDPI AG, p. 4813, Sep. 15, 2020. doi: 10.3390/en13184813.

[190]	Y. Cherdantseva, P. Burnap, S. Nadjm-Tehrani, and K. Jones, “A Configurable Dependency Model of a SCADA System for Goal-Oriented Risk Assessment,” Applied Sciences, vol. 12, no. 10. MDPI AG, p. 4880, May 11, 2022. doi: 10.3390/app12104880.
[191]	P. Simoes, T. Cruz, J. Gomes and E. Monteiro “On the use of Honeypots for Detecting Cyber Attacks on Industrial Control Networks,” European Conference on Information Warfare and Security, Jul. 2013.
[192]	K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security,” National Institute of Standards and Technology, Jun. 2015. doi: 10.6028/nist.sp.800-82r2.
[193]	M. Abbasi, M. Plaza-Hernandez, J. Prieto, and J. M. Corchado, “Security in the Internet of Things Application Layer: Requirements, Threats, and Solutions,” IEEE Access, vol. 10. Institute of Electrical and Electronics Engineers (IEEE), pp. 97197–97216, 2022. doi: 10.1109/access.2022.3205351.
[194]	A. Djenna and D. Eddine Saïdouni, "Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure," 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, France, 2018, pp. 1-4, doi: 10.1109/CSNET.2018.8602974.
[195]	M. Alsheikh, L. Konieczny, M. Prater, G. Smith and S. Uludag, "The State of IoT Security: Unequivocal Appeal to Cybercriminals, Onerous to Defenders," in IEEE Consumer Electronics Magazine, vol. 11, no. 3, pp. 59-68, 1 May 2022, doi: 10.1109/MCE.2021.3079635.
[196]	A. Djenna, D. E. Saidouni and W. Abada, "A Pragmatic Cybersecurity Strategies for Combating IoT-Cyberattacks," 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 2020, pp. 1-6, doi: 10.1109/ISNCC49221.2020.9297251.
[197]	B. Zhao et al., "A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1826-1840, 1 May-June 2022, doi: 10.1109/TDSC.2020.3037908.
[198]	A. Khurshid, R. Alsaaidi, M. Aslam, and S. Raza, “EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme,” IEEE Access, vol. 10. Institute of Electrical and Electronics Engineers (IEEE), pp. 129932–129948, 2022. doi: 10.1109/access.2022.3225973.
[199]	A. N. Bikos and S. A. P. Kumar, “Securing Digital Ledger Technologies-Enabled IoT Devices: Taxonomy, Challenges, and Solutions,” IEEE Access, vol. 10. Institute of Electrical and Electronics Engineers (IEEE), pp. 46238–46254, 2022. doi: 10.1109/access.2022.3169141.
[200]	B. Shabandri and P. Maheshwari, "Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2019, pp. 1069-1075, doi: 10.1109/SPIN.2019.8711591.
[201]	S. Raponi, M. Caprolu and R. Di Pietro, “Beyond SolarWinds: The Systemic Risks of Critical Infrastructures, State of Play, and Future Directions” ITASEC ’21: Italian Conference on Cyber Security, April 07–09, 2021.
[202]	Q. Sun et al., “A Comprehensive Review of Smart Energy Meters in Intelligent Energy Networks,” IEEE Internet of Things Journal, vol. 3, no. 4. Institute of Electrical and Electronics Engineers (IEEE), pp. 464–479, Aug. 2016. doi: 10.1109/jiot.2015.2512325.
[203]	https://www.eydap.gr/userfiles/Presentations/viosimi_anaptyxi_2021.pdf
[204]	https://www.eydap.gr/userfiles/Attachments/2022/dt_economist.pdf
[205]	https://www.eyath.gr/calls/symfonia-plaisio-me-titlo-promitheia-egkatastasi-thesi-se-leitoyrgia-kai-leitoyrgia-ydrometriton-oikiakis-chrisis-stin-periochi-drastiriotitas-tis-eyath-ae/
[206]	Y. Yan, R. Q. Hu, S. K. Das, H. Sharif and Y. Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," in IEEE Network, vol. 27, no. 4, pp. 64-71, July-August 2013, doi: 10.1109/MNET.2013.6574667.

[207]	https://deddie.gr/Documents2/DIAKIRIXEIS%202015/DD%20207%20SYMPLIROMA%20No7/%CE%A4%CE%B5%CF%8D%CF%87%CE%BF%CF%82%20%CE%91%20%CE%A0%CF%81%CF%8C%CF%83%CE%BA%CE%BB%CE%B7%CF%83%CE%B7%20%CE%A3%CF%85%CE%BC%CF%80%CE%BB%CE%AE%CF%81%CF%89%CE%BC%CE%B1%20%CE%9D%CE%BF7.pdf
[208]	S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, “Smart meters for power grid: Challenges, issues, advantages and status,” Renewable and Sustainable Energy Reviews, vol. 15, no. 6. Elsevier BV, pp. 2736–2742, Aug. 2011. doi: 10.1016/j.rser.2011.02.039.
[209]	M. P. McHenry, “Technical and governance considerations for advanced metering infrastructure/smart meters: Technology, security, uncertainty, costs, benefits, and risks,” Energy Policy, vol. 59. Elsevier BV, pp. 834–842, Aug. 2013. doi: 10.1016/j.enpol.2013.04.048.
[210]	E. McKenna, I. Richardson, and M. Thomson, “Smart meter data: Balancing consumer privacy concerns with legitimate applications,” Energy Policy, vol. 41. Elsevier BV, pp. 807–814, Feb. 2012. doi: 10.1016/j.enpol.2011.11.049.
[211]	F. M. Cleveland, "Cyber security issues for Advanced Metering Infrasttructure (AMI)," 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 2008, pp. 1-5, doi: 10.1109/PES.2008.4596535.
[212]	D. B. Avancini, J. J. P. C. Rodrigues, S. G. B. Martins, R. A. L. Rabêlo, J. Al-Muhtadi, and P. Solic, “Energy meters evolution in smart grids: A review,” Journal of Cleaner Production, vol. 217. Elsevier BV, pp. 702–715, Apr. 2019. doi: 10.1016/j.jclepro.2019.01.229.
[213]	P. Van Aubel and E. Poll, “Smart metering in the Netherlands: What, how, and why,” International Journal of Electrical Power & Energy Systems, vol. 109. Elsevier BV, pp. 719–725, Jul. 2019. doi: 10.1016/j.ijepes.2019.01.001.
[214]	V. Aravinthan, V. Namboodiri, S. Sunku and W. Jewell, "Wireless AMI application and security for controlled home area networks," 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 2011, pp. 1-8, doi: 10.1109/PES.2011.6038996.
[216]	H. Li, S. Gong, L. Lai, Z. Han, R. C. Qiu and D. Yang, "Efficient and Secure Wireless Communications for Advanced Metering Infrastructure in Smart Grids," in IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1540-1551, Sept. 2012, doi: 10.1109/TSG.2012.2203156.
[217]	C. Bennett and S. B. Wicker, "Decreased time delay and security enhancement recommendations for AMI smart meter networks," 2010 Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 2010, pp. 1-6, doi: 10.1109/ISGT.2010.5434780.
[218]	I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller, and M. Gruteser, “Neighborhood watch,” 2012 ACM Conference on Computer and Communications Security. ACM, Oct. 16, 2012. doi: 10.1145/2382196.2382246.
[219]	A. M. Khattak, S. I. Khanji, and W. A. Khan, “Smart Meter Security: Vulnerabilities, Threat Impacts, and Countermeasures,” Advances in Intelligent Systems and Computing. Springer International Publishing, pp. 554–562, 2019. doi: 10.1007/978-3-030-19063-7_44.
[220]	P. Gope and B. Sikdar, "Privacy-Aware Authenticated Key Agreement Scheme for Secure Smart Grid Communication," in IEEE Transactions on Smart Grid, vol. 10, no. 4, pp. 3953-3962, July 2019, doi: 10.1109/TSG.2018.2844403.
[221]	C. -I. Fan, S. -Y. Huang and Y. -L. Lai, "Privacy-Enhanced Data Aggregation Scheme Against Internal Attackers in Smart Grid," in IEEE Transactions on Industrial Informatics, vol. 10, no. 1, pp. 666-675, Feb. 2014, doi: 10.1109/TII.2013.2277938.
[222]	S. McLaughlin, P. McDaniel, and W. Aiello, “Protecting consumer privacy from electric load monitoring,” 18th ACM conference on Computer and Communications Security. ACM, Oct. 17, 2011. doi: 10.1145/2046707.2046720.
[223]	https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019L0944&from=EN

[224]	[P. C. Verhoef et al., “Digital transformation: A multidisciplinary reflection and research agenda,” Journal of Business Research, vol. 122. Elsevier BV, pp. 889–901, Jan. 2021. doi: 10.1016/j.jbusres.2019.09.022.
[225]	Ministry of Digital Governance, Digital Transformation Strategy, 2020-2025, Dec. 2020.
[226]	https://www.ktpae.gr/diagwnismoi/%ce%b4%ce%b9%ce%b1%ce%ba%ce%ae%cf%81%cf%85%ce%be%ce%b7-%ce%b7%ce%bb%ce%b5%ce%ba%cf%84%cf%81%ce%bf%ce%bd%ce%b9%ce%ba%ce%bf%cf%8d-%ce%b1%ce%bd%ce%bf%ce%b9%ce%ba%cf%84%ce%bf%cf%8d-%ce%b4%ce%b9%ce%b5-4/
[227]	R. Iliev and K. Ignatova, “Cloud Technologies for Building a System of Data Centres for Defence and Security,” Studies in Big Data. Springer International Publishing, pp. 13–24, 2021. doi: 10.1007/978-3-030-65722-2_2.
[228]	I. Kanwal, H. Shafi, S. Memon, and M. H. Shah, “Cloud Computing Security Challenges: A Review,” Cybersecurity, Privacy and Freedom Protection in the Connected World. Springer International Publishing, pp. 459–469, 2021. doi: 10.1007/978-3-030-68534-8_29.
[229]	B. B. Gupta and O. P. Badve, “Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment,” Neural Computing and Applications, vol. 28, no. 12. Springer Science and Business Media LLC, pp. 3655–3682, Apr. 13, 2016. doi: 10.1007/s00521-016-2317-5.
[230]	https://www.gsis.gr/en/public-administration/G-Cloud
[231]	European Network and Information Security Agency., Critical Cloud Computing: A CIIP perspective on cloud computing services. 2012.
[232]	http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wHUdWr4xouZundtvSoClrL8yb7l1HobT0h5MXD0LzQTLWPU9yLzB8V68knBzLCmTXKaO6fpVZ6Lx9hLslJUqeiQ_D666Ef5eMVZ9_vCnX9uO2JR-_NBf_GRZw-9xUI6UnA.
[233]	https://www.gsis.gr/sites/default/files/2022-04/B1824.pdf
[234]	M. Schukat, "Securing critical infrastructure," The 10th International Conference on Digital Technologies 2014, Zilina, Slovakia, 2014, pp. 298-304, doi: 10.1109/DT.2014.6868731.
[235]	https://www.gsis.gr/sites/default/files/2022-04/%CE%A6%CE%95%CE%9A%204636%20%206-10-2021%20%20%CE%9A%CE%A5%CE%91%20%CE%94%CE%95%CE%97%2B%CE%94%CE%95%CE%94%CE%97%CE%95.pdf
[236]	https://www.gsis.gr/sites/default/files/2019-10/%CE%A6%CE%99%CE%9B%CE%9F%CE%9E%CE%95%CE%9D%CE%99%CE%91%20-%20%CE%BF%CE%B4%CE%B7%CE%B3%CE%B9%CE%B5%CF%82%20%CF%87%CF%81%CE%B7%CF%83%CE%B7%CF%82%20-procsurvey_UserGuide%20-%20v2.pdf
[237]	https://www.gsis.gr/sites/default/files/2022-07/manual_EDA_v4.pdf
[238]	A. V. Herrera, M. Ron and C. Rabadão, "National cyber-security policies oriented to BYOD (bring your own device): Systematic review," 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, Portugal, 2017, pp. 1-4, doi: 10.23919/CISTI.2017.7975953.
[239]	V. Hassija, V. Chamola, V. Gupta, S. Jain and N. Guizani, "A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6222-6246, 15 April15, 2021, doi: 10.1109/JIOT.2020.3025775.
[240]	V. Shalamanov, S. Matern, and G. Penchev, “Digitalization and Cyber Resilience Model for the Bulgarian Academy of Sciences,” Studies in Big Data. Springer International Publishing, pp. 77–92, 2021. doi: 10.1007/978-3-030-65722-2_6.

[241]	https://cloudsecurityalliance.org/research/cloud-controls-matrix/
[242]	I. Ghafir et al., “Security threats to critical infrastructure: the human factor,” The Journal of Supercomputing, vol. 74, no. 10. Springer Science and Business Media LLC, pp. 4986–5002, Mar. 26, 2018. doi: 10.1007/s11227-018-2337-2.
[243]	A. Georgiadou, A. Michalitsi-Psarrou, and D. Askounis, “Evaluating The Cyber-Security Culture of the EPES Sector,” 17th International Conference on Availability, Reliability and Security. ACM, Aug. 23, 2022. doi: 10.1145/3538969.3543813.
[244]	M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, “Panning for gold: Automatically analysing online social engineering attack surfaces,” Computers & Security, vol. 69. Elsevier BV, pp. 18–34, Aug. 2017. doi: 10.1016/j.cose.2016.12.013.
[245]	https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering
[246]	D. Airehrour, N. V. Nair, and S. Madanian, “Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model,” Information, vol. 9, no. 5. MDPI AG, p. 110, May 03, 2018. doi: 10.3390/info9050110.
[247]	N. Y. Conteh and P. J. Schmick, “Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks,” International Journal of Advanced Computer Research, vol. 6, no. 23. Association of Computer, Communication and Education for National Triumph Social and Welfare Society (ACCENTS), pp. 31–38, Feb. 12, 2016. doi: 10.19101/ijacr.2016.623006.
[248]	G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," in IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317-3318, July 2017, doi: 10.1109/TPWRS.2016.2631891.
[249]	Bundesamt für Sicherheit in der Informationstechnik, "Die Lage der IT-Sicherheit in Deutschland 2014," Nov 2014.
[250]	K. D. Mitnick and William L. Simon, "The Art of Deception: Controlling the Human Element of Security," 2003, John Wiley & Sons, Inc., USA.
[251]	N. Z. Khidzir, A. R. Ismail, K. A. M. Daud, M. S. A. A. Ghani, S. Ismail, and A. H. Ibrahim, “Human Factor of Online Social Media Cybersecurity Risk Impact on Critical National Information Infrastructure,” Advances in Intelligent Systems and Computing. Springer International Publishing, pp. 195–207, 2016. doi: 10.1007/978-3-319-41932-9_16.
[252]	Canadian Centre for Cyber Security, “An Introduction to the Cyber Threat Environment 2023–2024,” ISBN 978-0-660-45952-3, 2022.
[253]	N. C. Sia, A. Hosseinian-Far, and T. T. Toe, “Reasons Behind Poor Cybersecurity Readiness of Singapore’s Small Organizations: Reveal by Case Studies,” Cybersecurity, Privacy and Freedom Protection in the Connected World. Springer International Publishing, pp. 269–283, 2021. doi: 10.1007/978-3-030-68534-8_17.
[254]	C. W. Johnson, “Anti-social networking: crowdsourcing and the cyber defence of national critical infrastructures,” Ergonomics, vol. 57, no. 3. Informa UK Limited, pp. 419–433, Jul. 05, 2013. doi: 10.1080/00140139.2013.812749.
[255]	https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing
[256]	M. Safaei Pour, C. Nader, K. Friday, and E. Bou-Harb, “A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security,” Computers & Security, vol. 128. Elsevier BV, p. 103123, May 2023. doi: 10.1016/j.cose.2023.103123.
[257]	[N. R. Mead, “Critical Infrastructure Protection and Supply Chain Risk Management,” 2022 IEEE 30th International Requirements Engineering Conference Workshops (REW). IEEE, Aug. 2022. doi: 10.1109/rew56159.2022.00047.
[258]	https://www.cisa.gov/sites/default/files/publications/phishing_trends0511.pdf
[259]	T. Cuchta et al., “Human Risk Factors in Cybersecurity,” 20th Annual SIG Conference on Information Technology Education. ACM, Sep. 26, 2019. doi: 10.1145/3349266.3351407.
[260]	S. Purkait, “Phishing counter measures and their effectiveness – literature review,” Information Management & Computer Security, vol. 20, no. 5. Emerald, pp. 382–420, Nov. 23,

	2012. doi: 10.1108/09685221211286548.
[261]	R. Islam and J. Abawajy, “A multi-tier phishing detection and filtering approach,” Journal of Network and Computer Applications, vol. 36, no. 1. Elsevier BV, pp. 324–335, Jan. 2013. doi: 10.1016/j.jnca.2012.05.009.
[262]	G. L. Sanders, S. Upadhyaya and X. Wang, "Inside the Insider," in IEEE Engineering Management Review, vol. 47, no. 2, pp. 84-91, 1 Second quarter, June 2019, doi: 10.1109/EMR.2019.2917656.
[263]	Counter-Terrorism Committee Executive Directorate (CTED), "The protection of critical infrastructures against terrorist attacks: Compendium of good practices," 2018.
[264]	C. Czeschik, “Black Market Value of Patient Data,” Digital Marketplaces Unleashed. Springer Berlin Heidelberg, pp. 883–893, Sep. 15, 2017. doi: 10.1007/978-3-662-49275-8_78.
[265]	https://www.cisa.gov/sites/default/files/publications/20-02019b%20-%20Telework_Essentials-08272020-508v2.pdf
[266]	S. Marshall, “IT Consumerization: A Case Study of BYOD in a Healthcare Setting,” Technology Innovation Management Review, vol. 4, no. 3. Carleton University, pp. 14–18, Mar. 24, 2014. doi: 10.22215/timreview/771.
[267]	https://www.e-nomothesia.gr/kat-ergasia-koinonike-asphalise/nomos-4808-2021-phek-101a-19-6-2021.html
[268]	K. Ghazinour, D. M. Vakharia, K. C. Kannaji and R. Satyakumar, "A study on digital forensic tools," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 3136-3142, doi: 10.1109/ICPCSI.2017.8392304.
[269]	T. A. Wani, A. Mendoza, and K. Gray, “Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature,” JMIR mHealth and uHealth, vol. 8, no. 6. JMIR Publications Inc., p. e18175, Jun. 18, 2020. doi: 10.2196/18175.
[270]	https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/eidikoiskopoi/ergasiakessxeseis/faq_ergasiakes/tilergasia
[271]	European Network and Information Security Agency, "Consumerization of IT: Risk Mitigation Strategies," ENISA Report, Dec. 2012.
[272]	A. Redondo, A. Torres-Barrán, D. R. Insua, and J. Domingo, “Assessing Supply Chain Cyber Risks.” arXiv, 2019. doi: 10.48550/ARXIV.1911.11652.
[273]	N. Kshetri and J. Voas, "Supply Chain Trust," in IT Professional, vol. 21, no. 2, pp. 6-10, 1 March-April 2019, doi: 10.1109/MITP.2019.2895423.
[274]	Department of Defense, “Securing Defense-Critical Supply Chains: An action plan developed in response to President Biden's Executive Order 14017”, Feb 2022.
[275]	https://www.cisa.gov/information-and-communications-technology-supply-chain-risk-management
[276]	https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
[277]	T. M. S. do Amaral and J. J. C. Gondim, “Integrating Zero Trust in the cyber supply chain security,” 2021 Workshop on Communication Networks and Power Systems (WCNPS). IEEE, Nov. 18, 2021. doi: 10.1109/wcnps53648.2021.9626299.
[278]	https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
[279]	European Union Agency for Cybersecurity., Identifying emerging cybersecurity threats and challenges for 2030. LU: Publications Office, 2023. doi: 10.2824/117542.
[280]	https://news-web.php.net/php.internals/113838
[281]	https://incolumitas.com/2016/06/08/typosquatting-package-managers/
[282]	A. R. Nygård and S. Katsikas, “SoK: Combating threats in the digital supply chain,” 17th International Conference on Availability, Reliability and Security. ACM, Aug. 23, 2022. doi: 10.1145/3538969.3544421.
[283]	A. Coufalikova, I. Klaban, and T. Slajs, “Complex strategy against supply chain attacks,”

	2021 International Conference on Military Technologies (ICMT). IEEE, Jun. 08, 2021. doi: 10.1109/icmt52455.2021.9502768.
[284]	U. Javed Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal and A. Kumar, "Ransomware Threat and its Impact on SCADA," 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 2019, pp. 205-212, doi: 10.1109/ICGS3.2019.8688327.
[285]	European Union Agency for Cybersecurity., ENISA threat landscape for ransomware attacks. LU: Publications Office, 2022. doi: 10.2824/456263.
[286]	Homeland Security, “Ransomware Attacks on Critical Infrastructure Sectors,” 2022.
[287]	https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a
[288]	D. Manky, “Cybercrime as a service: a very modern business,” Computer Fraud & Security, vol. 2013, no. 6. Mark Allen Group, pp. 9–13, Jun. 2013. doi: 10.1016/s1361-3723(13)70053-8.
[289]	A. Higbee, “The role of crypto-currency in cybercrime,” Computer Fraud & Security, vol. 2018, no. 7. Mark Allen Group, pp. 13–15, Jan. 2018. doi: 10.1016/s1361-3723(18)30064-2.
[290]	A. Gazet, “Comparative analysis of various ransomware virii,” Journal in Computer Virology, vol. 6, no. 1. Springer Science and Business Media LLC, pp. 77–90, Jul. 04, 2008. doi: 10.1007/s11416-008-0092-2.
[291]	https://www.bleepingcomputer.com/news/security/ransomware-extortion-doesnt-stop-after-paying-the-ransom/
[292]	https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html
[293]	https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment
[294]	M. A. Branquinho, “Ransomware in Industrial Control Systems. What Comes After Wannacry and Petya Global Attacks?,” WIT Transactions on The Built Environment. WIT Press, Jun. 09, 2017. doi: 10.2495/safe170301.
[295]	S. R. Zahra and M. Ahsan Chishti, “RansomWare and Internet of Things: A New Security Nightmare,” 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, Jan. 2019. doi: 10.1109/confluence.2019.8776926.
[296]	M. Al-Hawawreh, F. d. Hartog and E. Sitnikova, "Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 4, pp. 7137-7151, Aug. 2019, doi: 10.1109/JIOT.2019.2914390.
[297]	A. Adamov and A. Carlsson, "The state of ransomware. Trends and mitigation techniques," 2017 IEEE East-West Design & Test Symposium (EWDTS), Novi Sad, Serbia, 2017, pp. 1-8, doi: 10.1109/EWDTS.2017.8110056.
[298]	https://www.cisa.gov/stopransomware/ransomware-guide
[299]	https://blog.cloudflare.com/ddos-attack-trends-for-2022-q2/
[300]	R. Shea and J. Liu, "Understanding the impact of Denial of Service attacks on Virtual Machines," 2012 IEEE 20th International Workshop on Quality of Service, Coimbra, Portugal, 2012, pp. 1-9, doi: 10.1109/IWQoS.2012.6245975.
[301]	https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf
[302]	S. Christensen, W. J. Caelli, W. D. Duncan, and E. Georgiades, “An Achilles heel: denial of service attacks on Australian critical information infrastructures,” Information & Communications Technology Law, vol. 19, no. 1. Informa UK Limited, pp. 61–85, Mar. 2010. doi: 10.1080/13600831003708059.
[303]	https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends
[304]	C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84, 2017, doi: 10.1109/MC.2017.201.
[305]	M. Özçelik, N. Chalabianloo and G. Gür, "Software-Defined Edge Defense Against IoT-Based DDoS," 2017 IEEE International Conference on Computer and Information Tech-

	nology (CIT), Helsinki, Finland, 2017, pp. 308-313, doi: 10.1109/CIT.2017.61.
[306]	R. K. Pandey and M. Misra, "Cyber security threats — Smart grid infrastructure," 2016 National Power Systems Conference (NPSC), Bhubaneswar, India, 2016, pp. 1-6, doi: 10.1109/NPSC.2016.7858950.
[307]	K. I. Sgouras, A. D. Birda and D. P. Labridis, "Cyber attack impact on critical Smart Grid infrastructures," ISGT 2014, Washington, DC, USA, 2014, pp. 1-5, doi: 10.1109/ISGT.2014.6816504.
[308]	A. Praseed and P. S. Thilagam, "DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 661-685, Firstquarter 2019, doi: 10.1109/COMST.2018.2870658.
[309]	Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," in Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765, Sept. 2016, doi: 10.1109/JPROC.2016.2558521.
[310]	https://www.cisa.gov/news-events/news/understanding-denial-service-attacks
[311]	H. Imran, M. Salama, C. Turner, and S. Fattah, “Cybersecurity Risk Management Frameworks in the Oil and Gas Sector: A Systematic Literature Review,” Lecture Notes in Networks and Systems. Springer International Publishing, pp. 871–894, 2022. doi: 10.1007/978-3-030-98015-3_59.
[312]	https://www.cisa.gov/uscert/ncas/alerts/aa22-011a
[313]	https://mindigital.gr/wp-content/uploads/2022/11/Cybersecurity-Self-Assessment-Tool-Greek-version.zip
[314]	“Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” National Institute of Standards and Technology, Apr. 2018. https://www.nist.gov/cyberframework, doi: 10.6028/nist.cswp.04162018.