applied sciences

MDPI

Article

Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure

Amir Djenna [1,*], Saad Harous [2,*] and Djamel Eddine Saidouni [1]

[1] Misc Laboratory, College of New Technologies of Information and Communication, University of Constantine2, Constantine 25000, Algeria; djamel.saidouni@univ-constantine2.dz
[2] College of Information Technology, United Arab Emirates University, Al-Ain 15551, United Arab Emirates
* Correspondence: amir.djenna@univ-constantine2.dz (A.D.); harous@uaeu.ac.ae (S.H.)

Abstract: As a new area of technology, the Internet of Things (IoT) is a flagship and promising paradigm for innovating society. However, IoT-based critical infrastructures are an appealing target for cybercriminals. Such distinctive infrastructures are increasingly sensitive to cyber vulnerabilities and subject to many cyberattacks. Thus, protecting these infrastructures is a significant issue for organizations and nations. In this context, raising the cybersecurity posture of critical cyber infrastructures is an extremely urgent international issue. In addition, with the rapid development of adversarial techniques, current cyber threats have become more sophisticated, complicated, advanced and persistent. Thus, given these factors, prior to implementing efficient and resilient cybersecurity countermeasures, identification and in-depth mapping of cyber threats is an important step that is generally overlooked. Therefore, to solve cybersecurity challenges, this study presents a critical analysis of the most recent cybersecurity issues for IoT-based critical infrastructures. We then discuss potential cyber threats and cyber vulnerabilities and the main exploitation strategies adopted by cybercriminals. Further, we provide a taxonomy of cyberattacks that may affect critical cyber infrastructures. Finally, we present security requirements and some realistic recommendations to enhance cybersecurity solutions.

Keywords: critical cyber infrastructure; cyber security; cyber attacks; Internet of Things (IoT)

Citation: Djenna, A.; Harous, S.; Saidouni, D.E. Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Appl. Sci.* **2021**, *11*, 4580. https://doi.org/10.3390/app11104580

Academic Editor: Antonio Ficarella
Received: 5 April 2021
Accepted: 7 May 2021
Published: 17 May 2021

1. Introduction

Human life has become increasingly dependent on modern information technology. Recent advances in new information and communication networks have led to a shift toward new emerged paradigms, such as smart grids [1], Internet of Things (IoT) [2], cloud computing [3], big data [4], and edge/fog computing [5,6]. The Internet of things occurs in cases where many devices are connected to the Internet for specific purposes through various techniques. Cloud computing brings a change in the investment mode and resource exploitation. The big data means of analyzing, extracting and processing complex data and large amounts of information. Edge/fog computing is an approach of pushing computing out of centralized systems for better and more scalable performance. Internet technologies have grown exponentially since the inception of the Internet. Currently, a new trend has emerged owing to future networking paradigms, that is, the fourth industrial revolution (Industry 4.0) [7,8]. The deployment of the IoT in manufacturing plans to provide optimized autonomous systems and self-configuring operations and make them intelligent is referred to as the industrial IoT (IIoT) [9–11]. Thus, IoT has become an inherent part of our everyday lives because many of its services are provided through billions of intelligent and autonomous objects around the world that are connected and communicate with each other [12]. This revolutionary paradigm creates a new dimension that eliminates the boundaries between the real and virtual worlds.

Cyber Physical System (CPS) [13] environments are industrial control and management systems, generally deployed on a large scale, allowing the monitoring, management

and administration of critical infrastructures in various fields: health, transport, nuclear, electricity, gas, water, and so forth. Unlike a traditional corporate IT network, the CPS environment allows business systems to be interconnected: industrial equipment, valves, thermal, chemical or medical sensors, command and control system, Human Machine Interface (HMI) rather than desktop computers. Thus, CPS is a set of digital and physical control systems such as (Industrial Control System/Supervisory Control And Data Acquisition (ICS/SCADA) [14–16], Distributed Control System (DCS) [15], Programmable Logic controller (PLC) [15], Remote Terminal Unit (RTU) [15] and Intelligent Electronic Device (IED) control machines [15], which enables it to perform monitoring and control (locally or remotely) of manufacturing processes, industrial production and distribution in real time. Therefore, Internet and ubiquitous networks have changed the way in which CPS communicate. In this context, IoT success is attributed to the advancements in hardware and communications technologies. The adoption rate of IoT devices will be extremely high as an increasing number of devices are connected to the Internet. As a pioneer in networked systems, Cisco predicts 4.8 ZB of Internet traffic by 2022, and the IP traffic is expected to triple in two years according to Cisco Visual Networking Index [17]. This growth will be driven by increases in numbers of Internet users and connected intelligent devices. Figure 1 shows the growth trend for the numbers of Internet-connected devices.

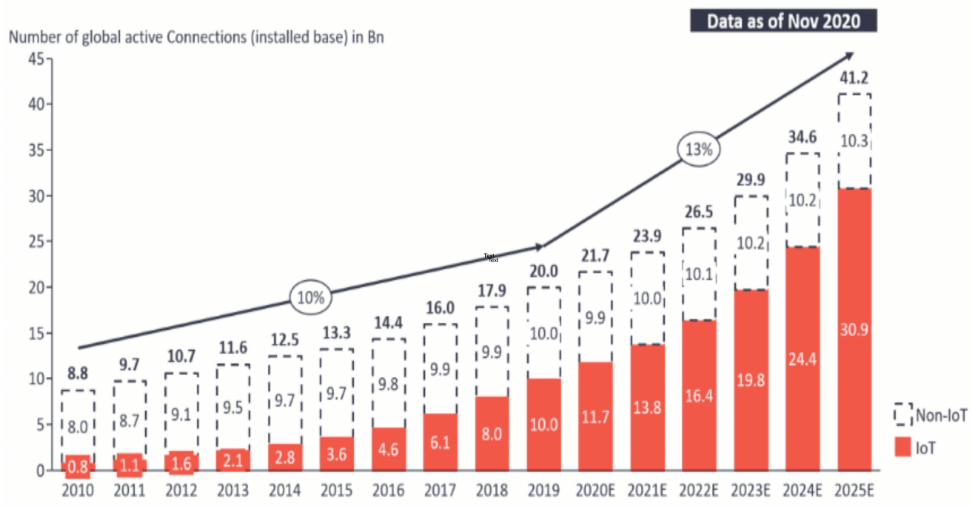

Figure 1. Estimated number of device connections by 2025 [18].

On 19 November 2020, the number of IoT connections (12 billion) exceeded the number of connections without IoT. By 2025, it is expected that there will be more than 30 billion IoT connections, with almost four IoT devices per person on an average [18]. According to IoT Analytics Research, the latest reports about the state of the IoT Q4 2020 and 2021 indicate that the number of IoT devices is predicated to increase much faster than that of non-IoT devices. Some predications expect 30.9 billion connected IoT devices by 2025 owing to the spread of 5G and 6G technologies. As expected, IoT trends suggest that the global number of connected IoT devices will significantly increase in the near future. IoT devices are cost-effective solutions that primarily rely on sensors and wireless communication systems to communicate with each other and transfer useful information to a centralized system. Moreover, the IoT has successfully integrated virtual spaces and the real world on the same platform [19]. The key strengths of IoT are upgrading and promoting smart environments and conscious autonomous devices, such as smart health [20,21], smart grid [22,23] and ICS [24]. Therefore, the power of the IoT is attributed to the non-necessity of any human intervention for the objects to communicate, analyze, process, store, and manage data autonomously. Undoubtedly, the diversity of connected devices in the IoT cyber infrastructure has improved the energy consumption, optimized production control and more or less better quality of service. However, the interconnection

to the internet, the integration of IoT and complex devices to modernize ICSs, smart grids, and smart health has opened up new security breaches. In this regard, intruders try to exploit the vulnerabilities of connected objects in order to penetrate into infrastructure and carry out harmful cyberattacks. Many large-scale cyberattacks have happened in the world. To this end, cyberattacks have had serious repercussions on cyber critical infrastructure. Next, we mention in Table 1 a non-exhaustive list of cyberattacks that have affected critical infrastructures in recent years:

Table 1. The famous cyberattacks in the history targeted critical cyber infrastructure.

Cyberattack	Year	Target	Description
Stuxnet	2010	ICS/SCADA	It was against Iranian nuclear centrifuges, a real example of a spectacular cyberattack, propagated as powerful and structured malware capable of infiltrating industrial programmable logic controllers that electrically control nuclear centrifuges.
ShaMoon	2012	ICS/SCADA	It occurred against the Saudi Arabia oil companies.
BlackEnergy	2015	Smart Grid	It happened against the Ukrainian smart grid, Germany in 2014, another example which allowed the deletion of data, the destruction of hard drives and the takeover of infected equipment. Ukraine's power central was unavailable through coordinated DDoS cyberattacks.
Mirai	2016	IoT Object	It was aimed at connected objects CCTV cameras.
WannaCry	2017	CPS/Healthcare	It was performed against hospitals in 2017.
SolarWinds	2020	Large-scale	Supply chain attack started in March 2020, carried out through an update compromise of Orion management and supervision platform. Among the victims: Governmental institutions, Microsoft, FireEye, Palo Alto Networks, Malwarebytes and Mimecast. Which shows that the targets are big security companies as well.
Hospital Ransomware	2021	CPS/Healthcare	In February 16th, 2021, Oloran-Sainte-Marie France hospital victim of ransomware cyberattack, which information system was paralyzed, none application works and neither external or internal network works.

These impactful incidents clearly show how harmful an IT security breach can be. It is also evident that the state of the art of cyber security has shifted to another dimension where intensive, furtive, perpetrated, complex, sophisticated and persistent cyberattacks are becoming the norm. Most cyberattacks cases are carried out by criminal organizations or nation states in a military-political context.

To this end, a new form of fifth-generation offensive cyberwarfare will be able to bring down a critical cyber infrastructure of a country without the use of arms. Indeed, ferocious cyberattacks have the appearance of cyber warfare. As a result, the cyber physical systems are attractive targets and the cyberattacks actors, aim to carry out industrial cyber espionage, sabotage, destabilization, colossal financial losses and loss of human life. Then cybersecurity concerns are a major obstacle to the evolution and correct functioning of critical cyber infrastructures. Identity theft, data corruption, sensitive information theft, advanced malware, and several modern massive cyberattacks, such as distributed denial of service and advanced persistent threats in particular, are the most serious issues that might arise at any critical cyber infrastructure. Hence, Cyber threats make cyber physical environments highly critical, in particular energy (electricity, gas, water, oil, nuclear, etc.) and cyber health infrastructures.

Despite the dysfunctions that cyberattacks can generate within critical cyber infrastructure, it also results the following risks: sensitive data theft, vital operations functioning disruption, critical services and resources unavailability, sessions hijacking, data alteration and deletion, industrial/medical equipment failures and destruction. For this purpose, critical cyber infrastructures are a fertile ground for malicious attacks. Therefore, they are

subject to devastating and dramatic cyberattacks if cyber security requirements are not taken into consideration.

Wherefore, protecting IoT-based critical cyber infrastructures from cyberattacks is essential. Herein, we answer the following relevant questions:

- Who are the targets?
- Who are the cyber attackers?
- How do they attack?
- How can we protect critical cyber infrastructures?

The primary contributions of this paper are summarized as follows:

- We provide a critical view of the most recent cybersecurity issues for IoT-based critical infrastructures.
- We discuss probable cyber threats and cyber vulnerabilities, followed by the main exploitation strategies adopted by cybercriminals. In addition, we provide an in-depth taxonomy of cyberattacks that may affect IoT-based critical cyber infrastructures.
- Finally, we present security requirements and some realistic recommendations and best practices to enhance cybersecurity solutions.

The rest of the paper is organized as follows: Section 2 describes smart health and industrial control system as a critical infrastructure, through the presentation of the main characteristics and functions. The architecture layers are discussed in this section as well. Section 3 surveys the different studies about security issues and their proposed solutions. Section 4 presents the most important assets of cyber physical system, describes in detail cyber threats, cyber vulnerabilities, including exploitation strategies, and provides a taxonomy in-depth of cyberattacks affecting IoT-based critical infrastructure, followed by the specific sources behind cyber threats. CPS security requirements are also depicted in this section. In Section 5, we present some realistic cybersecurity guidelines. Finally, we conclude the paper and suggest some future developments in the last section.

2. Smart Health and ICS as Critical Cyber Infrastructure

Generally, and according to the IEEE [25], "the IoT is a system consisting of networks of sensors, actuators, and smart objects whose purpose is to interconnect all things, including every day and industrial objects, in such a way as to make them intelligent, programmable, and more capable of interacting with humans and each other". In addition, IoT is used in healthcare to monitor the physiological health parameters of patients. However, there is no standard or unified definition of the IoT in healthcare. Some definitions emphasize the technical aspects, whereas the others focus more on uses and features.

With respect to healthcare, the IoT primarily manages and comprises a network of interconnected medical devices over the Internet to create smart healthcare environments [26]. Networked medical devices in smart health "can be worn (wearables) or implanted inside the body, for example, pacemakers," thereby providing services using smart methods. For example, "wearable health devices use an assortment of sensors to measure everything from heart rate, activity to sleep patterns and come equipped with communication capabilities. Such devices can form an IoT network for patient telemonitoring in hospitals and can also be used for home telemonitoring" [27]. Healthcare applications are projected to have the highest economic impact [28]. IoT-based healthcare and manufacturing applications are technologies that are expected to significantly affect society, as illustrated in Figure 2 [28].

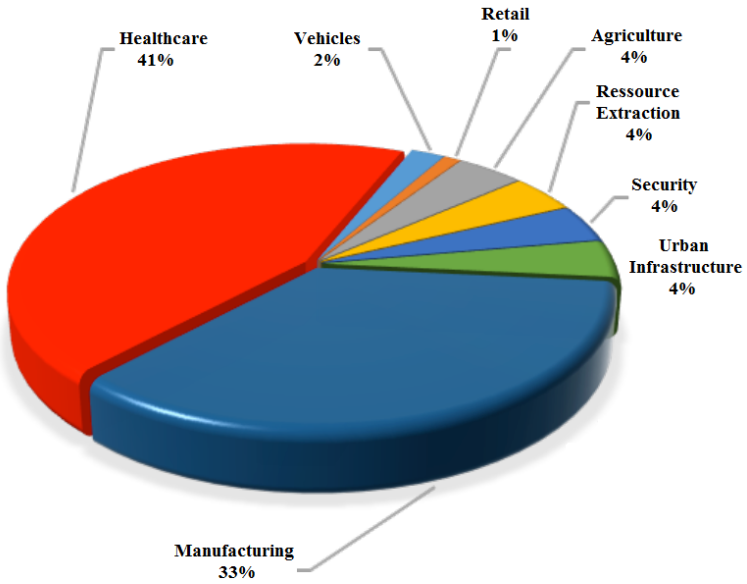

Figure 2. Predicted dominant IoT application by 2025.

An IoT-based healthcare system is a complex cyber infrastructure that deploys a range of devices and sensors that communicate discerningly across a fabric of heterogeneous, full distributed networks while providing ubiquitous services that are available at any place and time.This ecosystem of integrated care improves the quality of life for patients, reduces the time and the cost of care, and provides accurate and timely information to facilitate fast and effective decision-making and monitoring of patients with chronic diseases [29]. The key idea of IoT-based healthcare systems is the facilitation of useful functions via the "always-on" connectivity anywhere at any time for any patient [30], thereby providing remote diagnostics and treatment services, self-monitoring, and improving the quality of life by supporting a connected healthcare community.

The objective of the IoT-based CPS is to collect, manage, and analyze sensor data regardless of the corresponding protocols, formats, or network technologies used [31]. The development of such a flexible and adaptable architecture is essential. To this end, the IoT architecture comprises several layers that communicate with each other to connect the physical and virtual worlds. This architecture comprises three layers: the sensors/actuators, control/command and supervision levels [32–34]. Different typologies of architectures can be found in the literature to describe CPS; however, the Computer Integrated Manufacturing architecture (CIM) [35] will be presented to describe the different hierarchical levels. Figure 3 shows the architecture of an IoT-based CPS infrastructure. Each level is made up of characteristic elements and exchanges information with the other levels. The breakdown of this architecture is as follows:

Level 1 (Sensors—Actuators): In the perception layer, sensors are deployed in the perception layer to detect and collect environmental information. Thus, the perception layer is responsible for sensing and actuating physical processes, detecting certain physical parameters and identifying smart objects. Sensors and actuators make the link between the digital part and the physical part, forming the physical system. This level is also called the Operative Part (OP). The goal is to transform a raw material into a finished product via the production flow. Thus, the system brings the process from an initial state to a final state by acting on the production flow while guaranteeing productivity and reliability. In smart health context, it can identify hospitals, manage node networking, and collect related data, such as physician and nurse ID information, patient medical in formation, basic information about the location of pharmaceuticals, medical equipment, an object's geolocation in the hospital infrastructure, and information about the hospital environment [30]. The collected data are transmitted to the core network through various

communication technologies, for example, Wi-Fi, Bluetooth, RFID, NFC, UWB, BLE, LTE-A, and IEEE 802.15.4.

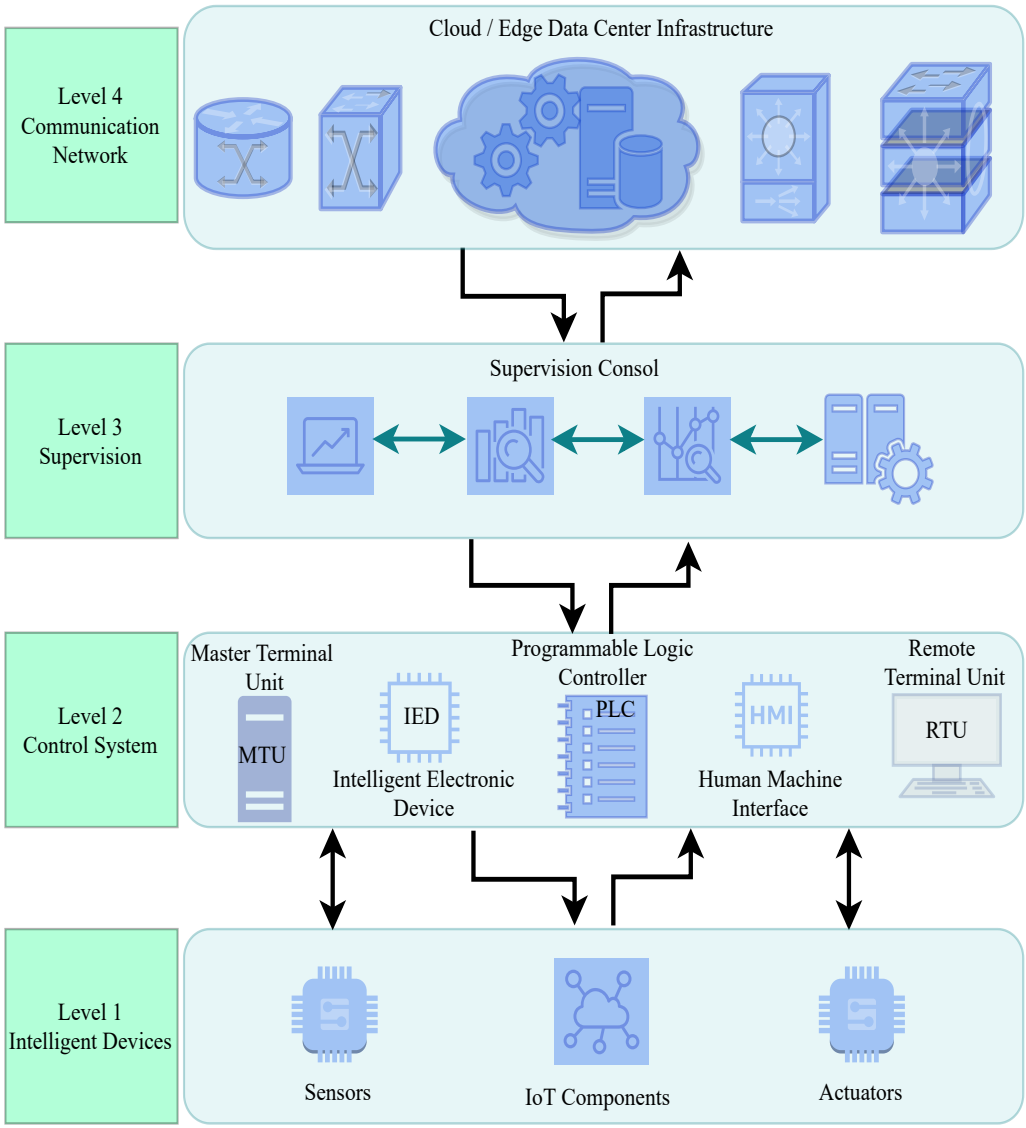

Figure 3. Architecture of an IoT-based CPS infrastructure.

Level 2 (Control/Command): This layer receives the data sent from the field by the sensors (level 1), controls the actuators (level 1) and communicates with the operators via the local Human Machine Interfaces (HMIs) and the supervision room. The main element of this level is the Programmable Logic Controller (PLC), which controls the system in real time.

Level 3 (Supervision): The role of this layer is to give an image at a point in the process. Thus, the data acquired by the lower levels are fed back. Operators can also control the system via production orders to adapt the control law and avoid damage. The term Supervisory Control And Data Acquisition (SCADA) can be used to refer to this part. Further, a set of applications dedicated to hospital computerization, management of medical technology, and all other aspects concerning management and supervision of health services [30], such as the computerization of ambulatory care management, visit management, diagnostics, radiology, pathologies, and physical therapy, medication management, material management, patient management, and financial management.

fLevel 4 (Communication Networks): Communication networks allow the different layers to be connected. Originally, ICSs used analog, digital or proprietary communication

protocols to exchange information, however, in recent architectures, TCP/IP is widely used to increase the volume and speed of data transported [36]. The communication networks is the backbone of CPS infrastructure. It supports access to the IoT backbone [37] and facilitates the transmission and reception of medical and industrial data. Furthermore, it facilitates the use of specific communications, including virtualization technologies when migrating to an IaaS Cloud. Thus, this layer is a platform of services that provides an open interface [38] for the various services related to end users.

However, cyber vulnerabilities in critical cyber infrastructure dramatically expose patients, medical staff, monitoring medical devices, industrial equipment, PLC and the entire ICS to a variety of serious cyber threats. Therefore, a CPS in cyber health, smart grid and industrial control environment are critical cyber infrastructures that must have maximum protection against malicious cybercriminals.

3. Literature Survey

IoT-based critical infrastructures are subject to a wide variety of cyberattacks, particularly massive cyberattacks, which are orchestrated stealthily through IoT botnets [39]. Thus, the greatest issue in IoT is cybersecurity because the consequences of cyberattacks can have significant impacts. A previous study [40] discussed security and privacy issues related to the implementation of the wireless body area network. In Reference [41], the authors provided an overview of potential risks to healthcare data. The study was based on quantitative analysis methods of historical data related to security incidents. Furthermore, in Reference [42], the authors described IoT threats and vulnerabilities in the healthcare context, and the authors of [43] reviewed the most recent security and privacy solutions offered in the IoT. They specifically discussed benefits that can improve security and privacy in the IoT relative to flexibility and scalability, as well as blockchain and Software-Defined Networking (SDN) technologies. In addition, they presented a general classification of attacks and threats. The International Medical Informatics Association investigated data protection in healthcare networked systems [44], and the ISO/TS18308 standard defines the privacy and security issues for electronic health records [45]. The authors of [46] discussed the vulnerabilities faced by the edge-side layer of the IoT. The authors of [47] presented a study on cyber security problems for smart grid. The study is focused on security requirements, network vulnerabilities, security protocols, some countermeasures, and future research directions to secure smart grid. In [48], the authors discussed the potential threats for cyber-physical systems and proposed a matrix classification of threats based on four elements (attack type, attack impact, attack intent and attack incident). The authors of [49] focused on security threats of SCADA systems, software and hardware vulnerabilities, and potential points of attack occurred on SCADA architecture. In [50], the authors developed a survey on security control and attack detection inside cyber physical system. Three types of attack were discussed in this work namely: denial of service attacks, replay attacks and deception attacks. The authors of [51] reviewed the vulnerability assessment of SCADA systems, focusing on several aspects such as asset discovery, vulnerabilities and threats identification, attack mitigation and the presentation of main risks related to confidentiality. The work in [52] focused on the main threats, protection measures in terms of legal, technical and organizational aspect, as well as the cyberattacks attribution. The authors of [53] have investigated the cyber security issues related to CPS. An analysis of the different methods, approaches and tools are presented in order to highlight some cyber security features related to critical infrastructure.

Vulnerability is seen as a weakness that can be exploited in IoT devices, mobile applications, firmware, operating systems, industrial equipment, medical devices, networks, people and business processes. A threat is the potential to exploit a vulnerability or a failure. In this regards, many researchers proposed different solutions. In [54], the authors review the cybersecurity risks of critical infrastructures such as supervisory control and data acquisition (SCADA) systems in the IoT environment. They provided security management strategies to beef up the security of SCADA networks. An overview of IoT reference model

and related security concerns are reviewed as well. In addition, vulnerabilities of SCADA systems as well as risk assessment approaches and risk management strategies to help mitigate vulnerabilities and threats are also examined.

In [55], the authors presented a comprehensive survey on attacks, security issues and blockchain as solution for IoT and IIoT. The survey attempts to classify the attacks based on the objects of vulnerability.

The authors in [56], provided an exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. Four distinct developments are investigated, including cryptography, fog computing, edge computing and Machine Learning (ML), to extend the degree of IoT security.

The authors [57] discussed case studies of major cybersecurity attacks on ICS infrastructures. They described attacks in terms of the goal and the consequences.

In [58], the authors reviewed the SCADA system architectures and comparative analysis of some communication protocols, followed by attacks on such systems. They presented a short investigation of the current state of intrusion detection techniques in SCADA, followed by a brief study of testbeds for scada systems.

The work in [59] analyzed the research landscape about Deep Learning (DL) approaches applied to IoT security. The study is based on three main research questions, namely, the security aspects involved, the used DL network architectures and the engaged datasets. The paper highlights the drawbacks and vulnerabilities of the DL approaches in the IoT security scenarios.

In [60], the authors analyzed how the different IoT platforms handle security and privacy vulnerabilities affecting the most common security services of confidentiality, integrity, availability and access control.

The work [61] investigated various opportunities and threats of using artificial intelligence (AI) technology in the manufacturing sector with consideration for offensive and defensive uses of such technology.

The work in [62] presented an analytical study of detecting anomalies, malicious activities, and cyber-attacks in a cyber-physical of critical water infrastructure in the IIoT infrastructure. The study uses various machine learning algorithms to classify the anomaly events including several attacks and IIoT hardware failures.

The European Network and Information Security Agency (ENISA) publishes a series of good practice guides on the industrial systems security. The documents [63,64] propose measures focused on particular issues, both strategic and organizational and addressed to political decision-makers.

The National Institute of Standards and Technology (NIST) published a guide on the security of industrial systems [65]. Its content is very similar to ISO 27019. The Center for the Protection of National Infrastructure (CPNI) based in United Kingdom published a series of guides on the security of industrial systems [66]. They offer a high level vision by proposing strategic, managerial and organizational practices. The topics covered range from risk analysis to third party risk management and incident response. These guides are supplemented by documents which provide technical information on issues such as security audits of industrial systems. The international standard IEC/CEI 62645 [67] is the benchmark for the safety of industrial systems in the nuclear field. It emphasizes the fact that security measures must not conflict with operational safety measures. The international standard IEC/CEI 62351 [68] aims to develop the security of communications protocols used in the distribution of electricity (power grid), targeting dedicated protocols. The standard offers protection measures in accordance with the state of the art in terms of security (use of the TLS protocol, public key infrastructure, etc.). The American Gas Association (AGA) has published a series of guides called Cryptographic Protection of SCADA Communications [69]. These guides analyze the possibility of adding Hardware Security Modules (HSMs) to existing programmable logic controllers and SCADA to allow them to use cryptographic primitives. The Cyber Security Forum Initiative (CSFI) published a guide called CSFI ATC (Air Traffic Control) Cyber Security Project [70]. This

document offers a technical analysis of the risks and countermeasures targeting the field of air traffic control.

In the United Kingdom, the Rail Safety and Standards Board (RSSB) and the Department for Transport have published a guide called Rail Cyber Security Guidance to Industry [71], similar to the CPNI guides. This document remains superficial and does not deal in detail with the security technical aspects.

However, previous studies have not provided an in-depth classification of modern cyberattacks and their exploitation strategies. Moreover, there is a lack of realistic and pragmatic cybersecurity solutions against cyberattacks. Therefore, to the best of our knowledge, this paper provides the first in depth taxonomy of modern cyberattacks that targets IoT based critical cyber infrastructures coupled with realistic and pragmatic solutions inspired by the industrial experience of authors.

4. Modern Cyberattacks Taxonomy

Currently, industry-based critical IoT cyber infrastructures use advanced technologies to improve business assets. However, most of the deployed objects and applications are not designed to mitigate or prevent intrusions. Moreover, they are designed without any security mechanisms, which increases the surface and cyberattack vectors targeting these cyber infrastructures.

Therefore, critical cyber infrastructures are exposed to several cyber threats, including those inherited from the Internet and IoT as shown in Figure 4. In addition, such infrastructures can function as a springboard for the generation of new cyber threats and cyberattack vectors.

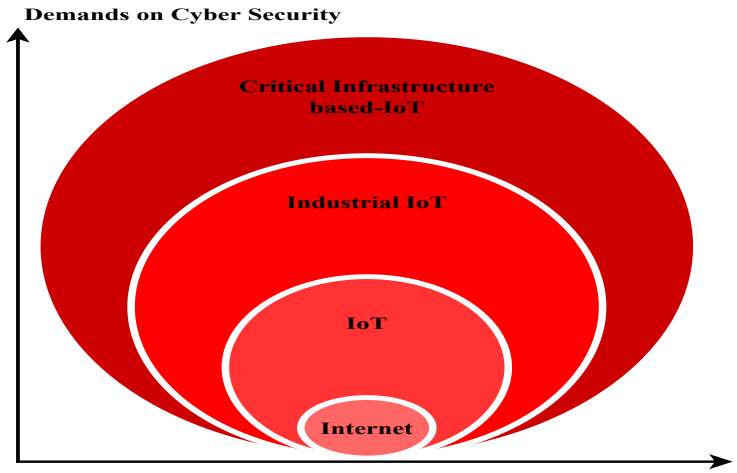

Figure 4. Top Cyber Security Demands.

A previous study [72] showed that 70% of IoT devices can be attacked easily. In addition, an increase in the number of attacks by 10% compared with 2017 (77.39%) has been observed, which evidences that cyberattacks are growing in number, intensity, severity, and sophistication. Figure 5 [73] presents dominant cyberattacks as of July 2020.

The sublime objective ensures the sustainable protection of health infrastructure (operations, patients, doctors and medical equipment), ICS/SCADA (industrial operations, PLC, RTU, industrial equipment), data and network, and preserves the continuity of services even if presence of cyber threats and cyberattacks. However, prior to discussing cyber vulnerabilities and potential cyber threats, it is rational to first identify the cyber assets of a target CPS. Figure 6 shows the cyber security landscape of critical cyber infrastructure.

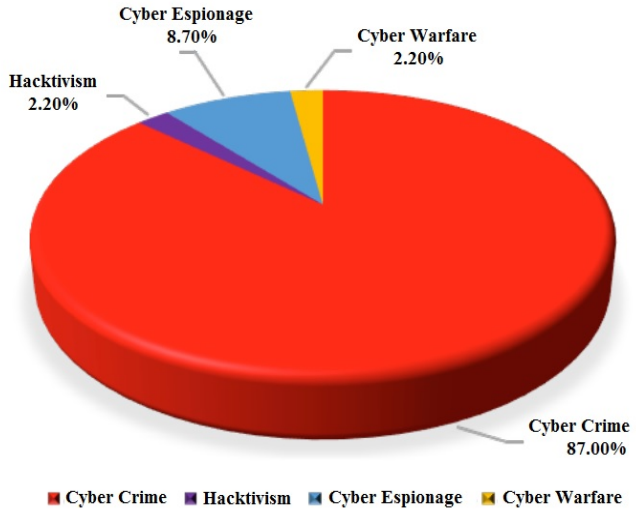

Figure 5. Dominant Cyberattacks as of July 2020.

4.1. Main Cyber Assets

Many risks can emerge in an IoT-based critical cyber infrastructure. In CPS environments, several catastrophic scenarios may occur if industrial/medical equipment suffers a denial of service attack or attempted privacy breaches when medical record/sensitive industrial information are intercepted. In addition, malicious actions, human errors, and fatal failures can lead to significant consequences or even loss of life. Hijacking medical/industrial terminals to create backdoors in CPS networks is the ultimate goal to take full control of the entire critical infrastructure. The primary assets that cyber attackers may exploit to incur serious damages in CPS environments are:

- Network Infrastructure;
- Information system;
- Remote Access;
- Medical/Industrial Equipment;
- Mobile Devices.

4.2. Main Cyber Threats

In cyber physical environments, the IoT facilitates the deployment of personal networks to control and monitor industrial process/clinical signs, particularly for the elderly. This facilitates remote monitoring of patients and provides solutions for the autonomy of people with reduced mobility. However, IoT-based CPS is a critical cyber infrastructure. IoT devices are frequently delivered in an unsafe state and do not offer security patches, which poses serious cyber threats to industrial/healthcare workers and hospitalized or non-hospitalized patients because these devices are often part of a botnet controlled remotely by an attacker. Consequently, these critical cyber infrastructures face numerous threats to industrial information system, industrial equipment, electronic health records and human lives in particular. Therefore, determining the baseline factors for cyber threats and cyber vulnerabilities is the first step to reducing cyber risks. Figure 7 shows the main cyber threats that can considerably affect this kind of critical infrastructure.

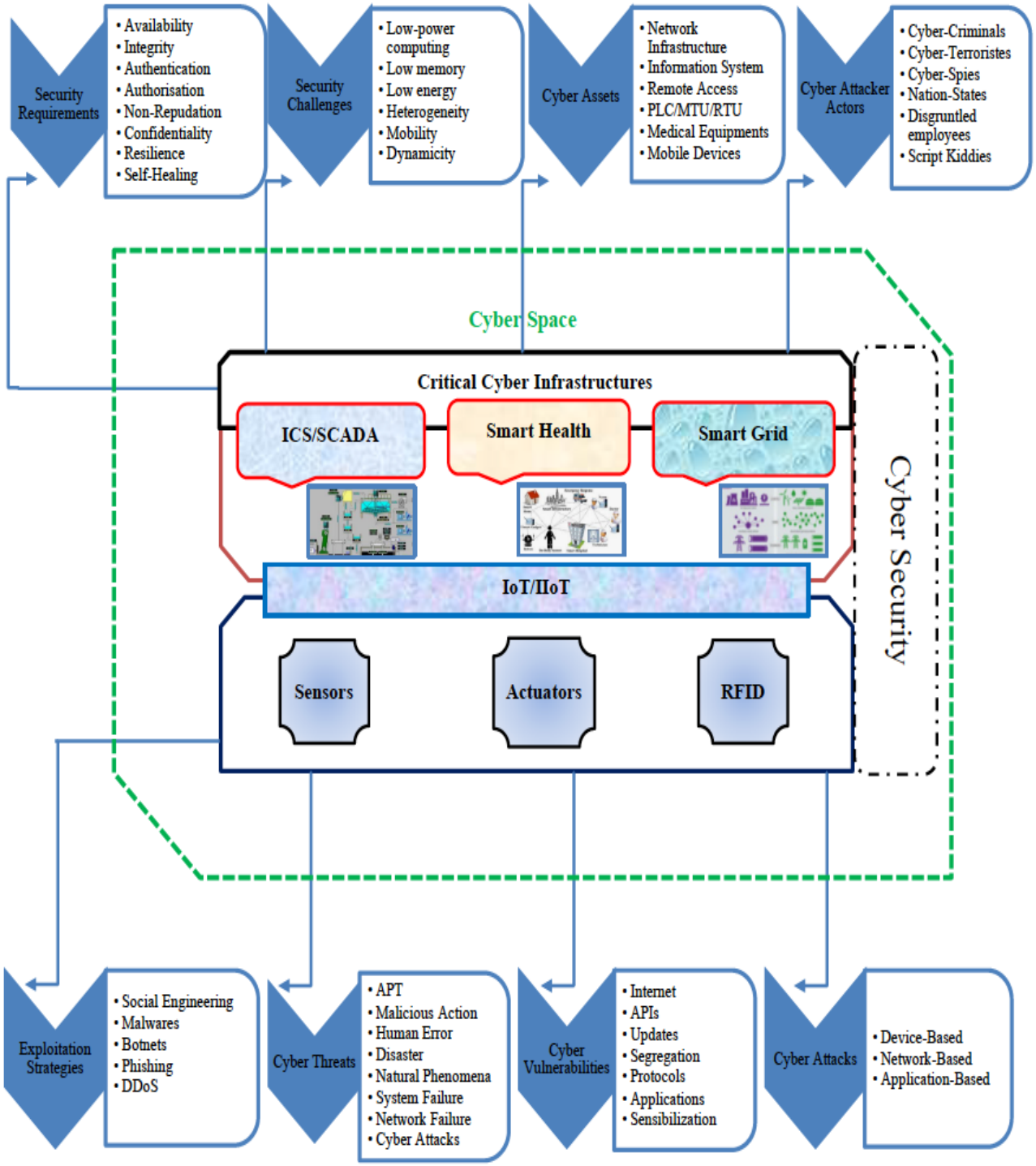

Figure 6. Cyber Security Landscape of Critical Cyber Infrastructure.

Figure 7. Major Cyber Threats impacting Critical Cyber Infrastructure.

4.2.1. Cyberattacks

In recent years, cyberattacks have grown in number (700 million in 2017) [74], intensity, severity and sophistication, and they advance faster than the development of defense techniques and controls. Modern cyberattacks are coordinated, invisible, transnational, and numerous, and this number is increasing constantly. Cyber attackers primarily use several tools in the following stages: reconnaissance and foot printing, scanning and enumeration, gaining access, maintaining access, and covering tracks. Wannacry, Mirai, NotPetya, SamSam, Memcached, Stuxnet, SolarWinds are large scope samples of large-scale and peerless cyberattacks. The deployment of the IoT in a critical infrastructure makes such infrastructures appealing targets for attackers. In the healthcare context, paralyzing emergency, cardiology, resuscitation, and blood transfusion services can have immediate and fatal consequences. In this context, according to the results of Vectra Networks' quarterly post intrusion analysis report in the first quarter of 2017, healthcare was the most targeted sector for cyberattacks [75]. The National Healthcare Service of the United Kingdom was among the victims in that year. No healthcare infrastructure is safe when it comes to international cyberattacks from multiple countries and organizations. The consequences of cyberattacks that target an IoT-based healthcare system can be severe, and they can cause shutdown of connected medical equipment, paralysis of health information systems, disclosure of sensitive medical data, financial losses and loss of life.

In the industrial control context, a large group of cyber attackers steal IT remote-access passwords through phishing attacks. These attackers eventually compromise the Active Directory Domain Controller, create new accounts for themselves, and give the new accounts universal administrative privileges, including access to ICS equipment. The attackers log into the ICS equipment and observe the operation of the ICS HMI until they learn what many of the screens and controls do. When the group attacks, the cyber attackers take control of the HMI and use it to misoperate the physical process. At the same time, co-attackers use their administrative credentials to log into ICS equipment, erase the hard drives, and where practical, erase the equipment firmware.

4.2.2. System Failures

System failures are critical inside industrial/medical environments. Such failures can be related to software that affects industrial/medical processes. A failing device with reduced capacity can significantly affect real-time data collection, for example, chemical,

gas, uranium, glucose and blood pressure monitoring. In addition, IoT sensors can be tampered with to provide false data. For example, the results can be extremely critical when connected turbines or thermic gas sensors are tampered with.

4.2.3. Network Failures

Most modern critical infrastructures heavily rely on telecommunication networks. Therefore, correct operations are important for the protection and propagation of incidents and failures. Thus, network failures are a major handicap in an IoT-based critical infrastructure. As IoT networks grow, their complexity increases and the risk of becoming unstable owing to network failures increases. Network failures can have negatively impact critical infrastructure and can spread to other infrastructures, which can result in serious consequences for the economy, public health and national security. In addition, many flaws hamper interconnected networks dedicated to critical infrastructure through the Internet and breaches that allow unauthorized users to access control systems, alter data, compromise critical elements, and interrupt vital operations. Compromising an IoT-connected device is an easy task [76], therefore, building a botnet network can be done quickly and efficiently by exploiting network vulnerabilities. Through such a vulnerable network whose main source is the connected object, critical equipment, for example, cardiology or radiology equipment can be altered easily, and the consequences can be fatal in the case of network failure because everything is connected to the Internet through a network.

4.2.4. Natural Phenomena

Owing to their disruptive or destructive impact, particularly on critical infrastructures, natural phenomena can also cause major incidents. Moreover, natural phenomena may affect the delivery of remote services, even if their impact did not target the infrastructure in itself. For example, the industrial infrastructure of a central or metropolitan network can be threatened by an earthquake, fire, or flood. Furthermore, no legal action can be taken to identify the culprits. In addition, penetration testing or forensic security investigation approaches are useless in such situations because these methods cannot achieve sufficient results. Therefore, it is imperative that vital functions be restored as quickly as possible to return to an acceptable level of functionality and avoid further risk.

4.2.5. Disasters

Are events that can damage the operations and vital activities of a critical infrastructure (i.e., industrial accidents, inadequate configuration, terrorism acts). A disaster can occur at any time, and we cannot know or predict the exact moment at which a disaster may occur. Thus, post disaster recovery with the anticipation of taking preventative actions like disaster recovery plan, disaster automated incident response, and resiliency, are the best actions to undertake, because in the case of a disaster, the critical infrastructure turns into extremely vulnerable and the damage is potentially dramatic for the well-being, the economy, and the nation.

4.2.6. APT

Advanced Persistent Threats (APT) [77] are organized advanced network intrusions with longer access that can stay undetected for a long period of time. Such attacks employ multiple technics and procedures using intelligence gathering and advanced hidden malware. The long duration of APTs limits the likelihood of detection. The objective of APTs is data exfiltration, espionage, or stealing sensitive and valuable data. More precisely, in the APT context, “advanced” refers to the full spectrum of connected objects, networks and infrastructure intrusion technologies with sophisticated techniques; “persistent” refers to a structured series of cyberattacks with a long term goal, external command/control, continuous interaction, and target monitoring; and “threat” implies that criminal operators coordinate orchestrated cyberattack actions. Essentially, APTs have some common characteristics, e.g., multi-vector and multistage cyberattacks, stealthiness, advanced evasion

technics, data exfiltration, espionage, zero-day attacks, encrypted payloads, not running if a sandbox is detected, and hiding payloads among normal objects.

4.3. Main Cyber Vulnerabilities

In general, critical cyber infrastructures face several types of cyberthreats and cyberattacks due to the exploitation of existing weaknesses and known/unknown vulnerabilities. According to the Global ICS CyberX report [78] 84% of industrial sites have at least one device that can be accessed remotely, 53% of infrastructure have obsolete OS such as Win XP, 40% of industrial sites have at least one direct connection to the public Internet, several machines and sessions are operational via easy passwords or by default. Before taking the appropriate steps to prevent, detect and mitigate CPS cyber threats, it is useful to better understand the cyber vulnerabilities that can potentially be exploited for harmful purposes.

4.3.1. Internet Exposition

In traditional CPSs, operations were limited to the factory without resorting to the Internet. With the diversity of industrial/medical operations, integration with other platforms is recommended. Some companies have connected their CPS or part of the infrastructure to the Internet. Thus, insecure connections can allow backdoor access to malicious party accounts to penetrate CPS environments and take control of their infrastructures. Furthermore, remote access is often allowed for maintenance purposes, which is a significant vulnerability especially when vulnerable protocols do not fulfil security policies that are implemented.

4.3.2. Interfaces/Passwords Breaches

As CPS integrates a large part of connected devices, sensors and actuators, most IoT objects are provided with insecure web/mobile interfaces, and do not allow modification of password by default. This weakness leaves them vulnerable to brute force attacks or dictionary attacks in order to force passwords cracking, compromise connected objects, industrial/medical devices and create backdoors. In addition, medical equipment and industrial PLCs are controlled and commanded remotely, and are administered by vulnerable environments such as HMI platforms equipped with unpatched Windows OS. Which can highly harm the operation and generate a prodigious volume of damages.

4.3.3. Update Lack

With the absence of secure updates, there is no guarantee that the security of IoT devices deployed within CPSs will be suitable. Indeed, while a device receives an update, it may be doped with a malicious code. Otherwise, security updates and patches address known vulnerabilities. However, modern cyberattacks exploit permissions and unknown vulnerabilities more than they exploit known vulnerabilities, which often raise problem to 0-Day attacks. In addition, security updates can be very expensive on CPS. Every change to the source code is potential threat to correct continuous and efficient operation of the physical industrial/medical process.

4.3.4. Low Segregation

Low segregation between Information Technology (IT) and Operative Technology (OT) environments is one of the common factors leading to compromise inside CPS. Poor access control can allow a connected machine to the computer network to reach a device on the CPS network, and a malware attack on the computer system can allow malware to easily spread to the OT configuration. Which can generate corrupted modifications, functioning disruptions or outright destruction on a large scale.

4.3.5. Weak of CPS Protocols

CPSs rely on the use of a variety of dedicated communication protocols. The original protocols used in CPS were not designed with security in mind. The same protocols are used

in the current CPS configuration. For instance, the Inter Control Center Communication Protocol (ICCP) has a vulnerability related to buffer overflow. The MODBUS protocol uses clear text communication, which can allow the attacker to listen for traffic. The MODBUS [79] protocol does not have proper authorization, which can lead to unauthorized actions such as updating the ladder logic program or stopping the PLC. It is also possible that MODBUS's requests are generated by non-legitimate applications. Distributed Network Protocol 3 (DNP3) [80] is primarily used for communications between SCADA master stations, Remote Terminal Units (RTUs), and Intelligent Electrical Devices (IEDs). Through a crafted DNP3 packet, remote attackers may be able to cause a denial of service, buffer overflow or buffer over-read if NDEBUG, otherwise assertion failure.

4.3.6. Weak of CPS Applications

Applications related to ICS and HMI are potentially vulnerable to the web or to heavy client-based attacks like SQL injection, malicious update injection or parameter manipulation. The lack of a strong and robust encryption protocol leads to the detection of credentials. A cross-site scripting attack can result in session hijacking as well.

4.3.7. Leak of Sensitization

In most cases, humans are the weakest link in the cyber security chain due to a lack of awareness. In fact, employees are often victims of social engineering, phishing, and spear phishing attacks. Sometimes a single click from the victim is enough to be compromised. From this compromised machine, an attacker can pivot further into the CPS by lateral movements.

4.4. Exploitation Strategies

Modern society is hyper-connected. Unfortunately, this does not reflect an idyllic world because entities attempt to exploit its vulnerabilities, cybercrime is proliferating and asymmetric warfare has become the norm. IoT-based critical infrastructures constitute as much of backdoors for cyber attackers who are rarely identified. Figure 8 shows the main exploitation strategies adopted by cyber attackers.

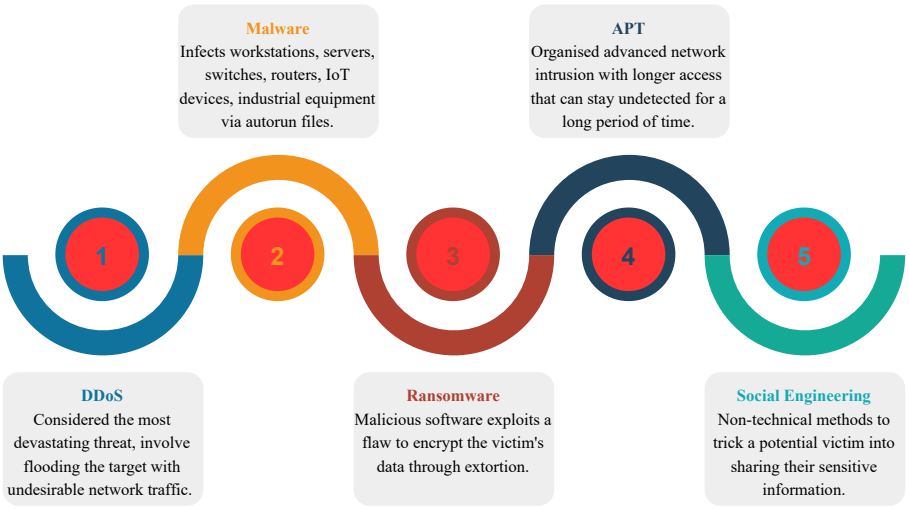

Figure 8. Exploitation Strategies.

Their modes of operation do not solely rely on the deployment of viruses. Moreover, cyber cyberattacks are organize and perform using various strategies, including social engineering, organizational failure, malware injection, vulnerability scanning, weakness exploitation, APTs, maintaining access, privilege escalation and covering tracks.

4.5. Common Cyberattacks impacting CPS Taxonomy

The ubiquity of communicating objects without physical protection and monitoring makes them easy targets for hardware attacks. In addition, the low power of connected objects makes them easy targets for software cyberattacks. Such items can be stolen, cloned, corrupted, and counterfeited. Thus, securing the vital functions in a critical cyber infrastructure is only possible if the cyber threats and cyber vulnerabilities are identified accurately. In other words, prior to implementing effective and efficient countermeasures, it is important to identify the attack methods accurately. In this context, a taxonomy of dangerous and probable cyberattacks is shown in Figure 9.

4.5.1. Malware

The COVID-19 pandemic is not the only threat faced by humanity and cyber health infrastructures are overwhelmed. Malware attacks have increased as the pandemic has expanded. Malware is a special type of malicious software to obtain data through extortion. Here, a cyber attacker exploits a flaw to encrypt the victim's data. Malware is spread via email attachments, infected applications, and compromised websites. There is a phenomenal amount of unwanted or malicious software. In fact, Malware is a very generic term that encompasses all unwanted programs that interfere with the productive use of a computer, network, mobile devices, and connected objects. But under this name hides very different sub-families. Among the most used to harm critical cyber infrastructure: ransomwares, backdoors, stealer, rootkits, and droppers. Recent malwares are becoming autonomic (self-moving and rapid-propagation) with advanced features. Cryptomalware typically prevents an organization from accessing elements of its critical systems and uses different methods to extort money. The most well-known ransomware are Cryptolocker, Cryptowall, TeslaCrypt, and Wannacry.

WannaCry [81,82] and Samsam [83] are representative examples for ransomwares. If a hospital cannot access its health information system, patient care could be delayed or compromised. Here, establishing backup plans, healthy recovery points, and disaster recovery strategies are essential to deal with ransomware attacks. Ransomware infects an ICS workstation, and medical servers. It spreads via autorun files on network shares, USB drives, and known network vulnerabilities. The ransomware spreads for several days before triggering the encryption process. Multiple machines on both IT and ICS networks are thus infected. Authors of autonomous ransomware can be very sophisticated cyber wise, producing malware that can spread quickly and automatically through a network while evading common antivirus systems and other security measures. The malware exploits known vulnerabilities that have not yet been patched on the CPS network, encrypts the engineering workstation, and spreads to most Windows hosts in the CPS. Most Windows hosts in the industrial network are thus encrypted by the attack, shutting down the control system. The impaired control system is unable to bring about an orderly shutdown. Within a few minutes, the plant operator triggers an emergency safety shutdown.

4.5.2. Session Medjacking

Currently, cyberattacks can take several forms and adopt offensive operation methodologies to compromise a target. One new form in the healthcare context is session medjacking, which poses a serious threat to all session key establishment schemes in a health system. Session medjacking relies on the use of a valid session of a physician, nurse, surgeon, or patient to gain unauthorized access to information in a health database or create backdoor access. With medjacking, simple authentication via login systems without session key generation is not sufficient to guarantee security. The session key must be refreshed after each session and should be secured using a one-way hash function such that the adversary cannot derive another session key.

4.5.3. Denial of Service

Denial of service attacks attempt to disrupt the operation of a single service or an entire system by rendering it unavailable and unusable. Such attacks involve flooding the target with undesirable network traffic or sending data that trigger a crash. Thus, denial of service is considered the most devastating threat within an IoT-based critical infrastructure. With the tremendous growth and implementation of connected objects, IoT-based critical infrastructure can have prolonged periods of downtime owing to the unavailability of vital services. In industrial Control System/SCADA context, RTUs are connected to MTUs via various forms of communication. A cyber attacker can interrupt communications between RTU and MTU through denial of service attacks. In this case, the MTU will not be able to acquire data from several RTUs because the converted analog signals by the RTUs cannot reach the control centers.

4.5.4. Network Denial of Service

Another compromised maneuver is based on the harming of the routing table at the IoT gateways, which leads to congestion and possibly denial of services. CPS is based on the use of several communication technologies, including IoT networks which is a heterogeneous network of constrained devices connected to each other. The 6LoWPAN protocol is a communication protocol that provides minimal consumption of resources and high data capacity. However, 6LoWPAN networks are vulnerable to denial of service attacks from compromised connected objects to flood critical ICS and healthcare servers. Routing Protocol for Low Power and Lossy networks (RPL) is a distance vector routing protocol standardized for low power lossy IoT. The RPL could be vulnerable to routing attacks following a compromise of any node in the CPS. The root node in the Destination Oriented Directed Acyclic Graph (DODAG) tree is a single point of failure in the RPL topology. To this end, several malicious nodes by coordination can lead to distributed denials of services. RPL Flood, 6LoWPAN Flood, IoT Gateway Flood attacks negatively affect the transmission of industrial/medical data, and consequently generate critical destruction.

4.5.5. Transport Denial of Service

The transport layer is responsible for end-to-end data communication. Attacks in this category mainly use hijacking via TCP or UDP protocols. TCP is a connection-oriented protocol, which implies that a three-way handshake mechanism is required. That said, a cyber attacker after having spoofed the addresses of the victim nodes, can send a significant number of SYN packets (synchronization request) to industrial servers, historian servers, electronic health record servers. Upon receipt of SYN-ACK packets from industrial/medical servers to spoofed nodes, industrial/medical servers would not receive any ACK-type packets in return. This implies that semi-open connections are created, resources are mobilized, and other connections are pending. This results in a buffer overflow and possibly denial of service as resources are exhausted and the servers are unable to respond or accept new legitimate connections. The denial of service mode of operation, can undertake a variety of implementation via the TCP protocol, among others: SYN flood, TCP-ACK flood, TCP-ACK & PUSH-ACK flood, TCP-FIN and RST flood. These attacks multiply from a network of connected objects as the cyber attacker possesses an army of connected objects useful for launching denial of service attacks targeting critical cyber infrastructure.

4.5.6. Application Denial of Service

The Constrained Application Protocol (CoAP) is an application protocol designed as a replication of HTTP for IoT devices. The CoAP protocol is based on the UDP protocol and follows a request/response model, which makes it particularly vulnerable to amplification attacks. An attacker could send a malformed CoAP packet to a given device in the CPS. Through an exploit, the attacker could force the CoAP server to shut down, interrupt IoT communications and potentially cause denials of service of vital industrial activities. Moreover, the DNS amplification attack is based on the reflection of a significant number

of compromised connected objects with a wide scope. To this end, an attacker attempts to exploit open DNS resolvers to overwhelm industrial/medical servers with a large amplification factor, causing collateral damage to all legitimate CPS users. Thus, despite the amplification generated, the attack makes the critical cyber infrastructure inaccessible and to complicate the task of the defense mechanisms, in particular because the attack is carried out in rebound.

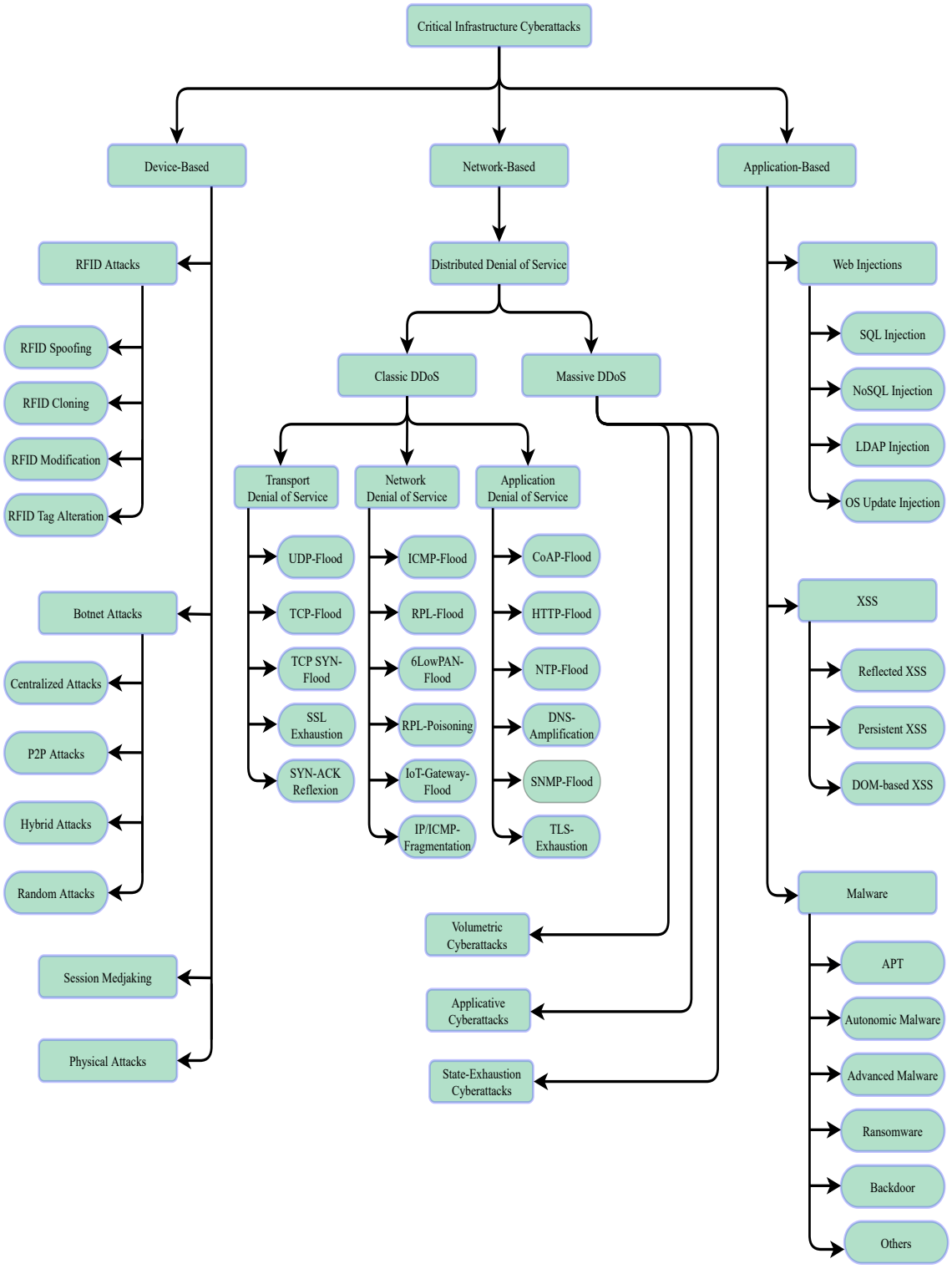

Figure 9. Taxonomy of Top Cyberattacks targeting Critical Cyber Infrastructure.

4.5.7. RFID Attacks

Radio Frequency Identification (RFID) is a contactless communication technology, making it possible to store and record data on a medium and to retrieve it remotely. RFID system [84] are extremely useful and diverse in IoT environments. Such systems can provide decision-makers with valuable data in a timely manner and can help improve outcomes. RFID systems can also track and identify the date of things. However, they are an excellent source of information. Furthermore, RFID systems have several vulnerabilities that can be exploited. A simple interrogation of an RFID tag can reveal its identifier, which will be easy to reproduce and clone. The attacker can spoof an RFID tag, intercept the information exchanged between the reader and the tag, deactivate RFID tag, perform malicious traceability, and finally shutdown an entire RFID system. Many compromised and replicated nodes can be placed in different locations of cyber physical system in order to cause an inconsistency. This cloning maneuver allows the attacker to hijack behavior, inject false data and consequently disrupt the functioning of CPLs, medical equipment, MTUs and RTUs.

4.5.8. Web Injection

In the broad sense, web injection attack involves providing untrusted input to a program. This entry is processed by an interpreter as part of a command or a request. To this end, the attacker injects code written in the language of the application, this code will be used to execute operating system commands in order to gain more privileges and compromise the web server. Critical cyber infrastructures are subject to the injection of false information, corrupted data, codes or updates. For this purpose, medical equipment, industrial controllers, CPS applications are involved. Medical database server, industrial IS infrastructure server or external website constitute the main assets. Thus, cyber criminals can manipulate, steal, modify, destroy important data, escalate their privileges or take control of PLC, medical, industrial equipment, by exploiting the security vulnerabilities of a database, operating system, website or application by injecting malicious code. In addition, the operators of legitimate requests in an industrial or cyber health physical system are obliged to manipulate data and enter information. The input fields used are targeted by cyber criminals to inject malicious scripts, sent to various applications and executed directly on the corresponding databases. These cyberattacks are highly achievable, mainly due to insufficient input validation, and the consequences are potentially harmful as many vital operations are carried out by the application within a CPS. Web injection can be carried out by exploiting flaws such as modifying the expected behavior of Lightweight Directory Access Protocol (LDAP) request, protocol designed to facilitate the search for active directory objects within a fairly large network infrastructure like CPS, in order to insert control characters, because LDAP queries involve the use of special control characters. Web injections can also be combined to write arbitrary files on industrial, medical servers via SQL, NoSQL instructions whose objective is to bypass authentication, disclose industrial secrets, industrial/medical data manipulation and generate denial of service of the CPS system.

4.5.9. XSS

Cross Site Scripting (XSS) cyberattacks pose a frightening threat in CPSs. These attacks are primarily performed by injecting arbitrary scripts such as JavaScript or Ajax into a legitimate web application or trusted website because data can be transferred without verification. The injected script will be executed on the victim's machine through his/her browser. Consequently, this flaw will allow the cyber attacker to access session tokens, cookies and stored sensitive information (e.g. trade secrets), install Trojans or execute malicious code. XSS cyberattacks can be reflected (the malicious script is reflected in a response that includes the input sent to the server as a search result or error message); persistent (the injected script is permanently stored on the target CPS servers. As soon as the browser sends a data request, the victim extracts and executes the malicious script from

the server) or Document Object Model-based (DOM-based), (is a structure to represent a document in a browser. The attack will take place when a JavaScript function is modified by a request that can be controlled by attacker).

4.5.10. Botnet Attacks

Basically, a botnet, or network of infected machines called zombies (that can be IoT devices, GPS terminals, IP cameras, servers, computers, switches, routers, etc.), is a set of computer resources capable of performing ordered operations, via a computer network, by a command and control infrastructure. In a cyber security context, a botnet refers to a network of a large number of machines controlled without the knowledge of their owners, capable of carrying out coordinated offensive actions, as the case of the following bots: (Conficker, Mariposa, Generic, Zeus ..). The IoT has become an integral part of CPS. This implies that the physical cyber ecosystem is no longer isolated, but rather very open to the outside, and its architecture is highly distributed. Basically, the IoT is a set of sensors, actuators, RFID ... etc. This army of connected objects is safe from the attacker in order to form remotely controlled and commanded IoT botnets, able to generate massive data traffic to overwhelm a target or crash a vitally important operation in critical cyber infrastructure. But also the dissemination of malicious code. A botnet is a set of compromised machines transformed into zombies, embedding malicious code in order to divert all possible resources deployed in a CPS. Botnets propagate through connections as legitimate traffic, confusing monitoring and detection tools. The explosion in the number of connected objects is helping to offer new efficiencies in the structuring of botnets. Mirai, QBot, known as Bahtile and Torii, are great examples of showing IoT's weaknesses. The botnet structure can be centralized, distributed, hybrid, or random. Connected object botnets are made up of personalized systems, often with limited resources and without protections. Which allows the attacker to have an efficient operating mode to build and execute massive cyberattacks targeting critical cyber infrastructure.

4.5.11. Insider/Physical Attacks

This is a moderately sophisticated attack. CPS technicians tend to have a good knowledge of how to operate control system components to bring about specific goals, such as a shutdown, but less knowledge of fundamental engineering concepts or safety systems that are designed into industrial processes. A disgruntled CPS technician steals passwords by "shoulder surfing" other technicians, logs in to equipment controlling the physical process using the stolen passwords and issues shutdown instructions to parts of the physical process, thus triggering a partial plant shutdown. In addition, this class of incident is most often able to cause a partial or complete plant shutdown. More serious consequences may be possible, depending on the insider and on details of the industrial process.

4.5.12. Massive Distributed Denial of Service

It is an extension of an ordinary denial of service attack. When many nodes are involved in an attack to deny service to the same target, the attack is called a distributed denial of service attack (DDoS). The attack sources correspond to infected nodes called zombies controlled by a botnet through a command and control server (C&C) [85]. A botnet is a number of IoT-connected devices, each of which is running one or more bots. IoT botnets can be used to perform massive DDoS attacks. The communication between IoT infected nodes or bots through master nodes or C&C servers is either centralized or peer to peer. DDoS attacks, which can be volumetric or involve amplification, are one of the most severe existing network attacks [85]. DDoS occurs when the action involves a network of infected machines and connected objects (zombies) to interrupt services, which implies that servers, switches, routers, sensors, actuators, RFID tags [86], and IoT-gateways are affected. In addition, industrial equipment and programmable logic controllers can be hi-jacked and compromised as botnets. The distributed denial of services can generate a huge

amount of network traffic, for example, 1 Tbps, which is more than sufficient to disrupt all ICS/health infrastructures as well as the information systems of all interconnected clinics. On hospital platforms, the main assets targeted by DDoS attacks include: the data center, critical network equipment, processing servers, clinical network information systems, network medical devices, connected health objects and the entire hospital infrastructure. If at least one health data center critical server is targeted, then multiple critical services and resources will be unavailable, for example, local and remote access to remote health records. When this occurs, it becomes easy to amplify the disruptive traffic. DDoS attack can have extremely harmful consequences, particularly for patients with chronic diseases, those scheduled for surgical interventions and patients who are undergoing an actual surgery. Mirai [87–89] and Memcached [90] are specific samples of this type of cyberattack. In addition, volumetric DDoS attacks are designed to massively overwhelm the capacity of critical infrastructure and even centralized or distributed industrial equipment with significantly high volumes of malicious traffic. These DDoS attacks attempt to consume bandwidth either within the target network/service or between the target ICS network/service and the rest of the Internet. State-exhaustion DDoS attacks are primarily focused on removing underlying services deployed within industrial infrastructure. This can involve an attack targeting DNS name servers with invalid name queries, causing increased load on DNS server, and disruption of services. As the name suggests, these DDoS attacks target stateful devices such as next generation firewalls in an attempt to populate TCP state tables with bogus connections. These DDoS attacks are typically used by determined attackers who monitor and adjust their attacks for maximum impact. This means that these attacks will primarily be launched using discrete smart clients, typically IoT devices, and cannot be spoofed. Application DDoS attacks are designed to attack the application itself, focusing on specific vulnerabilities or issues, which prevent the application from delivering content to the user. Applicative DDoS attacks are designed to attack specific industrial applications, the most common being web servers, but can include network such as large scale routing services, for example Border Gateway Protocol (BGP). These DDoS attacks are typically low to medium in volume because they must conform to the protocol used by the application, which often involves protocol negotiations and application compliance.

4.6. Cyber Attacker Actors

The specific sources of cyber threats targeting critical cyber infrastructure primarily include the following:

(1) Script kiddies: Script kiddies are novices who use existing cyberattack tools to hack vulnerable objects, computers, systems, and networks. By engaging in such activities, they aim to earn money or boost their egos.

(2) Cybercriminal Organizations: Criminal organizations engage in illegal activities, such as denial of service attacks and ransomware infections, to disrupt services and steal data, including state secrets.

(3) Nation-states: State-sponsored cybercriminal activities target enemy nations to disrupt the victim nation's economy or critical infrastructure. Such activities may result in death, disruption of state-sponsored programs, and may even involve attempts to overthrow the government.

(4) Cyberterrorists: Cyberterrorists attempt to cause nationwide losses and major disruption of critical societal infrastructure, such as power system blackouts.

(5) Cyber-Spies: (including business competitors). Cyber-spies steal trade secrets to gain an unfair business advantage.

(6) Disgruntled Employees: Employees who are stressed and unhappy with their jobs, have disputes with management, or who are motivated by other exacerbating factors attempt to cause financial or reputation losses to the organization by executing cyberattacks against company resources.

(7) External Cyber Attackers and Insider Threats: Experts with skills and a solid grasp of IT resource functioning as well as human behavior attempt to exploit vulnerable systems

and gain (mainly financially) from such acts or simply disrupt the normal operations of the organization.

4.7. CPS Security Requirements

One of the best ways to get into a CPS is by exploiting its IT infrastructure. Hence, it is more efficient to take advantage of IT to access OT. In fact, Cyber physical systems are specific in terms of the properties they require. Most systems focus on the properties set by the confidentiality, integrity and availability (CIA) triad. Cyber physical systems follow this trend with more focus on availability, integrity, authenticity and other required properties. The properties desired for cyber physical system are:

4.7.1. Availability

It ensures that there is no failure in a system during intended periods of use (potentially all the time). Indeed, cyber physical systems generally require above all being profitable and any interruption of service is most often a loss of earnings for the operator. It goes without saying that in the case of so-called critical cyber infrastructure, shutdown can have serious consequences for humans and the environment. Availability is also a property of liveliness, ensuring that a property will be true from a certain stage of execution. Therefore, in the case of CPS, availability is also intended to ensure that an entity requesting a resource will ultimately obtain it on time. DDoS attacks are strategic cyberattacks that violate availability. In this context, connectivity, critical operations, PLCs, industrial/medical equipment are important resources that must be available 7 days a week and 24 h a day within critical cyber infrastructure and protected against denial of service.

4.7.2. Authenticity

It is often called abuse-of-language authentication. It aims to ensure that an entity (a human/component) is who it claims to be. The method to guarantee authenticity can be done on (i) what we know (a password), (ii) what we have (a certificate, an authentication token), (iii) what we are (biometrics), or (iv) information on the context (for example where we are). This method of ensuring authenticity is called authentication. Authentication based on several factors described previously is said to be strong. This property makes it possible in particular to control access, which prevents an entity from performing actions that it is not authorized to do. It is also particularly important in critical cyber infrastructure because each action in the logical world has a potentially destructive consequence in the physical world. It is therefore necessary to guarantee that only authorized entities can send orders within the limit of their authorization.

4.7.3. Integrity

It is the preservation and assurance of the consistency of data over time. This definition can vary a lot depending on the context. In particular, two meanings arise in the case of the integrity of messages transferred over a CPS network. On one hand, protection against accidental changes can be guaranteed, in particular by using error detection mechanisms such as cyclic redundancy or CRC. On the other hand, integrity in the cryptographic sense aims to protect industrial/medical data against intentional modifications by an attacker. It requires the use of cryptographic primitives such as hash functions or signatures. While also protecting against accidental modification, cryptographic integrity costs more in terms of message size and time. Partly for this reason, critical cyber infrastructures have historically relied on error protection. Their physical isolation from the outside world has already provided them with sufficient form of protection to focus on errors and failures.

4.7.4. Non-Repudiation

It is the inability of an agent to deny that he/she has taken an action or that an action has been taken against him/her. For example, the inability of an industrial operator or medical staff (surgeon, nurse, administrator ... etc.) to deny that he/she sent a message

if it is causing a problem. It could also be the inability of the operator to deny receiving any information about the process. This property is essentially based on communication protocols and is therefore currently happens very rarely (or even completely absent) in critical cyber infrastructure.

4.7.5. Dependability

Authentication, integrity, confidentiality and non-repudiation are so-called security properties. They have the particularity of being verifiable on a given trace (as opposed to liveliness properties such as availability [91]. However, security is not limited to safety checks, in particular operational safety aims to guarantee specific properties of the logic application of the CPS. For example, checking that an insulin pump never exceeds a certain dose for a given patient. It is traditionally properties of this type that cyber physical systems are built to verify by default. However, they are rarely verified in the presence of a cyber attacker. Safety of operation is also often opposed to security and it is sometimes difficult to reconcile both.

4.7.6. Traceability

It ensures that actions or attempted actions in the CPS are kept in a log. The traces must also be exploitable by providing, for example, the reasons for which an action is refused. Certain security properties are often rarely required for critical cyber infrastructures and they happen when data is present (for example electric meter readings).

4.7.7. Anonymization

It consists of modifying data in order to prevent any link with its owner. This property is specifically required in the presence of customer data (provided that this link is not useful for the CPS). Historically, few industrial systems manipulate customer data, making this property marginal. However, due to the increase in the interconnection of systems and the growing distrust of users with regard to data collection, anonymization has become an important property in industrial systems. It is also increasingly highlighted or even imposed by regulations.

4.7.8. Confidentiality

It ensures that only authorized persons have access to information intended for them. This property is infrequent in CPS, because like integrity, it requires the use of cryptographic primitives which are computationally expensive. In addition, it requires that all the elements analyzing the state of the physical process be able to access the content of the messages exchanged, which can be complicated when they are encrypted. Confidentiality is nevertheless starting to be a necessary property, for example when sending passwords (introduced by recent communication protocols) and specific data over the CPS network.

4.7.9. Resilience and Self-healing

Given the increased sophistication of attackers, medical / industrial devices are now being attacked at deeper levels in critical cyber infrastructure. Therefore, it is imperative that cyber security approaches include self-healing and resilience as security requirements. These fundamental properties enhance protection against 0-day attacks that cannot be detected by traditional security solution that can be infected like SolarWinds. Moreover, the detection of abnormal behavior becomes faster and with less false positives.

4.8. Realistic Cyber Security Guidelines

The IoT can only succeed when there is acceptable security for objects and IoT communication networks. A strong policy that prevents malicious objects or unauthorized actors that can intercept or alter medical/industrial data is essential. Thus, we need to create a new lightweight and robust mechanism that ensures security in CPS environments.

The sustainability of the security of an IoT-based critical infrastructure requires multiple levels of security, ranging from physical to operational security. Therefore, to obtain secure services in each level, it is necessary to concentrate on the following security requirements:

The system must provide strong authentication to allow an IoT device to guarantee the identity of the user. In cyber health context, the system must maintain high availability to ensure the survivability of internal and external health care services to authorized parties. Even in the event of a denial of service attack, the system must provide a minimum of services. In addition, the system must ensure that an opponent does not change medical data sent or received in transit and the integrity of stored medical data and content are not compromised. Adequate confidentiality requirements must be implemented to ensure that unauthorized users do not access medical information. If confidential messages are intercepted, their content must not be disclosed. The system must be resilient, if interconnected health/industrial IoT devices are compromised, a security system should protect the network, critical nodes, and the information system from any type of aberration. Finally, the system must include a self-healing mechanism that allows medical/industrial devices in an IoT-based critical infrastructure network to collaborate and provide continuity of service even if the presence of a set of crashing devices.

When we consider DDoS attacks [92], we must also consider APTs [93]. If both types of attacks target IoT-based critical cyber infrastructure simultaneously, the consequences are devastating. Typically, IT professionals consider the source of the problem to be operating issues of routers or servers that cannot respond because over time traffic returns to the nominal state. This is attributed to the state of security being changed. In other words, the current security solutions are parametric regardless of the existing security equipment, for example, WAF, load balancer, firewall, and UTM devices. Regardless of the constructor, the security solutions are statistical and state-based. If an APT occurs in IoT-based critical cyber infrastructure, and if active and critical elements are saturated, there is no guarantee that they will continue to function normally and use cyberattacks as a smoke screen.

Moreover, no existing firewall can block all attacks, no IDS can detect all intrusions, and no antivirus can eliminate all malware. In other words, no security countermeasure can handle all cyberattacks because these can come in different forms and ways.

Furthermore, we cannot concretely protect against what we cannot see. Therefore, it is imperative to build a visibility plan by identifying the most important assets, preparing a corpus to generate logs, capturing relevant real-time flows, and centralizing and correlating to develop scenarios to counter cyberattacks with resilient and intelligent cyber security strategies.

Further, it is obvious that the establishment of good conduct guides making it possible to understand the cyber security issues around critical cyber infrastructure are necessary. To this end, it is essential that:

- Security must be integrated natively;
- The implementation of proactive measures to prevent cyberattacks, avoid disruption of services and vital importance operations, real time and fast reaction to emerging cyber threats;
- Segmentation of ICS/SCADA, cyber health network architecture in order to separate HMIs from PLCs, supervision systems, remote control units and communication infrastructures;
- Adoption of a defense-in-depth strategy with security layer in all level of critical cyber infrastructure;
- Artificial intelligence is a good way for predicting new families of 0-day malware, ransomware and unknown vulnerabilities;
- Resilience and self-healing incident response.

As more vulnerable IoT devices come online, they create a very large attack surface, which increases the potential scale and severity of massive DDoS attacks targeting critical cyber infrastructure. IoT device manufacturers, service providers, standardization bodies,

regulators and users should be aware of the potential risks. Therefore, building a secure and reliable ecosystem, based on a collaborative security approach is essential.

As Bruce Schneier said: *"If you think technology can solve your security problems, then you do not understand the problems and you do not understand the technology"* [94]. The ecosystem is based on a very complex interconnection. Therefore, The IoT infrastructure's security should not be concerned with only connected components. Thus, it includes software, platforms, communication supports, services and storage and processing centers in the cloud, where political decision-makers have an important role in the implementation of strategic principles and effective regulations, helping to better secure the IoT.

Cyber security of critical cyber infrastructure is a global concern, and must be seen through a collaborative approach in depth, included at all levels and on an ongoing basis. On the other hand, there is a need to promote the use of certification techniques for risk assessment, investigation, cyber threat intelligence in order to support the analysis of security risks in anticipatory manner.

The security audit and penetration testing must be periodic and compatible with IIoT and CPS, in order to identify specific vulnerabilities at the appropriate time, to mitigate potential threats in real time and to minimize cyber risks as much as possible.

Recent advances in artificial intelligence, especially machine learning and deep learning techniques, can be leveraged to significantly contribute to the cyber security of critical cyber infrastructure through the emergence of more resilient, robust and reliable models.

5. Discussion

Industrial/medical equipment's based IoT play fundamental role for critical cyber infrastructure. However, these devices face serious vulnerabilities and are accessible on the internet, which exposes them to all kind of attacks. Periodically, the zero-day vulnerabilities are discovered and published under Common Vulnerability Exposure (CVE) report. Moreover, the complexity, heterogeneity, and large-scale CPS networks make the cyber security equation more complicated. Therefore, many cyber security challenges are faced when designing solutions to protect critical cyber infrastructure. The lack of the visibility of the cyber space as well as holistic and resilient approaches are considered as the main obstacles to maintaining and managing efficiently cyber security of critical cyber infrastructure. Thus, the primary goal is to reduce the cyberattack surface vector and minimise the cyber risk caused by potential cyber attacker actors.

6. Conclusions

Currently, corporate institutions and states have substantial digital assets that are connected to global technological advanced networks. At the same time, cyber attackers are becoming increasingly sophisticated, operate more aggressive, furtive and can bypass checkpoints and defense controls. Typically, critical cyber infrastructures are complex, large-scale, fully distributed, and run in open contexts. Moreover, CPS based IoT systems generate huge amounts of data that contain highly sensitive information. Thus, an IoT-based critical cyber infrastructure is vulnerable to a range of significant cyber threats and malicious activities that could be the basis for the generation of new types of massive cyberattacks that could cause significant consequences such as financial losses, welfare losses and loss of life. As a result, cyber security is a fundamental concern for the evolution and proper functioning of such ecosystems. Therefore, rigorous research is required to develop resilient cybersecurity approaches, models, and technologies to provide effective responses to new cyber challenges. This study presents a critical view of the most recent cybersecurity issues for cyber critical infrastructure, probable cyber threats and cyber vulnerabilities, the main exploitation strategies used by cybercriminals, a new taxonomy of modern cyberattacks impacting cyber critical infrastructure, and some realistic recommendations and best practices to enhance cybersecurity solutions.

Current and Future Developments: Cybersecurity issues targeting IoT-based critical infrastructures significantly impede the evolution and rapid deployment of this flagship

technology. These kinds of issues cannot be addressed by conventional security protocols and existing solutions because most of them do not ensure acceptable performance and are not adapted to cater to the capacity of objects that are generally extremely limited in terms of computation, storage and energy. To address these issues, the state-of-the-art of actual security solutions must be changed. In the future, we will investigate data science and advanced AI techniques to provide a new model that is more comprehensive, strategic, holistic and persistent to deal with massive cyberattacks.

Author Contributions: Conceptualization, A.D.; methodology, A.D. and S.H.; formal analysis, D.S.; investigation, A.D.; resources, A.D.; writing—original draft preparation, A.D.; writing—review and editing, A.D. and S.H.; visualization, A.D., S.H. and D.S.; funding acquisition, S.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge the anonymous reviewers for their helpful and insightful comments.

Conflicts of Interest: The authors declare that there are no conflict of interest regarding the publication of this paper.

Abbreviations

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
IIoT	Industrial Internet of Things
CPS	Cyber Physical System
ICS	Industrial Control System
SCADA	Supervisory Control And Data Acquisition
DCS	Distributed Control System
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
IED	Intelligent Electronic Device
CIM	Computer Integrated Manufacturing
OP	Operative Part
OT	Operative Technology
IT	Information Technology
HMI	Human Machine Interface
RFID	Radio-Frequency Identification
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
RPL	Routing Protocol for Low power and Lossy networks
DODAG	Destination Oriented Directed Acyclic Graph
CoAP	Constrained Application Protocol
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
DNP	Distributed Network Protocol
BGP	Border Gateway Protocol
DNS	Domain Name System
SDN	Software-Defined Networking
WAF	Web Application Firewall

UTM	Unified Threat Management
APT	Advanced Persistent Threat
DoS	Denial of Service
DDoS	Distributed Denial of Service
XSS	Cross Site Scripting
DOM	Document Object Model
CC	Command and Control
NIST	National Institute of Standards and Technologies
ENISA	European Network and Information Security Agency
CPNI	Center for the Protection of National Infrastructure
CSFI	Cyber Security Forum Initiative
RSSB	Rail Safety and Standards Board
ICCP	Inter Control Communication Protocol

References

1. Gungor, V. C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G. P. A survey on smart grid potential applications and communication requirements. *IEEE Trans. Ind. Informatics* **2012**, *9*, 28–42.
2. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142.
3. Bera, S.; Misra, S.; Rodrigues, J.J. Cloud computing applications for smart grid: A survey. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 1477–1494.
4. Cai, H.; Xu, B.; Jiang, L.; Vasilakos, A.V. IoT-based big data storage systems in cloud computing: Perspectives and challenges. *IEEE Internet Things J.* **2016**, *4*, 75–87.
5. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646.
6. Hu, P.; Dhelim, S.; Ning, H.; Qiu, T. Survey on fog computing: Architecture, key technologies, applications and open issues. *J. Netw. Comput. Appl.* **2016**, *98*, 27–42.
7. Hermann, M.; Pentek, T.; Otto, B. Design principles for industries 4.0 scenarios. In Proceedings of the IEEE 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016.
8. Lee, J.; Bagheri, B.; Kao, H. A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23.
9. Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Informatics* **2014**, *10*, 2233–2243.
10. Schneider, S.; Geng, H. The industrial internet of things (IIoT). In *Internet of Things and Data Analytics*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2017.
11. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Informatics* **2018**, *14*, 4724–4734.
12. Centenaro, M.; Vangelista, L.; Zanella, A.; Zorzi, M. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wirel. Commun.* **2016**, *23*, 60–67.
13. NIST Framework for Cyber-Physical Systems. Release 1.0, NIST Cyber Physical Systems Public Working Group 2016. Available online: http://www.nist.gov/ (accessed on 1 November 2020).
14. Galloway, B.; Hancke, G.P. Introduction to Industrial Control Networks. *IEEE Commun. Surv. Tutorials* **2013**, *15*, 860–880.
15. Stouffer, K.; Falco, J.; Scarfone, K. Guide to industrial control systems (ICS) security. *NIST Spec. Publ.* **2011**, *800*, 16.
16. ENISA, ICS SCADA. Available online: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada (accessed on 22 December 2020).
17. Cisco Visual Networking Index: Forecast and Trends, 2017/2022 White Paper. Available online: https://cloud.report/whitepapers/cisco-visual-networking-index-forecast-and-trends-2017-2022/9017 (accessed on 17 October 2020).
18. Total Number of Device Connections by 2025. Available online: https://iotanalytics.com/state-of-the-iot-2020-12-billion-iot-connectionssurpassing-non-iot-for-the-first-time/ (accessed on 17 October 2020).
19. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Networks* **2010**, *54*, 2787–2805.
20. Islam, S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The internet of things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708.
21. Jimenez, J.I.; Jahankhani, H.; Kendzierskyj, S. Health care in the cyberspace: Medical cyber-physical system and digital twin challenges. In *Digital Twin Technologies and Smart Cities*; Springer: Cham, Switzerland, 2020; pp. 79–92.
22. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart grid technologies: Communication technologies and standards. *IEEE Trans. Ind. Informatics* **2011**, *7*, 529–539.
23. Faheem, M.; Shah, S.B.H.; Butt, R.A.; Raza, B.; Anwar, M.; Ashraf, M.W.; Gungor, V.C. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Comput. Sci. Rev.* **2018**, *30*, 1–30.
24. Khaitan, S. K.; McCalley, J.D. Design techniques and applications of cyber physical systems: A survey. *IEEE Syst. J.* **2014**, *9*, 350–365.

25. Logvinov, O.; Kim, S. IEEE Standards for an Architectural Framework for the Internet of Things (IoT). In *IEEE Std 2413-2019*; IEEE, New York, USA, 10 March 2020; pp. 1–269.
26. Machorro-Cano, I.; Ramos-Deonati, U.; Alor-Hernández, G.; Sánchez-Cervantes, J.L.; Sánchez-Ramírez, C.; Rodríguez-Mazahua, L.; Segura-Ozuna, M.G. An IoT-based architecture to develop a healthcare smart platform. In Proceedings of the International Conference on Technologies and Innovation, Guayaquil, Ecuador, 24–27 October 2017; Springer: Cham, Switzerland, 2017.
27. Misra, S.; Maheswaran, M.; Hashmi, S. Case studies of selected iot deployments. In *Security Challenges and Approaches in Internet of Things*; Springer: Cham, Switzerland, 2017; pp. 77–94.
28. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutorials* **2015**, *17*, 2347–2376.
29. Woo, M. W.; Lee, J.; Park, K. A reliable IoT system for personal healthcare devices. *Future Gener. Comput. Syst.* **2018**, *78*, 626–640.
30. Singh, G. IoT for Healthcare: System Architectures, Predictive Analytics and Future Challenges. In *Handbook of Multimedia Information Security: Techniques and Applications*; Springer: Cham, Switzerland, 2019; pp. 753–773.
31. Atzori, L.; Iera, A.; Morabito, G. From smart objects to social objects: The next evolutionary step of the internet of things. *IEEE Commun. Mag.* **2014**, *52*, 97–105.
32. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future internet: The internet of things architecture, possible applications and key challenges. In Proceedings of the IEEE 10th international conference on frontiers of information technology (FIT), Islamabad, Pakistan, 17–19 December 2012.
33. Wu, M.; Lu, T.J.; Ling, F.Y.; Sun, J.; Du, H.Y. Research on the architecture of Internet of Things. In Proceedings of the IEEE 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 20–22 August 2010.
34. Lake, D.; Milito, R.M.R.; Morrow, M.; Vargheese, R. Internet of things: Architectural framework for ehealth security. *J. ICT Stand.* **2014**, *3*, 301–328.
35. Williams, T.J. A reference model for computer integrated manufacturing from the viewpoint of industrial automation. *IFAC Proc. Vol.* **1990**, *23*, 281–291.
36. Knapp, E.; Langill, J. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. In *Industrial Network Protocols*; Syngress 2015; MA, USA ; pp. 55–87. Available online: https://www.amazon.com/Industrial-Network-Security-Securing-Infrastructure/dp/1597496456 (accessed on 20 March 2021).
37. Yu, L.; Lu, Y.; Zhu, X. Smart hospital based on internet of things. *J. Networks* **2012**, *7*, 1654–1660.
38. Razzaque, M.A.; Milojevic-Jevric, M.; Palade, A.; Clarke, S. Middleware for internet of things: A survey. *IEEE Internet Things J.* **2015**, *3*, 70–95.
39. Kaspersky. Available online: https://www.kaspersky.com/about/pressreleases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019 (accessed on 15 November 2019).
40. Kumar, M. Security issues and privacy concerns in the implementation of wireless body area network. In Proceedings of the IEEE International Conference on Information Technology, Bhubaneswar, India, 22–24 December 2014.
41. Van Deursen, N.; Buchanan, W. J.; Duff, A. Monitoring information security risks within health care. *IEEE Comput. Secur.* **2013**, *37*, 31–45.
42. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the IEEE symposium on computers and communication (ISCC), Larnaca, Cyprus, 6–9 July 2015.
43. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. *Comput. Networks* **2018**, *141*, 199–221.
44. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the IEEE International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 10–11 February 2017.
45. Habib, K.; Leister, W. Threats identification for the smart internet of things in ehealth and adaptive security countermeasures. In Proceedings of the IEEE 7th International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 27–29 July 2015.
46. Mosenia, A.; Jha, N.K. A comprehensive study of security of internet-of-things. *IEEE Trans. Emerg. Top. Comput.* **2016**, *5*, 586–602.
47. Wang, W.; Lu, Z. Cyber security in the smart grid: Survey and challenges. *Comput. Networks* **2013**, *57*, 1344–1371.
48. Al-Mhiqani, M.N.; Ahmad, R.; Yassin, W.; Hassan, A.; Abidin, Z.; Ali, N.S.; Abdulkareem, K.H. Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 499–508.
49. Fillatre, L.; Nikiforov, I.; Willett, P. Security of SCADA systems against cyber–physical attacks. *IEEE Aerosp. Electron. Syst. Mag.* **2017**, *32*, 28–45.
50. Ding, D.; Han, Q.L.; Xiang, Y.; Ge, X.; Zhang, X.M. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing* **2018**, *275*, 1674–1683.
51. Coffey, K.; Maglaras, L.A.; Smith, R.; Janicke, H.; Ferrag, M.A.; Derhab, A.; Yousaf, A. Vulnerability assessment of cyber security for SCADA systems. In *Guide to Vulnerability Analysis for Computer Networks and Systems*; Springer: Cham, Switzerland, 2018; pp. 59–80.
52. Maglaras, L.; Ferrag, M.; Derhab, A.; Mukherjee, M.; Janicke, H.; Rallis, S. Threats, countermeasures and attribution of cyber attacks on critical infrastructures. *EAI Endorsed Trans. Secur. Saf.* **2018**, *5*, 1–9.
53. Choraś, M.; Kozik, R.; Flizikowski, A.; Hołubowicz, W.; Renk, R. Cyber threats impacting critical infrastructures. In *Managing the Complexity of Critical Infrastructures*; Springer: Cham, Switzerland, 2016; pp. 139–161.

54. Aikins S.K. Managing Cybersecurity Risks of SCADA Networks of Critical Infrastructures in the IoT Environment. In *Security, Privacy and Trust in the IoT Environment*; Springer: Cham, Switzerland, 2019; pp. 3–23.
55. Sengupta, J.; Ruj, S.; Bit, S.D. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481.
56. Mahbub, M. Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *J. Netw. Comput. Appl.* **2020**, *168*, 102761.
57. Alladi, T.; Chamola, V.; Zeadally, S. Industrial Control Systems Cyberattack trends and countermeasures. *Comput. Commun.* **2020**, *155*, 1–8.
58. Yadav, G.; Paul, K. Architecture and security of SCADA systems: A review. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100433, ISSN 1874-5482.
59. Aversano, L.; Bernardi, M.L.; Cimitile, M.; Pecori, R. A systematic review on Deep Learning approaches for IoT security. *Comput. Sci. Rev.* **2021**, *40*, 100389.
60. Babun, L.; Denney, K.; Celik, Z.B.; McDaniel, P.; Uluagac, A.S. A survey on IoT platforms: Communication, security, and privacy perspectives. *Comput. Networks* **2021**, *192*, 108040.
61. Bécue, A.; Praça, I.; Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artif. Intell. Rev.* **2021**, 1–38, doi:10.1007/s10462-020-09942-2.
62. Selim, G.E.I.; Hemdan, E.E.D.; Shehata, A.M. Anomaly events classification and detection system in critical industrial internet of things infrastructure using machine learning algorithms. *Multimed. Tools Appl.* **2021**, *80*, 12619–12640.
63. Cimpean, D.; Cano Bernaldo de Quirós, P.; García Gutiérrez, F. Appropriate Security Measures for Smart Grids—Guidelines to Assess the Sophistication of Security Measures Implementation. Tech. Rep., European Union Agency for Network and Information Security 2012. Available online: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids (accessed on 5 July 2020).
64. Pauna, A.; Moulinos, K. Window of exposure. . . a real problem for SCADA Systems. European Union Agency for Network and Information Security 2013. Available on: https://www.enisa.europa.eu/publications/window-of-exposure-a-real-problem-for-scada-systems (accessed on 5 July 2020).
65. Stouffer, K.; Lightman, S.; Pillitteri, V.; Abrams, M.; Hahn, A. Guide to industrial control systems (ICS) security. *NIST Spec. Publ.* **2015**, *800*, 82.
66. CPNI, Good Practice Guide—Cyber Security Assessments of Industrial Control Systems. Tech. Rep. 2011, Centre for the Protection of National Infrastructure. Available online: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf (accessed on 1 July 2020).
67. Yastrebenetsky, M. IEC-62645 Nuclear power plant instrumentation and control systems for safety and security. *International Electrotechnical Commission*; IGI Global: Hershey, PA, USA, 2014; pp. 1279–1316
68. Bochtler, J.; Quinn, E.; Bajramovic, E. Development of a new IEC standard on cybersecurity controls for I&C in Nuclear Power Plants–IEC 63096. *NPIC & HMIT*; San Francisco, 2017; pp. 23–24. Available online: http://npic-hmit2017.org/wp-content/data/pdfs/158-20165.pdf (accessed on 20 March 2021).
69. American Gas Association (AGA). Cryptographic Protection of SCADA Communications, Background, Policies and Test Plan. In *AGA Report*; 2016, American Gas Association, USA, No.12, Part 1. Available online: https://www.scadahacker.com/library/Documents/Standards/AGA (accessed on 20 March 2021).
70. Frankenberger, E. *Cyber Security Forum Initiative (CSFI) (Air Traffic Control) (ATC), Cyber Security Project*; Tech. Rep.; 2015. Available online: https://www.csfi.us/?p=projects (accessed on 20 March 2021). .
71. Rail Cyber Security: Guidance to industry. In *Rail Safety and Standards Board (RSSB)*; London, UK, Crown 2016; pp. 1–39. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/897091/rail-cyber-security-guidance-to-industry-document.pdf (accessed on 20 March 2021).
72. Global Business Fundamentals, Strategic Focus. Available online: https://www8.hp.com/us/en/hp-news/pressrelease.html?id=1744676#.YA0J36rdt0s (accessed on 22 January 2020).
73. Security Timelines and Statistics. Available online: https://www.hackmageddon.com/2020/09/24/july-2020-cyberattacks-statistics/ (accessed on 30 July 2020).
74. Information Age, Topics Cybersecurity, 700 Million Attacks on Consumer Transactions Prevented in 2017. Available online: https://www.information-age.com/700-million-attacks-prevented-2017-123470383/ (accessed on 30 July 2020).
75. Vectra Post-Intrusion Report. Available online: https://www.vectra.ai/press/vectra-networks-identifies-healthcare-as-the-industry-most-targeted-by-cyber-attacks (accessed on 30 July 2020).
76. Radcliffe, J. Hacking medical devices for fun and insulin: Breaking the human SCADA system. In Proceedings of the Black Hat Conference, Las Vegas, NV, USA, 30 July–4 August 2011.
77. Chen, J.; Su, C.; Yeh, K. H.; Yung, M. Special issue on advanced persistent threat. *Future Gener. Comput. Syst.* **2018**, *79*, 243–246.
78. Assante, M. A data-driven analysis of vulnerabilities in our industrial and critical infrastructure. In *Global ICS IIoT Risk Report*; CyberX-Labs, Waltham-USA. 2019. Available online: https://get.cyberx-labs.com/hubfs/Reports/CyberX (accessed on 30 July 2020). .
79. Modicon Bus (Modbus), Modbus-Plus. Available online: http://www.modbus.org (accessed on 22 January 2021).
80. Distributed Network Protocol 3 (DNP3), DNP-Three. Available online: http://www.dnp3.org (accessed on 22 January 2021).

81. Berry, A.; Homan, J.; Eitzman, R. WannaCry Malware Profile FireEye, May 2017. Available online: https://www.fireeye.com/blog/threat-research/2017/05/wannacrymalware-profile.html (accessed on 25 November 2020).
82. Mohurle, S.; Patil, M. A brief study of wannacry threat: Ransomware attack 2017. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 1938–1940.
83. Kraszewski, K. SamSam and the Silent Battle of Atlanta. In Proceedings of the IEEE 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 28–31 May 2019.
84. Murofushi, R.H.; Tavares, J.J. Towards fourth industrial revolution impact: Smart product based on RFID technology. *IEEE Instrum. Meas. Mag.* **2017**, *20*, 51–56.
85. Djenna, A.; Saidouni, D.; Abada, W. A Pragmatic Cybersecurity Strategies for Combating IoT-Cyberattacks, In Proceedings of the IEEE International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020.
86. Buffi, A.; Michel, A.; Nepa, P.; Tellini, B. RSSI measurements for RFID tag classification in smart storage systems. *IEEE Trans. Instrum. Meas.* **2018**, *67*, 894–904.
87. Kambourakis, G.; Kolias, C.; Stavrou, A. The mirai botnet and the iot zombie armies. In Proceedings of the IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017.
88. Mirai: What You Need to Know About the Botnet Behind Recent Major DDoS Attacks. Available online: https://www.symantec.com/connect/blogs/miraiwhat-you-needknow-about-botnet-behind-recent-major-ddos-attacks (accessed on 29 October 2020).
89. Herberger, C. The DNA of Modern IoT Attack Botnets, Radware 2019. Available online: https://www.cisco.com/c/dam/m/hr_hr/trainingevents/2019/ciscoconnect/pdf/radware_the_dna_of_mirai_modern_iot_attack_botnets_cisco.pdf (accessed on 29 October 2020).
90. Norbye, T. KV Engine Architectural Overview. Available online: https://github.com/couchbase/Memcached/blob/master/docs/Architecture.md (accessed on 29 October 2020).
91. Alpern, B.; Schneider, F.B. Recognizing safety and liveness. *Distrib. Comput.* **1987**, *2*, 117–126.
92. IoT Devices Used in DDoS Attacks. Available online: https://www.ibm.com/blogs/internetof-things/ddos-iot-platformsecurity (accessed on 29 October 2020).
93. Kaspersky Labs—Global Research & Analysis Team Carbanak APT: The Great Bank Robbery. Available online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf (accessed on 29 October 2020).
94. Schneier, B. Schneier on Security. Available online: https://www.schneier.com/books/secrets-and-lies-pref/ (accessed on 13 March 2021).