9-17-2020

Toward a sustainable cybersecurity ecosystem

Shahrin Sadik

Mohiuddin Ahmed
Edith Cowan University, mohiuddin.ahmed@ecu.edu.au

Leslie F. Sikos
Edith Cowan University, l.sikos@ecu.edu.au

A.K.M. Najmul Islam

10.3390/computers9030074
Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. K. M. (2020). Toward a Sustainable Cybersecurity Ecosystem. *Computers, 9*(3), 74. https://doi.org/10.3390/computers9030074

computers

MDPI

Article

Toward a Sustainable Cybersecurity Ecosystem

Shahrin Sadik [1], Mohiuddin Ahmed [2,*], Leslie F. Sikos [2] and A. K. M. Najmul Islam [3]

[1] Department of Computer Science and Engineering, International Islamic University of Chittagong, Chittagong 4318, Bangladesh; shahrinsadik.ss@gmail.com
[2] School of Science, Edith Cowan University, Joondalup 6027, Australia; l.sikos@ecu.edu.au
[3] School of Engineering Science, LUT University, FI-53851 Lappeenranta, Finland; najmul.islam@utu.fi
* Correspondence: mohiuddin.ahmed@ecu.edu.au

Received: 20 July 2020; Accepted: 11 September 2020; Published: 17 September 2020

Abstract: Cybersecurity issues constitute a key concern of today's technology-based economies. Cybersecurity has become a core need for providing a sustainable and safe society to online users in cyberspace. Considering the rapid increase of technological implementations, it has turned into a global necessity in the attempt to adapt security countermeasures, whether direct or indirect, and prevent systems from cyberthreats. Identifying, characterizing, and classifying such threats and their sources is required for a sustainable cyber-ecosystem. This paper focuses on the cybersecurity of smart grids and the emerging trends such as using blockchain in the Internet of Things (IoT). The cybersecurity of emerging technologies such as smart cities is also discussed. In addition, associated solutions based on artificial intelligence and machine learning frameworks to prevent cyber-risks are also discussed. Our review will serve as a reference for policy-makers from the industry, government, and the cybersecurity research community.

Keywords: sustainability; cybersecurity; cyber-risk assessment; cybersecurity life cycle; smart grid; anomaly detection; network traffic analysis; cybernetics; data analytics; blockchain; smart city; Internet of Things

1. Introduction

Cybersecurity covers the inception and preservation of processes relating to the detection of upcoming cyberthreats and the minimization of associated costs [1–11]. In fact, it is a prerequisite for adopting a sustainable computing ecosystem having responsibilities to safeguard the operation of modern, technology-based societies [12]. There is a growing need for improving the cybersecurity environment, but security developments lag behind because of constantly increasing malicious online activities. According to the 2019 Global Risks Report of the World Economic Forum, cybersecurity attacks are currently among the top risks globally [13]. Cyberattacks can result in multibillion-dollar losses in the business sector, especially when servers of banks, hospitals, power plants, and smart devices are compromized. Unfortunately, stability and trust have become the two major barriers in the development of IT environments due to a lack of effective cybersecurity measures. This may lead to severe damages for the IT society instead of supporting continuous development. Even though missing or inadequate security measures may not cause severe breakdowns initially, the IT society gradually will lose trust, resulting in a devastating decline in development [14–17].

According to the World Economic Forum, the estimation for the market value of cybersecurity is expected to increase from 120 to 300 billion by 2024. They claim that cybersecurity, in general terms, incorporates a huge domain, which ranges from structuring robust systems that can resist attacks to designing methods and systems that can contribute to detecting threats and anomalies, as well as assuring the resilience of a system and declaring system responses to any attack [13].

Cybersecurity strategies systematically document cybersecurity features, and have been rapidly adapted globally since 2011 [18]. There has been a gradual growth in the development of these strategies throughout the evolution of cybersecurity. The various versions of cybersecurity strategies evolved over time in countries individually according to local needs. These changes clearly indicate the progress in realizing the significance of cybersecurity not only by security professionals, but also by common people. As a result, cybersituational awareness has reached new heights, and more specific security countermeasures are planned.

This paper covers the details of identifying security risks and corresponding preventive measures. These are based approaches, models, methodologies, and conditions suitable for safeguarding and providing a secure and sustainable cybersecurity ecosystem. The discussion on major cybersecurity issues is provided to better understand almost every requirement of sustainable cybersecurity environments. This paper, unlike other works in the literature on sustainable cybersecurity (shown in Table 1), covers the security issues of emerging technologies such as smart cities, smart grids, and blockchain and AI-powered security applications. The rest of the paper is organized as follows. Section 2 contains a discussion on the background of sustainable cybersecurity research. Section 3 discusses cybercrime and cybersecurity challenges. Section 4 explains the Community Cybersecurity Maturity Model. Section 5 covers common cyber-risks and preventive strategies. Section 6 portrays the connection between information technology and industrial control systems. Section 7 showcases cybersecurity in smart grids. Section 8 includes emerging trends, and Section 9 discusses the security considerations of smart cities. The role of artificial intelligence, and machine learning in particular, in sustainable cybersecurity is discussed in Section 10. Finally, the paper is concluded in Section 11.

Table 1. Comparison with relevant papers.

Reference	Frameworks	Smart City	Smart Grid	Machine Learning	Blockchain	Cyberattacks
[19]	✓	×	×	×	×	×
[20]	✓	×	✓	×	×	×
This paper	✓	✓	✓	✓	✓	✓

2. Background

Cybersecurity attempts to protect data from attackers, which is crucial to all individuals as well as to all public and private organizations, as an integral part of cyberthreat mitigation strategies [21]. It is of utmost importance to achieve sustainability in cyberspace, thereby securing data and protecting information. It is in everyone's interest to work on preserving the data environment from hackers and malware—think of the implications of the massive waves of ransomware in recent years. Cyberthreats are rapidly increasing with sophisticated and sinister schemes, and a motive to intrude information systems. Understanding and identifying vulnerabilities that might be exploited by cyber-spies, such as that of foreign governments, has become a general requirement for security professionals. The effects of intrusions might bring organizations to their knees and can be devastating. The mindset of the cybersecurity community shifted from "if we are hacked" to "when we are hacked" [21], which is the main idea behind cyber-resilience: be prepared rather than being unrealistic by expecting cyberattacks to be completely avoidable, and maintain productivity/deliver outcomes despite any attack that might occur.

According to the University of Illinois Law Review, monitoring plays a significant role in creating sustainable online environments [14]. How to identify threats and backdoors are among the main concerns for every member of the information security community, considering that prevention relies on successful detection. Encryption, pseudonymization, and the aptitude to guarantee the ongoing confidentiality, integrity, and availability of personal data play a major role when implemented by technical and organizational measures so that the required level of security can be provided. It is always recommended to involve the IT staff in the training and support of every department of an organization

that uses the Internet, and raise awareness and prevent security issues that otherwise could rapidly escalate. Cybercriminals are, by nature, distributed and independent, whereas the industry standards or regulations integrate large bureaucratic processes; this leaves room for cyberattacks that target production systems [22]. They can continuously evolve their attack methodologies, and aid in understanding the importance of compliance with security practices. Restricting data access and alleviating real-time risks constitute the best model for compliance.

A sustainable cybersecurity ecosystem is crucial in terms of saving and securing organizations from being exploited or suffering data breaches [23]. The cornerstone of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is to review risks in cyberspace before controlling them. NIST also warns organizations to be careful of ransomware variants and vulnerabilities, both known and unknown. To achieve this, an approach called Security-First Compliance can be used, which means working towards constant system monitoring, auditing, review, and checking requirements to ensure compliance. This approach creates an environment that entirely concentrates on sustainable security. At its core, this security-first approach must begin by concentrating on securing information effectively, and then reviewing the alignment of the set controls before paying attention to the compliance mandates, which in turn will aid organizations to take their necessary actions according to regulations or industry standards.

Cybercriminals such as hackers tend to constantly evolve their attack strategies, which makes monitoring tools crucial to assess risks and obtain cyber-situational awareness. Efficient monitoring and logging can be complemented by complex behavior analysis performed by automated software agents, which utilize artificial intelligence in cybersecurity applications [24]. The security-first approach particularly benefits small to medium-sized businesses with very limited resources to secure their network [25]. This approach initially requires financial investment for the major requirements so that severe threats can be prevented. The achieved sustainable security solution enables security monitoring on a regular basis. This contributes to conserving resources rather than getting compromised.

Honeypots are security systems that appear to be legitimate parts of a production system and thereby bait attackers, but are actually isolated and monitored. They are widely deployed in large organizations in an attempt to identify ways cybercriminals use to gain access to company resources [26]. The logs generated by honeypots can be used to identify and address vulnerabilities in information systems. Keep in mind, however, that while security measures provide a firm base, no system is completely secure. Nevertheless, constant monitoring and documentation of the countermeasures taken for attacks undoubtedly contribute to a robust data protection approach.

Cyber-physical systems (CPSes) triggered the rise of globally deployed information and communication technologies, in which each individual is considered a stakeholder. Considering the individual level and the organizational level in a CPS, it is clear that they enable us to learn about the world and allow us to improve our communication efficiency. They also enhance efficiency, efficacy, and productivity across industry, government, and academia and highly contributes towards economy and national security. The very same systems are beneficial for cybercriminals, whose primary goal is to breach security. Unfortunately, efforts of the online workforce to improve performance, reliability, extensibility, and affordability have not been matched with advanced security practices, and many challenges remain. The authors in [27] suggested the development of computer architectures from the ground up with security in mind in the form of hardware-enhanced security. This could self-protect data, take precautions for implementing only trusted software, and new models for better security in cloud environments. Engineering security hardware can limit security breaches inherently.

In [28], the authors presented an optimal network architecture for safe and secure content delivery, the operation and effectiveness of which were proven via a case study. In another study [29], it has been observed that cyber-denial and deception exaggerate the need for proactive investigation and getting the competitors involved to influence their immediate responses. The four main factors for acquiring a safe and sustainable CPS ecosystem are improvement of hardware security, redesigning the networks related to content delivery, executing proactive defenses, and increasing the communication between all the levels.

3. Cybercrime and Cybersecurity Challenges

A cyberattacker uses techniques like phishing, spam messages, and distributed denial-of-service attacks (DDoS) to harm the data environment and to proactively monitor the system, making it necessary to plan continuous monitoring strategies [2,4]. To deploy such monitoring strategies globally, there is a rapidly increasing demand for security professionals. However, there is a shortage of skilled domain experts, which highlights the need for wider awareness and relevant undergraduate courses. With the help of cloud computing, easy access to remote services can be provided for training courses in cybersecurity. While such courses are becoming common, adequate training require tutors with hands-on skills from the industry. However, the growing number of cybersecurity qualifications does not necessarily keep up with the explosion of positions available in this field.

The efficient development and utilization of security countermeasures rely on professional with an adequate training and hands-on skills from the industry.. These can only be achieved if cybersecurity courses overcome geographical, institutional, and technical constraints, both in terms of development and delivery [30]. Training materials in cybersecurity should not only be up-to-date, but also comprehensive, covering authentic real-world attack scenarios, and actions taken by a security operation center (SOC) using which security information and event management (SIEM) software tools (RSA NetWitness, LogRhythm, Elastic SIEM, IBM QRadar, Splunk, etc.), and in which phase of the *MITRE ATT&CK Matrix* (https://attack.mitre.org) and the *Lockheed Martin Cyber Kill Chain* (https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf). This is invaluable for students to become job-ready.

There are multiple definitions available for cybercrime and cybersecurity, but no single definition is accepted globally. However, according to [31], there is no requirement for a single definition of the term "cybercrime" unless it is used for legal purposes. The authors clearly highlighted the different kinds of offences on confidentiality, data availability and integrity, IT and content-related issues, and offences regarding copyright. THE ITU defines cybersecurity as the assembly of various tools, security safeguarding concepts, related policies, and guidelines. It also manages risks and actions to train, assure, and utilize the technologies to protect and preserve IT infrastructures.

A solid understanding of cybercrime and cybersecurity is imperative for developing effective offensive and defensive security countermeasures. According to McAfee, the inclusion of law enforcement and legal frameworks, education, and awareness programs, and well-developed technological innovations could be the best choice to fight against cybercrime. Having the nature of today's Internet usage, whether social media applications or e-commerce, a clear rise can be observed in cybercrime from individual data theft to community data breaches.

As for dynamic capabilities and competitive advantage, [32] defines dynamic capability to be one of those abilities that can incorporate, construct, and redesign all the internal and external competencies for a fast-growing and varying environment. This definition indicates the need for flexibility. According to Barney, competitive advantage is the capability to execute a unique strategy that is not being utilized by any other present or dominant competitor. A sustained security advantage provides the benefit of security and prevents criminals from exploiting system vulnerabilities (apart from zero-days) by utilizing entire nations' capabilities, and via consistent capacity building and development. Further challenges including managing the scalability and heterogeneity issues derived from Big Data and the Internet of Things (IoT), which need further research. More and more organizations are working towards developing cybersecurity programs for addressing cyberthreats. Both communities and nations are affected, including public and private entities. Nowadays, what makes securing IT infrastructures particularly challenging is that the freely available hacking tools and publicly disclosed software vulnerabilities are not in balance with preventive measures, which are still in their infancy. This is the reason behind the development of the *Community Cyber Security Maturity Model (CCSMM)* [33], which helps narrowing this gap by guiding practitioners to recognize the requirements of states and communities, and ultimately generate a feasible and sustainable cybersecurity program.

4. Community Cybersecurity Maturity Model (CCSMM)

According to the Community Cybersecurity Maturity Model, the three significant mechanisms needed for every community member are a "yardstick", a "roadmap," and an ordinary point for reference and terminology. These are to be utilized by officials to discover and enhance the present posture of cybersecurity and its level of maturity through various states, with local communities sharing their experiences. CCSMM recognizes the features of states and communities as they go through a rigorous inspection of factors, such as awareness on cybersecurity, sharing of information in the organizations, developing and executing processes, planning actions for security, and the involvement of cybersecurity in all the plans related to communities and states to ensure operation continuity and incidence response planning. This model successfully identifies security factors that help evolve the maturity level of cybersecurity for nations as well as local communities by infusing required technologies, training, practices and test plans, as well as policies and plans of actions that must be included in security plans and implemented accordingly. This model portrays every possible feature of a community at multiple maturity levels. of the model defines five levels of maturity: initial, established, self-assessed, integrated, and vanguard. Leaders involved in the first level of the community might have very little awareness of cyberthreats. At the state level, there would be no sharing of information between entities within cities or appropriate organizations or agencies. The quote [33] "you are only as secure as your weakest link" needs to be considered, and the workforce should act accordingly. There are frequently asked questions regarding this model. One of them is whether every nation and local community need to be at the fifth level i.e., the highest maturity level. Another one is how long does it take to reach any level of the model. The answer to the first question is that it level 5 might be unrealistic. The goal is determined by the probable threat level expected for a given community. Let us assume that a community at level 4 will inspect and examine its capabilities of responding to cyberthreats and critical aspects of their infrastructure, and come up with a definite plan of action for implementing operations for any sort of cyber-incident. Despite having such strong models, nations still lag behind due to the shortage of funding the implementation of such programs. This model has been proven to be amongst the best and most viable ones for providing a sustainable cybersecurity ecosystem; nevertheless, the highest maturity levels must be given more attention during implementation to be adequately strong. In parallel with the growing dependence on critical cyber-infrastructures, vulnerabilities to cyberthreats are also increasing [34]. Conventional information sharing provides an opportunity for each party to communicate their findings, however, this is not always efficient and scalable. In contrast, collaborative information sharing can aid a community to discover cyber-risks and prevent a system from cyberattacks at a very early stage [34]. It also promotes a response to cyber-events, along with the associated practices. Access control (AC) needs to be implemented to be able to "share, but protect." According to the approached framework in [34], a community is generally comprised of sector groups, non-sector organizations, and super groups. Here a community integrates a super group to give functions that are similar, and this group is accountable for gaining information from the non-sector organizations and from external sources such as neighboring communities and the state government to the collaboration group. Intelligence information analysis is performed in order to identify and detect risks. Coordination between information sharing and cyber-event management among various sector groups is also possible. Vital factors include sharing event responses, strategies for mitigation, recommendations for recovery, alert, and warnings with members of a super group. This group is created by experts of the cybersecurity domain. Some major sectors, such as finance, energy, water management, healthcare, police, and telecommunications, are represented by a community that involves several sector groups. Each sector group promotes information-sharing among different organizations that form the relevant sector. A non-sector organization improves and promotes information exchange even for those organizations that are not referred to any key sector within a community, but may give out vital information for cybersecurity events. The key concern is that because participants of collaborative information sharing belong to multiple organizations, they might be at times reluctant

and may also hesitate to share sensitive user and organizational information. By providing better data privacy, every organization would share their information more enthusiastically with their external collaborative network.

The CCSM model has been enriched with collaborative information in [34] by adding an extra layer to a sustainable cybersecurity program.

5. Cyber-Risks and Preventive Strategies

The ability to identify and manage cybersecurity risks in a timely manner is vital for the success and survival of any organization. All staff members need to be involved in cybersecurity risk management to be able to properly identify and assess risks [23], which have to be categorized and prioritized. There are multiple ways to categorize cyber-risks, depending on their nature and potential ways to manage them. Figure 1 shows a hierarchy of cybersecurity risks.

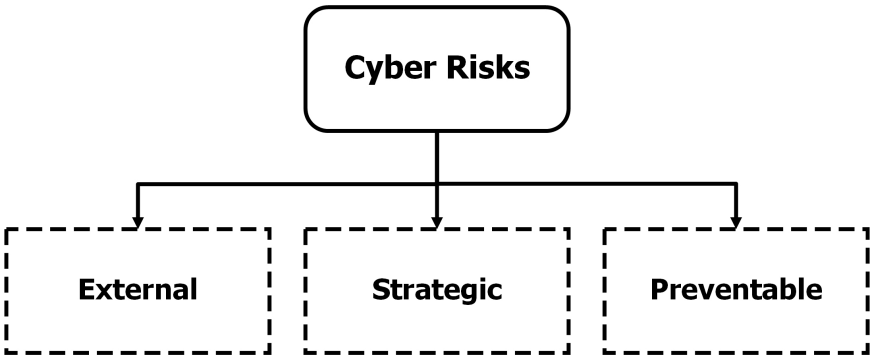

Figure 1. A simple hierarchy of cyber-risks (adapted from [22]).

Not every risk has a negative impact, even though most cyber-events do not benefit an organization. Cyber-risk assessments are crucial to provide organizations with a clear and accurate picture of all the relevant security risks, which is fundamental for cyber-situational awareness. Conducting several surveys, workshops, and interviewing staff members individually or in groups can give an insight to what they think of the risks, and help the organization become aware of the currently insignificant yet soon-to-be-major threats. A sustainable cybersecurity posture relies on continuous risk management, including continuous monitoring and data collection. By using governance, risk, and compliance (GRC) tracking tools, the level of cybersecurity risks can be tracked and evaluated [35]. When described in the context of assets, threats, and vulnerabilities, risks can be detailed with purpose-designed knowledge organization systems, the most widely deployed of which is the Structured Threat Information Expression (STIX) (https://oasis-open.github.io/cti-documentation/stix/intro.html). STIX defines objects such as attack pattern, indicator, and malware, set of intrusion, risk factor, vulnerability, etc., and can also capture the relationships between these.

According to the NIST framework [36], the lifecycle of cyberthreat mitigation strategies consists of five phases: identify, protect, detect, respond, and recover (see Figure 2). Each of these phases plays a vital role in sustainable cybersecurity.

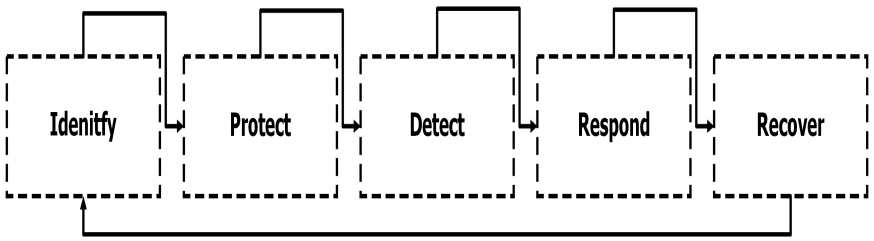

Figure 2. Cybersecurity lifecycle (adapted from [21]).

For improving the existing cybersecurity measures, several steps have to be considered, namely, data classification, implementation of security controls, routine verification for security control performance, plans and tests for breach preparedness, and acceptance and mitigation of risks. Figure 3 shows the steps of continuous improvement of cybersecurity.

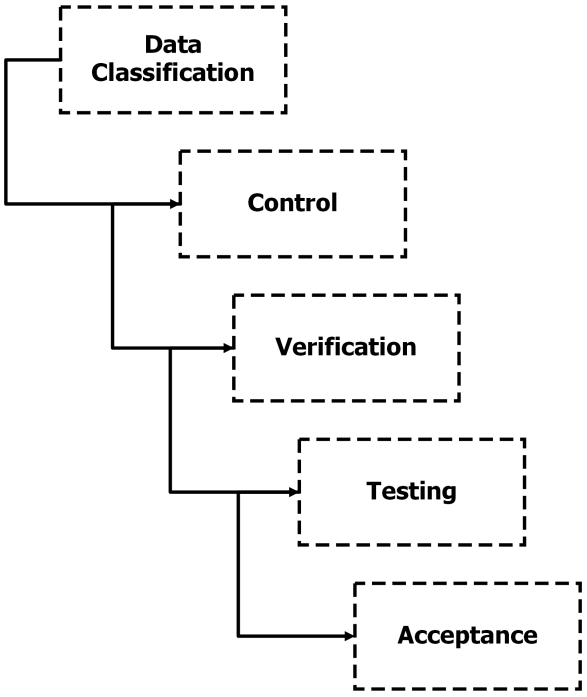

Figure 3. Continuous improvement of cybersecurity (adapted from [21]).

Data classification helps organizations determine the cost and effort associated with securing critical information assets used by the management for decision-making [21]. This involves identifying and cataloging critical data and setting up user access with the principle of least privilege. The three most common cybersecurity frameworks every organization should implement are the following:

- *Security and Privacy Controls for Federal Information Systems and Organizations (NIST 800-53)*: the standard of security control utilized by the organizations involved in business with the U.S. Government [37];
- *ISO 27001 International Standard* (https://www.iso.org/isoiec-27001-information-security.html);
- *SANS Critical Security Controls* (https://www.sans.org/critical-security-controls/).

It is important to regularly evaluate the security controls in place through ethical hacking techniques, such as penetration tests, thereby strengthening the overall security infrastructure. Planning for data breaches is also crucial, which requires establishing an incident response team [23]. Security mechanisms that prevent data exfiltration are also needed. If a data breach occurs, it is important to identify the source and acknowledge the data confidentiality levels of the company.

A holistic approach is proposed in [31], comprising of six steps: simulation, analysis, planning, developing, building, and operating. The first two phases, simulation and analysis, contribute to initiating sustainable protection, whereas the third, planning, sits between the commencing phase and the implementation phase. The final phase, implementation, deals with providing and constructing resources needed to protect a system against cyberattacks. There is an important step of recursion from the implementation phase to the starting phase so that the strategies needed to keep a check on the updates and sustainability of the system can be examined. This methodology can be applied in areas such as smart grids and power plants. The simulation phase consists of four steps, during which a model with the key components of the network topology is constructed (covering computers and other

connected devices, software, and organizational units). The variables are defined for unique incidents having potential cyberattacks on several nodes and connectors and the whole model network and probability values are assigned to each.

Next, the discrete simulation of each incident is performed according to the network model and its probable variable values in regard to cyberthreats. The results of this simulation are assembled to statistically explore and detect the vulnerabilities of each involved object that are dependent yet interconnected. The second phase is somewhat challenging, because it involves the analysis of the risks associated with each interconnected object. This phase contributes to various aspects of the modeled network, being the devices connected and as such, a risk in any of them might bring out a crucial risk for the entire system. The plan phase has another important role, because it involves all three components of the *CIA Triad* (confidentiality, integrity, and availability). The amalgamation of the first three processes is done in the implementation phase by considering human resources and hardware and software components. Finally, the last two phases (building and operation) are executed.

Small individual events, such as data theft, and even some large breaches, relevant to corporate databases are often not considered large enough issues to be addressed by state or local officials (even if they tend to become a public concern) because of their scope [33]. While the corresponding losses can be significant, without having data maintained by a state or federal government agency, government involvement is not justified. This raises the question: when do government officials have to get involved? It all comes down to impact. A computer "glitch" that might trigger security issues in an IT infrastructure, for example, might cause local damages or disrupt business, but has a minimal effect on communities or a nation. Government agents need to be involved in case cyber-events occur that affect computer users across the country, such as cyberattacks that completely cut off entire sectors for extended periods of time [33].

Even though the response of local and federal government officials vary greatly depending on the severity and scope of cyber-incidents, one thing is sure: they need to be ready to restrict, detect, respond, and recover from cyberattacks. By implementing an effective and stable security management system, cyber-risks can be minimized; however, no matter what kind of security systems are deployed, there is always a probability of data breach. It is important to emphasize that IT security is not the sole responsibility of the IT department, but the shared responsibility across an entire organization.

6. Industrial Control Systems (ICSs)

Ensuring cybersecurity in industrial control systems (ICSes) lags behind that of IT systems [19]. ICSes are used in several system controls for utility facilities. There are various ICS security issues that remain unaddressed due to their reliance on platforms based on control networks. ICSes introduced a change in software design as they unified commercial off-the-shelf (COTS) operating systems (OSes) and the Transmission Control Protocol /Internet Protocol (TCP/IP). These have been purposefully designed to replace proprietary network components. ICSes have an extensive use of wireless communications for remote device accessing, both for support and for maintenance. While this results in technological advancement, it also makes it difficult to preserve the confidentiality and protect the integrity of the data traversing the network nodes. This opens doors for digital vulnerabilities, increasing the number of potential security incidents. Plant system controls should be directly connected to business IT systems to make information sharing possible in all directions. Control networks of factories similarly employ Ethernet and TCP/IP.

Allowing operators to remotely monitor utility facilities via multiple devices through secured wireless communications on the operation level helps control room operators. There are a number of ways to implement cybersecurity measures both in ICSes and in IT systems. However, ICS implementations are more challenging due to their need of continuous operation, proprietary subsystems, vendor-specific software, limited resources and computing capacity, and their often hybrid (cyber-physical) nature. These are the main reasons why industrial control systems prioritize availability, and why security implementers need to consider the potential impact on performance and

productivity. In order to secure ICSes, security mechanisms, usually referred to as defense-in-depth, should be constructed around the multi-layered controllers. The less controller services and connections are incorporated (i.e., limited network services and closed ports), the less the chance of security breaches in the defensive layers. Only the ports for the TCP socket remain intact as they allow TCP socket communication in the application layer. This strategy can successfully provide protection even against zero-day attacks, which are notorious for being difficult to analyze. The intensity of cyberattacks is increasing at a rapid pace, and many target military, financial, energy, or financial infrastructures.

In parallel with the increasing IT demands, failures caused by system vulnerabilities also tend to increase. The networks of Internet of Things (IoT) devicesprovide unique opportunities for all the users. However, they also increase the possibility of cyberthreats and vulnerabilities . Smart grids are among the biggest IoT applications, and they allow real-time balancing and data tracking. Smart srids can be considered critical infrastructures (CIs), with vulnerabilities enabling cyberattackers to even cut off energy generation. This is why it is important to ensure the CIA triad in such systems. The components of the CIA triad are considered vital security aspects that must be satisfied. Smart grid systems are composed of multiple phases (generation, transmission, distribution, consumption). Smart grids are complex infrastructures consisting of several appliances and facilities. For electricity generation and storage, a periodic flow of data is expected depending on real-time requirements. In these systems, operations rely on protecting, tracking, analyzing, and controlling regular processes.

7. A Closer Look at Smart Grids

Smart grid is the lineage of an electrical power system that aims to attain reliability, flexibility, efficiency, and provides peaceful operation in the ecosystem [5]. The utilization of renewable energy resources has been exponentially increased in order to produce more energy around the globe. The most vital component to be protected from the cybercriminals in smart electric grids is the digital communication network, because it relies on a shared real-time information system. The maintenance and control functions of a grid also depend on this particular component. According to the Technological Platform of Europe's definition, smart grid is a kind of electric network that takes the users' actions into account to effectively deliver and share secure electronic supplies that are sustainable and economically advantageous for all connected to it. The International Council on Large Electric Systems and The International Electrotechnical Commission (IEC) has been devoted to work for a decade on issues concerning cybersecurity in power systems.

The IEC Technical Committee 57 (IEC TC57) defined a security standard, IEC 62351 (https://webstore.iec.ch/publication/6912), in order to recognize security matters for distinct operations of power systems and their communication channels. The evolution of smart grid technologies involves the traditional generation of power, transmission networks, along with distribution networks. It is vital to have a bilateral power flow in the electrical network and information flow in the communication network, allowing operation optimizations. Substations are those nodes that link up all the cables and lines for distributing electricity in the grid. They generally acquire data and pass it to and from sensors or actuators present in the power grid [38–40].

In the 1980s, the architecture of electric grids gradually evolved from being reliable on copper wiring to directly utilizing assisting solutions established using modem technologies. Conventional supervisory control and data acquisition (SCADA) systems had a range of alarming issues regarding interoperability between devices, making it necessary to restructure their protocols. In 1994, this resulted in IEC and IEEE introducing a general standard for communication. IEEE also established the Utility Communication Architecture (UCA) Framework. The IEC 61850 standard (https://webstore.iec.ch/publication/6028) defines the communication protocols for communication networks and systems. Updated versions to this standard have later been released (between 2002 and 2005).

Taking a closer look at attack scenarios in recent years indicate that Stuxnet disrupted several industrial sites and a nuclear plant in Iran. This was the first known advanced persistent threat (APT)

attack on a SCADA system, performing not only cyber-espionage, but also taking over a part of its operation control. Notable variants and descendants of Stuxnet include Duqu, Flame, and Gauss. Such computer worms can even initiate a cyberwar.

There is a saying that "when the electricity stops, everything stops;" this should be kept in mind for grid systems that are advancing via computerization, including solutions to proprietary control equipment. This reduces deployment costs, but increases vulnerabilities.

There is a range of security measures and tools for preventing unauthorized access to substation control systems, the primary ones of which are firewalls and unidirectional security gateways. Unidirectional security gateways have a very unique physical layer security with a transmitting and a receiver. These devices are present in both control and corporate networks. The presence of a laser and a photocell in both devices restrict the communication from the receiver to the transmitter, yet allows communication both ways, which can prevent vulnerability exploitation over the network.

Constant changes in communication networks make it difficult to adequately maintain security firewalls and gateways. The IEC TC57 Working Group 15 constantly evolves cybersecurity standards for information and security infrastructures of power system communication. They focused on communication protocols, as witnessed by IEC 60870-5/6, 61850, 61970, and 61968. The IEC 62351 security standard highlights the security mechanism for preserving communications established in the aforementioned IEC 61850. This cybersecurity mechanism prominently affects the performance of real-time communication in substations. It is now a growing demand of the power industry to have a basic framework for security in order to save and secure computational resources, and to preserve the entire ongoing communication in a network [2,6].

7.1. Cybersecurity in Smart Grid Systems

Cybersecurity issues are among the key concerns in smart grids due to the high-speed communication technologies and the large number of Internet-enabled power elements involved. Because networks are constantly exposed to cyber-risks, smart grids become more vulnerable due to the utilization of interconnected devices and the communication between them. The three main aspects of security (CIA triad) need to be assured for smart grids, because attempts to block or delay communication, illegally alter data, and acquire unauthorized access to the system are the three corresponding attack types [41]. Further requirements in smart grid systems include authentication, authorization, accountability, and providing privacy, dependability, and survivability. Authentication and authorization are needed to prevent unauthorized access. In such systems, cryptography plays a key role in securing two components of the CIA triad: confidentiality and integrity. Encryption is a basic cryptographic method that assures communication security. There are several existing schemes based on authentication and algorithms for encryption in smart grids.

Symmetric and asymmetric cryptography are used to block cyberattacks in the system. Along with cryptographic solutions, providing basic security solutions for the infrastructure, as for example, confirmation of peripheral components via safety engineering methods, utilizing policies for activation and security, methods for mitigation, and before plan finalization, simulation. Moreover, plans for cryptographic mechanisms and processes should be suitable for handling emergency incidents in a timely manner and managing faults concerning isolation, removal, location, and even data recovery. Required countermeasures required for providing cybersecurity in such systems include anonymity, risk assessment, data privacy, sandboxing, regular software updates, and complex and frequently updated passphrases. Cyberattacks on smart grids are usually coordinated, and they launch concurrent attacks, which are particularly challenging to handle, and may defeat the general defense mechanism. Security approaches relevant to network layers are considered efficient solutions for such smart grid applications [11].

7.2. Attack Types and Countermeasures

The types of cyberattacks against smart grids are determined by which components of the CIA triad and network layers are involved [42]—see the respective Tables 2 and 3 below.

Table 2. Attack type by CIA triad component, adapted from [43].

CIA Triad (Security Aspects)	Attack type
Confidentiality	Data Injection, Eavesdropping, Masquerading, Sniffing, Social Engineering, Traffic Analysis, Unauthorized Access.
Integrity	False Data Injection, Load-Drop Attacks, Masquerading, Replay, Spoofing, Time Synchronization, Wormhole.
Availability	Buffer Overflow, Denial of Service, Low-rate DoS, Masquerading, Spoofing, Smurf, Teardrop, Time Synchronization, Wormhole.

Table 3. Attack type by network layer, adapted from [43,44].

Network Layer	Attack type
Application	Data Injection, Eavesdropping, Social Engineering, Masquerading, Sniffing, Traffic Analysis, Unauthorized Access.
Transport	Buffer Flooding, Buffer Overflow, Covert Attack, Denial of Service, Data Injection, IP Spoofing, Packet Sniffing, Wormhole.
MAC	ARP Spoofing, Denial of Service, Jamming Attack, Masquerading, Traffic Analysis.
Physical	Eavesdropping, Jamming Attacks, Smart Meter Tampering.

The countermeasures should consider all the loopholes of a system in order to defend it from cyberthreats. The aforementioned attacks have associated countermeasures, only some of which are effective. Plans should be made for risk assessment during, after, and between attacks. Security policies should be regularly exchanged and vulnerabilities and suspicious events reported to maintain a good security posture. Artificial intelligence can be used for establishing security methods for constructing a robust system with advanced defensive mechanisms. Recommendations for a security framework for smart grid systems include the following procedural steps:

- The flow of communication within the system should be strictly maintained by means of authentication and access control.
- Detecting threats and planning preventive measures to fight them are significant and should be utilized appropriately in smart grids.
- At least basic cryptographic functions must be present at every node of the system.
- Protocol security for the network should be constructed from the application to the MAC layer.
- Platforms must be designed and executed for testing and assessing risks and cyberthreats of smart grid infrastructures.

Completely securing a smart grid from cyberattacks is unrealistic; therefore, the traffic status of a network should be properly monitored. Whenever an attacker plans to increase vulnerability as a part of a strategy, a system operator should starts working on decreasing the attack surface. The best defensive strategy for a system might be determined using game theory. Probabilistic risk assessment (PRA) deals with measuring the probability of cyber-threats and energy loss. This helps in assessing the vulnerabilities based on event statistics. However, if a relevant historical record is not available, such as in case of a DoS attack, it might be difficult to evaluate the chances of such attacks. For this reason, a model based on graph theory, in which a networked cyber-physical system is prioritized for evaluating attacks, might work better for smart grid systems, providing that there is sufficient interconnectivity between the devices. Graph theory appears to be convenient to introspect the interconnectivity

between all the vertices and edges (representing devices and connections, respectively), as well as the cyberthreats and attacks on a grid system.

8. Emerging Trends: Blockchain and IoT

The authors in [11,45] focus on *blockchain*, which has an emerging presence in power systems. Blockchain, along with the IoT, are considered significant for the automation of electric grids, bringing revolutionary changes in the future. The application of peer-to-peer management systems for charging electric vehicles, trading systems for energy, financing for renewables, energy billing and metering processes, services and schemes flexible for markets, etc. can have advantages in modern power systems. Blockchain promotes the joint operation of renewable sources with the facilities that store energy. It allows easy evaluation of service charge, making payments flexible by enabling an immediate and secure connection for service providers and receivers. This technology, when combined with the power system, can improve efficiency and overall performance, and will ensure the security of financial transactions. Blockchain is a distributed ledger based on cryptography, which is considered having an everlasting impact, as it allows reliable transactions between unreliable participants of a network. The unique features of this technology have drawn the attention of various fields, and its application is considered one of the best choices for a range of contexts. [27] presents a systematic literature review and a portrayal of how and where blockchain can contribute to sustainable and secure cybersecurity measures. The authors formulated three research questions to clarify the options to deploy blockchain in cybersecurity:

- What are the recent and latest applications of blockchain in the field of security?
- How is this technology utilized in improving cybersecurity?
- What are the available procedures for solutions relevant to blockchain in managing security without the need for a cryptocurrency token?

Some of the main cybersecurity applications of blockchain include the following:

- IoT: the deployment can be secured via the peer-to-peer (P2P) up-grade of authenticity of the network and connected devices. This covers risk detection and malware prevention.
- Data sharing and storage: it ensures that cloud data remains intact and no unauthorized access can take place; the list of hashes allows secure searching and secured and verified data exchange from dispatch to receipt [46].
- Network security: blockchain authenticates critical data as it stores the data in a decentralized way.
- Navigation and utility of the World Wide Web: ensuring the validity, utilization and navigation of interconnected wireless Internet access points by forwarding to the appropriate web page with the help of absolute records of DNS and web applications via encrypted and secured techniques.

Blockchain, with its unique capability of storing immutable transaction records and its decentralized nature, can be used efficiently to provide cybersecurity measures in a system [47]. Each members of a blockchain has an absolute copy of the whole transaction, making it easier for the peers to get historic information when and where required. Any changes to the chain can only be done when the majority of the nodes or members of the chain agree to the contribution in the previously ordered chain. Private blockchains are implemented in networks to allow the control of permitted devices, thereby securing tracking and managing data records and staying alert about unauthorized accesses. The security deployment through P2P during data exchange via authentication and identification is accepted. Blockchain can work as an intermediary between two network layers: the application layer and the transport layer. This uses token rewards as a means of units for voting. Furthermore, both public and private blockchains remove sources of failure for protecting data from any tampering in the data store, allowing the owner to have full control over their data, which makes it completely traceable. Blockchain is increasingly used for providing a sustainable network by improvising software-defined networks (SDNs). Containers are also used for authenticating critical

data in order to robustly store them in a decentralized manner. Cluster-based approaches are designed for the SDN controller when unified with blockchain, enabling clear communication within the network nodes. This further addresses the necessary and relevant security issues of a network. Nevertheless, the irreversible nature of blockchain makes it difficult to use in systems with data privacy concerns.

With the motive to apply blockchain in cybersecurity applications, it has been observed that using multiple layers of blockchain can be accountable for trusted and authenticated transactions. Yet, there is no clear direction on how blockchain can be used, or is there any possible need to develop a blockchain-based architecture for the purpose, and even the use of tokens is rather ignored in the literature. Systems based on the proof-of-work consensus mechanism are to the only ones that allow scaled security measures at all the network levels.

With the advantages come some major issues and challenges regarding deployment. Computational overhead might be the first challenge; other factors include scalability, bandwidth constraints, and blockchain governance . This is due to the mining pool defending against 51% of the attackers of smart grids [45]. Only after the aforementioned challenges are overcome can blockchain bring a substantial change in future smart grid systems.

9. Smart Cities: Sustainable Future

A smart city involves bringing together all administration, citizens, society, health and education systems, and every other significant element of the surroundings of a city, to be under the control of information and communication technology (ICT). This is done by combining advanced integrated technologies and IoT devices with the network, which has records, monitoring and controlling devices, and various choice selection algorithms.

Ref [48] displayed a basic idea on existing scenarios of cybersecurity in a smart city, including all cyberthreats that have a severe impact on the city and its belongings. The remote tracking of the traffic system, street lighting, water system management, city administration, etc. are the bindings of the smart city. It is very easy to hack any sensor-enabled system and harm the whole ecosystem. The basic challenges of a smart city concerning security are the following:

- Tools of IoT: Radio-Frequency Identification, Wireless Sensor Network, Smart Mobile Phones and Grid.
- Causes of governance: unsafe framework, mobility and management of smart devices.
- Economic and social aspects: smart communication, services, privacy, and e-commerce.

Another research work [16] addressed the concept and the cybersecurity concerns of smart cities in a broader way. A Hybrid Smart City Cyber Security Architecture (HSCCA) was proposed to ensure risk management at the regional level by enhancing efficiency, easing access, and exploring. It, in general, deals with only an smart city framework appropriately designed while taking all the schemes relevant to security, and without taking any gap of information, availability, and flexibility into account. This way, the response to information and any relevant incidents can be almost immediate. The source development should be directly able to access real-time data for optimizing the consumption of resources in both the department and city level. HSCCA involves the privacy of public data and intelligent methods to tackle threats and risks, and includes several tools to identify threats.

10. The Role of Artificial Intelligence in Sustainable Cybersecurity

Artificial intelligence, and machine learning in particular, provides advancements to cybersecurity, but are difficult for the wider community to adopt and understand [49]. The application of artificial intelligence in cybersecurity have both challenges and opportunities. There is a need for more research in AI implementations and effort in more secure training, as well as models verified in terms of security and privacy.

In [50], a Cybersecurity Autonomous Machine Learning Platform for Anomaly Detection (CAMLPAD) has been proposed in order to detect anomalies in real time. CAMLPAD is a platform

based on unsupervised machine learning, which aims to efficiently detect anomalies in cyberspace. A range of network data has been used in the development of the model, including YAF, BRO, SNORT, PCAP, and Cisco Meraki. This framework can not only detect anomalies, but can also determine the threat level of possible security breaches. Five machine learning algorithms are used for this purpose: K-means clustering, histogram-based outlier detection, multivariate Gaussian, isolation forest, and cluster-based local outlier factor. The data needs to be appropriately transmitted from the sensors to a local Hadoop server, which is then fed into a Kafka queue for effective data storage. These data are forwarded to the Elastic Search database, which normalizes the data, and then a unique identification number is assigned. This is then forwarded to a different machine, which is directly accessible from the database, saving computation time. A data frame is created, which contains the updated information for detecting anomalies depending on the previous pattern recorded, and later converted to numerical values for further processing. Once the data perfectly fits the model, an outlier score is assigned to the test data, and depending on this score, a basic PCA algorithm is used for creating clusters that are later processed, and a map is induced in order to detect anomalies. Next, an ensemble model is constructed via a democratic voting system with an option for everyone to contribute for determining anomaly. The final map is produced after recording for each data type and reclassified to check for accuracy; the last model not only considers the outliers, but also any sort of Internet traffic found in various sensor data. The accuracy is evaluated with the help of an adjusted RAND score. Thus, these models process the data to determine the presence of any anomalies and in return alert the users or administrators for taking necessary steps. In this proposed system, Kibana is utilized to visualize and determine the rate of the real-time outlier score. Once the value of the outlier score reaches the threshold, it autonomously alerts the administrator about the chances of a security breach that is about to or has already been occurred. CAMLPAD is an innovative approach for detecting anomalies, because it utilizes a combination of democratic voting-based evaluation that involves several data types to provide a streamlined and holistic mechanism.

In [51], the current deep learning approaches have been surveyed for intrusion detection. Because dataset play a major role in detecting intruders, 35 of the most popular cyber-datasets are utilized, which are classified into seven categories. The classified datasets are based on network traffic, virtual private network, electrical network, Internet traffic, Android apps, IoT traffic, and Internet-connected devices. Seven deep learning models have been analyzed, which involved deep belief networks, recurrent neural networks, restricted Boltzmann machines, deep Boltzmann machines, convolutional neural networks, deep neural networks, and deep autoencoders. Two real-time datasets, CSE-CIC-IDS2018 (https://www.unb.ca/cic/datasets/ids-2018.html) and Bot-IoT (https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php, have been used for each of the seven models, and their performance evaluated via binary and multiclass classification. Efficiency was also measured via some popular indicators, such as false alarm rate, rate of detection, and accuracy.

Recent research shows that log clustering plays a vital role in cybersecurity [52]. The criteria for an evaluation set was constructed to distinguish the features of clustering concerning objectives, techniques, detection, and evaluation of anomalies. These characteristics are assessed by the authors using 59 available approaches. All approaches use either of the following: parsing and signature, sequences and dynamic anomaly detection, overview and filtering, and static outlier detection. After a thorough investigation of how the several types of anomalies in the data log can be detected and which method is suitable for the purpose was conducted, based on which the authors proposed a tool to choose the best clustering approach considering the data log and features. This tool aims to rank the methods by their ability to answer the queries relevant to all features, and aid in envisioning the appropriate clusters in a PCA plot.

11. Conclusions

This paper discusses methods to adapt advanced, state-of-the-art security measures for cyberthreat prevention and mitigation. Implementing proper system components by taking into account the cybersecurity lifecycle while applying guidelines and best practices is imperative and required to detect and verify cyberthreats efficiently. The potential implications of cyberthreats have been analyzed with real-world examples across different industries, including, but not limited to, industrial controls systems, more specifically smart grids and smart cities. In addition, emerging trends are also discussed. Cybersecurity solutions powered by artificial intelligence and machine learning are also discussed, along with the community cybersecurity model. This review paper was written to serve as a source of references for industrial and government policy-makers as well as the research community.

Author Contributions: Conceptualization, M.A.; data curation, S.S. and M.A.; formal analysis, M.A., L.F.S., and S.S.; Funding acquisition, M.A.; investigation, S.S., M.A., L.F.S., and A.K.M.N.I.; methodology, S.S., M.A.; project administration, M.A. and L.F.S.; supervision, A.K.M.N.I.; validation, M.A., L.F.S. and A.K.M.N.I.; Visualization, M.A. and S.S.; and writing—original draft, S.S., M.A., L.F.S.; writing—review and editing, M.A., L.F.S. and A.K.M.N.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ahmed, M.; Mahmood, A.N.; Hu, J. The State of the Art in Intrusion Prevention and Detection. In *Outlier Detection*; Pathan, A.-S.K., Ed.; CRC Press: New York, NY, USA, 2014; Chapter 1, pp. 3–21 .
2. Ahmed, M.; Mahmood, A.N.; Hu, J. A survey of network anomaly detection techniques. *J. Netw. Comput. Appl.* **2016**, *60*, 19–31 . [CrossRef]
3. Ahmed, M.; Mahmood, A.N.; Islam, M.R. A survey of anomaly detection techniques in financial domain. *Future Gener. Comput. Syst.* **2016**, *55*, 278–288. [CrossRef]
4. Ahmed, M. Thwarting dos attacks: A framework for detection based on collective anomalies and clustering. *Computer* **2017**, *50*, 76–82. [CrossRef]
5. Ahmed, M.; Anwar, A.; Mahmood, A.N.; Shah, Z.; Maher, M.J. An investigation of performance analysis of anomaly detection techniques for big data in scada systems. *EAI Endorsed Trans. Ind. Netw. Intell. Syst.* **2015**, *2*, e5. [CrossRef]
6. Ahmed, M.; Barkat Ullah, A.S.S.M. False data injection attacks in healthcare. In *Data Mining*; Boo, Y.L., Stirling, D., Chi, L., Liu, L., Ong, K.-L., Williams, G., Eds.; Springer: Singapore, 2018; pp. 192–202.
7. Ahmed, M.; Choudhury, V.; Uddin, S. Anomaly detection on big data in financial markets. In Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Sydney, Australia, 31 July–3 August 2017; pp. 998–1001.
8. Ahmed, M. An unsupervised approach of knowledge discovery from big data in social network. *EAI Endorsed Trans. Scalable Inf. Syst.* **2017**, *4*, 9. [CrossRef]
9. Ahmed, M. Collective anomaly detection techniques for network traffic Analysis. *Ann. Data Sci.* **2018**, *5*, 497–512. [CrossRef]
10. Ahmed, M. Data summarization: A survey. *Knowl. Inf. Syst.* **2019**, *58*, 249–273. [CrossRef]
11. Ahmed, M.; Pathan, A.K. False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure. *Complex Adapt. Syst. Model.* **2020**, *8*, 1–14 . [CrossRef]
12. Cavelty, M.D.; Wenger, A. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemp. Secur. Policy* **2020**, *41*, 5–32. [CrossRef]
13. Taddeo, M.; Bosco, F. We Must Treat Cybersecurity as a Public Good. Here's Why. 2019. Available online: https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good/ (accessed on 22 June 2020).
14. Vasiu, I.; Vasiu, L. Cybersecurity as an essential sustainable economic development factor. *Eur. J. Sustain. Dev.* **2018**, *7*, 171–178. [CrossRef]
15. Mary, G.S.; Kumar, S.M. Secure grayscale image communication using significant visual cryptography scheme in real time applications. *Multimed. Tools Appl.* **2019**, *79*, 10363–10382. [CrossRef]

16. Sengan, S.; Subramaniyaswamy, V.; Krishnan, S.; NaircIndragandhi, V.; Manikandan, J.; Ravi, L. Enhancing cyber—Physical systems with hybrid smart city cyber security architecture for secure public data-smart network. *Future Gener. Comput. Syst.* **2020**, *112*, 724–737. [CrossRef]
17. García-Guerrero, E.; Inzunza-González, E.; López-Bonilla, O.; Cárdenas-Valdez, J.; Tlelo-Cuautle, E. Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using pic-microcontroller via zigbee channels. *Chaos Solitons Fractals* **2020**, *133*, 109646. [CrossRef]
18. Štitilis, D.; Pakutinskas, P.; Malinauskaitė-van de Castel, I. Preconditions of sustainable ecosystem: Cyber security policy and strategies. *Entrep. Sustain. Issues* **2016**, *4*, 174–181, . [CrossRef]
19. Kafol, C.; Bregar, A. Cyber Security—Building a Sustainable Protection. *Daaam Int. Sci. Book* **2017**, 81–90.
20. Cassotta, S.; Sidortsov, R. Sustainable cybersecurity? rethinking approaches to protecting energy infrastructure in the european high north. *Energy Res. Soc. Sci.* **2019**, *51*, 129–133. [CrossRef]
21. Penzenstadler, B.; Raturi, A.; Richardson, D.; Tomlinson, B. Safety, security, now sustainability: The nonfunctional requirement for the 21st century. *IEEE Softw.* **2014**, *31*, 40–47. [CrossRef]
22. Difenda: How to Build a Sustainable Cybersecurity Risk Management Program. 2017. Available online: https://www.difenda.com/how-to-build-a-sustainable-cybersecurity-risk-management-program (accessed on 22 June 2020).
23. Walsh, K. Continuous Monitoring Drives Sustainable Cybersecurity. 2019. Available online: https://www.zeguro.com/blog/continuous-monitoring-sustainable-cybersecurity (accessed on 22 June 2020).
24. Sikos, L.F. (Ed.) *AI in Cybersecurity*; Springer: Cham, Switzerland, 2019.
25. Creating a Sustainable Cybersecurity Management Program. 2017. Available online: https://www.bakertilly.com/insights/implementing-an-effective-cybersecurity-management-program (accessed on 22 June 2020).
26. Cabral, W.Z.; Valli, C.; Sikos, L.F.; Wakeling, S.G. Review and analysis of Cowrie artefacts and their potential to be used deceptively. In Proceedings of the 6th Annual Conference on Computational Science and Computational Intelligence, Las Vegas, NV, USA, 5–7 December 2019; pp. 166–171.
27. Hsu, D.F.; Marinucci, D.; Voas, J.M. Cybersecurity: Toward a secure and sustainable cyber ecosystem. *Computer* **2015**, *48*, 12–14. [CrossRef]
28. Gillman, D.; Lin, Y.; Maggs, B.; Sitaraman, R.K. Protecting websites from attack with secure delivery networks. *Computer* **2015**, *48*, 26–34. [CrossRef]
29. Heckman, K.E.; Stech, F.J.; Schmoker, B.S.; Thomas, R.K. Denial and deception in cyber defense. *Computer* **2015**, *48*, 36–44. [CrossRef]
30. Paulsen, C.; McDuffie, E.; Newhouse, W.; Toth, P. Nice: Creating a cybersecurity workforce and aware public. *IEEE Secur. Priv.* **2012**, *10*, 76–79. [CrossRef]
31. Barclay, C. Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (cm^2). In Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World-Impossible without Standards? St. Petersburg, Russia, 3–5 June 2014; pp. 275–282.
32. Teece, D.; Peteraf, M.; Leih, S. Dynamic capabilities and organizational agility: Risk, uncertainty, and strategy in the innovation economy. *Calif. Manag. Rev.* **2016**, *58*, 13–35. [CrossRef]
33. White, G.B. The community cyber security maturity model. In Proceedings of the 2011 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 15–17 November 2011; pp. 173–178.
34. Zhao, W.; White, G. A collaborative information sharing framework for community cyber security. In Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–15 November 2012; pp. 457–462.
35. Asnar, Y.; Massacci, F. *A Method for Security Governance, Risk, and Compliance (GRC): A Goal-Process Approach*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 152–184.
36. Teodoro, N.; Goncalves, L.; Serrão, C. Nist cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements. In Proceedings of the TrustCom/BigDataSE/ISPA (1), Helsinki, Finland, 20–22 August 2015; pp. 418–425.
37. N. I. O. Standards and Technology. *NIST Special Publication 800-53 Information Security*; CreateSpace: Scotts Valley, CA, USA, 2011.
38. Moreira, N.; Molina, E.; Lázaro, J.; Jacob, E.; Astarloa, A. Cyber-security in substation automation systems. *Renew. Sustain. Energy Rev.* **2016**, *54*, 1552–1562. [CrossRef]

39. Takano, M. Sustainable cyber security for utility facilities control system based on defense-in-depth concept. In Proceedings of the SICE Annual Conference 2007, Takamatsu, Japan, 17–20 September 2007; pp. 2910–2913.
40. Moradi, J.; Shahinzadeh, H.; Nafisi, H.; Gharehpetian, G.B.; Shaneh, M. Blockchain, a sustainable solution for cybersecurity using cryptocurrency for financial transactions in smart grids. In Proceedings of the 2019 24th Electrical Power Distribution Conference (EPDC), Khoramabad, Iran, 19–20 June 2019; pp. 47–53.
41. Abrams, M.D.; Jajodia, S.G.; Podell, H.J. *Information Security: An Integrated Collection of Essays*, 1st ed.; IEEE Computer Society Press: Washington, DC, USA, 1995.
42. Cyber Breaches Survey. 2019. Available online: https://www.thebci.org/news/cyber-breaches-survey-2019.html (accessed on 22 June 2020).
43. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
44. Labrador Rivas, A.E.; Abrão, T.Faults in smart grid systems: Monitoring, detection and classification. *Electr. Power Syst. Res.*, **2020**, *189*, 106602. [CrossRef]
45. Ahmed, M.; Pathan, A.K. Blockchain: Can it be trusted? *Computer* **2020**, *53*, 31–35. [CrossRef]
46. Ziegeldorf, J.H.; Morchon, O.G.; Wehrle, K. Privacy in the internet of things: Threats and challenges. *Secur. Commun. Netw.* **2014**, *7*, 2728–2742. [CrossRef]
47. Ahmed, M. False image injection prevention using ichain. *Appl. Sci.* **2019**, *9*, 4328. [CrossRef]
48. AlDairi, A.; Tawalbeh, L. Cyber security attacks on smart cities and associated mobile technologies. *Procedia Comput. Sci.* **2017**, *109*, 1086–1091. [CrossRef]
49. Sagar, B.S.; Niranjan, S.; Kashyap, N.; Sachin, D.N. Providing cyber security using artificial intelligence—A survey. In Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019; pp. 717–720.
50. Hariharan, A.; Gupta, A.; Pal, T. Camlpad: Cybersecurity autonomous machine learning platform for anomaly detection. In *Advances in Information and Communication*; Arai, K., Kapoor, S., Bhatia, R., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 705–720.
51. Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.* **2020**, *50*, 102419. [CrossRef]
52. Landauer, M.; Skopik, F.; Wurzenberger, M.; Rauber, A. System log clustering approaches for cyber security applications: A survey. *Comput. Secur.* **2020**, *92*, 101739. [CrossRef]