Journal of Software Engineering and Applications, 2023, 16, 530-547
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Increasing Threats to United States of America Infrastructure Based on Cyber-Attacks

Robb Shawe, Ian R. McAndrew

The Department of Cyber Leadership, Capitol Technology University, Laurel, MD, USA
Email: rshawe@captechu.edu, irmcandrew@captechu.edu

How to cite this paper: Shawe, R. and McAndrew, I.R. (2023) Increasing Threats to United States of America Infrastructure Based on Cyber-Attacks. *Journal of Software Engineering and Applications*, **16**, 530-547.
https://doi.org/10.4236/jsea.2023.1610027

Received: August 31, 2023
Accepted: October 28, 2023
Published: October 31, 2023

Abstract

The United States of America faces an increasing number of threats to its critical infrastructure due to cyber-attacks. With the constant advancement of technology and the interconnectedness of various systems, the vulnerabilities in the nation's infrastructure have become more pronounced. Cyber-attacks on critical infrastructure, such as power grids, transportation networks, and financial systems, pose a significant risk to national security and public safety. These attacks can disrupt essential services, cause economic losses, and potentially have severe consequences for the well-being of individuals and communities. The rise of cyber-terrorism is also a concern. Cyber-terrorists can exploit vulnerabilities in cyberspace to compromise infrastructure systems, causing chaos and panic among the population. The potential for destructive attacks on critical infrastructure is a pressing issue requiring constant attention and proactive measures.

Keywords

Critical Infrastructure, Cyber-Attacks, Cybersecurity, Cyberspace, Cyber-Terrorism

1. Introduction

Cyberspace dangers are genuine, and power grid property managers and owners should spend appropriately on information technology. According to various scientists' previous research, most malicious attackers that attack critical infrastructure are well-funded and possess extensive understanding and skills [1]. Some computer hackers have targeted infrastructure for financial benefits or in competition with the nation or organization they are trying to affect through cyber-attacks [2]. Cyber-attacks are complex to correct once they occur. Therefore, operators and managers must take the correct precautions to avoid unex-

pected expenses and losses. To plan for and react to cyber assaults, the administrators of all these networks must have sufficient funds and sophisticated experience and competencies.

To address these threats, there is a need for robust cybersecurity measures. Governments, organizations, and individuals must work together to enhance critical infrastructure security and strengthen their defense against cyber-attacks. This includes implementing advanced threat detection and prevention systems, conducting regular security audits and assessments, and promoting a culture of cybersecurity awareness and education. Additionally, cooperation at an international level is vital to combatting cyber threats effectively. Sharing information, best practices, and intelligence across nations can help identify and mitigate potential threats before they cause significant harm. In conclusion, the increasing threats to the United States of America's infrastructure based on cyber-attacks necessitate a comprehensive approach to cybersecurity. By prioritizing the protection of critical infrastructure and fostering collaboration, we can better safeguard national security and the well-being of the American people.

2. Literature Review

[3] are among some researchers who investigated this topic to analyze the significant cyber threats and incidents that have so far occurred affecting industrial information technology systems. Paramount infrastructure security, a pressing issue in our day, will be exacerbated as the Internet of Things (IoT) grows in popularity [4] [5]. The IoT is a collection of pervasively connected computers, hardware, and software that enable new and creative functionalities. Such technologies have become ingrained in our ordinary activities, from the gadgets we carry to the automobiles we operate to the electronics that govern vital infrastructure components [6]. As the IoT is a natural evolution of corporate management technology, cybersecurity will become more sophisticated, needing more care to protect critical infrastructure [7].

Whereas companies, governments, and individuals are continually under attack, infrastructure is rapidly becoming a target for personal and national information security, which sees the opportunity to breach formerly impenetrable monitoring technology [8]. As a result, this action has demonstrated how vulnerable communities, governments, and countries are to this kind of hazard and the growing need to build global financial responsiveness. Cyber-attacks against high-profile targets are becoming more regular [7]. In the past years, the US administration had no trouble assigning culpability for losing the personal data of more than 7.8 million federal workers from the Department of Human Senior management software applications [3]. As a result, the United States of America (USA) quickly realized North Korea was responsible for the PlayStation cyber-attack. Computer security gives nations a proper position globally, providing significant power for all countries. While Japan, the USA, and China are the world's most prolific cyber-attackers, every nation is involved [9]. Every country has several

computer attackers.

Similar regulations will be finalized by the European Union eventually as a crucial first move in fighting off cyber-attacks [10]. The "Telecommunications and Computer Security Regulation" mandates member nations to implement more stringent cyber-security requirements and establishes a communication channel between the participating countries and administrators of essential systems such as power, commerce, and hospitals [11]. Other nations are making moves to follow in the footsteps of the USA. Unfortunately, no government has put aside sufficient funding to prepare for the rising threat of cyber-attacks on critical infrastructure [1]. No government, however, has a comprehensive plan for avoiding or successfully responding to the repercussions of such attacks [4], [5]. Several ransomware-impacting systems and applications have been discovered recently, including Havex, BlackEnergy, and Stuxnet, to name a few more notable ones. The ability of these distinct types of Malware to infiltrate Embedded Devices unnoticed by exploiting weaknesses and vulnerabilities in cyber security networks, masquerading as legitimate correspondence, or locating a secret entrance in the Central controller is what they have in common, including other characteristics [9].

3. Dominant Theories/Hypothesis

Due to its inherent vulnerability, the power business must commit more resources to secure its information systems and train employees to avoid participating in dangerous file-sharing activities. For example, in January 2016, the USA's National Security Agency (NSA) released a warning downplaying the possibility of a cyber-attack on the USA's energy grid [12]. Nonetheless, by April 2016, it had joined the Federal Bureau of Investigation (FBI) to roll out application-specific warning features nationwide about the possible effects of cyber-attacks to emphasize the problem's urgency [10].

Prior, the Senate Intelligence Committee on National Security and Regulatory Operations received a briefing on cyber-security in the power business from the National Institute of Standards and Technology [13]. One of the most immediate worries was developing thread strategies to aid the impacted communities [8]. The government within the global community has systems in place to cope with the loss of natural catastrophes; however, there are no procedures in place to cope with a blackout, which has to improve. For example, the states and local governments within the USA must collaborate with their federal partners to develop and execute measures to prevent future assaults.

Historically, industrial control systems research has been stored in a restricted space, emphasizing quality. Every device has been locked to prevent the operation from continuing if anything goes wrong [14]. However, the growth of online standards, IoT devices, and mobile connections across Internet Connection Sharing (ICSs) has considerably decreased complete isolation. According to the research findings, security measures not designed to withstand fraudulent

attacks are even more exposed than before to such attacks [8]. Much of the creative approach to cyber-attack detection in ICSs is based on traditional Intrusion Detection Systems (IDSs), initially designed for information technology (IT) security research. IDSs are classified into two categories: biometrics and training techniques. Moreover, signature-based strategies are excellent at recognizing frequent attacks using databases and pre-defined identifiers but useless at identifying unexpected or innovative assaults [15]. On the other hand, learning-based algorithms attempt to uncover operational patterns or patterns that improve the precision with which unplanned intrusions are dealt with when detected.

Similarly, cyberterrorism and infrastructure cyber-attacks are another area of the chosen topic that unites different thinkers and practitioners in their hypotheses and opinions. [16] relates cyber-attacks and chemical, biological, radiological, and nuclear (CBRN) threats. It creates malicious software, also known as malware, to build infrastructure cyber-attacks and deprive the government of control over different systems. Similarly, accessing a program developed by professional organizations and using it for personal purposes, sabotaging power grids, and disabling energy systems is straightforward [16] [17]. Compared to CBRN attacks, infrastructure cyber-attacks are characterized by a large scale and the possibility of returning [18]. Terrorism aims to raise money, control people, demonstrate superiority, or entertain the public. In the chosen realm, infrastructure cyber-attacks can threaten governments or particular organizations due to overall access to the Internet [19] [20]. Due to the impossibility of ceasing action using technologies and services online, cyberspace is constantly under terrorist threats out of legal control.

Additionally, the future of infrastructure cyber-attacks depends on how effective anti-terrorist policies and statements are developed and distributed in society. The Bureau of Counter-terrorism (2019) report proves that many countries thoroughly analyze international cyber-attacks and CBRN threats, including the USA, China, and Germany-terrorism; policies are not only a governmental need to identify the characteristics of terrorists but an obligatory measure to reduce radicalization [21] [22]. Other hypotheses about the future of terrorism are connected to the impact of population growth, access to information about terrorism, and cultural differences [23] [24]. These arguments and explanations prove that infrastructure cyber-attacks are not restricted to the USA. Still, the future of the global community poses certain dangers and unpredictable consequences for human beings.

4. Methodology

The research conducted by ICS was the observation method. Researchers observed all the processes in the industry on the information technology systems to note the defects observed in information security [25]. For anomalous identification in intelligent pervasive computing networks, references employed a

standard route searching approach. The researchers devised a strategy for detecting attacks depending on the Statistical linear relationship between two sensors [15]. In their approach technique for an intrusion detection system, the authors used an IDS built on the Gaussian distribution. Even though these methods successfully identify abnormal activity, they could be more reliable due to infrastructure improvements resulting in various IDS configurations [14]. Learning-based I.D.S.s, on the other hand, is built around a reasonable distance that constantly evolves and learns new risks.

These algorithms use current databases to reproduce the program's regular performance and detect the unusual combinations as anomalies [26]. The article developed recurrent neural networks and a multilayer auto-encoder-based object-tracking approach for ICS. Furthermore, Support Vector Machine (SVM) and RF identify Denial of Service (DoS) assaults [4] [5]. Following findings of monitoring assaults, the reference proposed an automated approach for the critical instructional of data breaches. There is a computer hackers' identification in treatment plants, including coevolutionary neural network types [7]. Long Short-Term Memory (LSTM) networking to identify ICS anomalies is proposed to detect these abnormalities. The authors suggested approaches for detecting assaults using Patriarchal Social Neural Networks. As an alternative, employing Recurrent Neural Networks (RNNs) offered a more profound training IDS using a recurrent neural network [27].

4.1. Strengths and Weaknesses

The limitation of the study was that many processes were conducted in privacy as the leadership needed to secure the identity of the researchers since they could not just trust their words because they also wanted to secure their information [27]. The leadership was worried that the researchers would disclose their essential information to other organizations that functioned as competitors, including the findings to acknowledge the managers [6]. Since they were working smart regarding information security, which showed how they were aware of cyber-attacks, some happened quickly through deceiving acts and mistrust from either employees or people of unknown, untrusted identities [12]. This study recommended that all information technology system managers should always be careful of unauthorized users who may present themselves as good people. Nevertheless, they are hackers and might bring down their infrastructure, thus affecting the whole nation [12].

Researchers have produced many studies on the technology used in these regions for other infrastructures, such as the marine environment. They detailed all cyber-attacks that occurred and those projected to emerge due to human mistakes. The study conducted by [28] on cyber-security in the marine sector provides more information on the types of cyber-attacks that occur in the business and the methods by which they appear. In addition, this paper provides a brief explanation of how these assaults affect the sector, including the resulting

losses [28]. Creating a survey to examine the effect of different players in a maritime corporation's preparedness and competence on cyber security was the goal of this project, with the results being compared to research results [2]. As a result, it is possible to find security weaknesses and critical aspects in maritime industry operations.

According to [29], addressing cyber-attacks in the maritime industry, on the other hand, is more challenging as the magnitude of the problem still needs to be determined. As a result of the computerization of the distribution process and its various facets in the current internet age and the post-globalization of marine vessels, the authors argue that it is necessary to enhance the sustainability of its essential components [3]. Getting inoculated against one ailment does not rule out the possibility of other hazards developing or increasing. Put another way, having antimalware software does not automatically make you immune to threats; instead, the key is to utilize it [3]. The authors urge that researchers interested in the maritime industry go further into their research to understand better how cyber-attacks occur in the industry and how they are dealt with and prevented from reoccurring in the future.

4.2. Gaps in Knowledge

There is a gap between the actions of players in the maritime industry and the vulnerability of infrastructure to a natural disaster [15]. While the report suggests what should happen and how specific preventive measures are implemented in the maritime industry to minimize losses caused by cyber-attacks, it does not specify how to implement them. In information technology, improving education and implementing practical ideas have become crucial [10]. The skills acquired through the instruction on information technology can help prevent marine cyber-attacks and keep the sector on up-to-date resolutions [27]. Consequently, the maritime industry must raise education levels to strengthen the interaction between the adapters and the distribution network between seaport networks. Furthermore, the naval sector should provide cyber-risk training to inform those in the information technology industry about current cyber risks and prevent attacks [13]. New workers should also be informed about assaults and help them realize that cyber-attacks are widespread and may occur at any moment, even when anticipated [25].

The program's potential relevance in the marine environment is shown by implementing a cybercrime training curriculum and developing cyber-security goals [6]. Another study has shown that incidents are occasionally triggered by individuals sacked from their jobs. They are more likely to do this as a form of retaliation or out of rage. The world has vast security dangers that still need to be acknowledged [26]. When dealing with a cyber-attack-related issue, shipping companies, distribution network players, and consumers may find themselves at a distinct advantage. Marine cyber-attacks disrupt international commerce export and import operations and, as a result, directly impact the economy of the

USA [7].

Compared to information technology initiatives with a narrower focus to interact with current company processes, technological advancements are more outwards focused, integrating gadgets to deliver superior cloud capabilities and improved client involvement [29]. New research indicates that digitization has gone to the top of organizational management beliefs. Almost 90% of business leaders in the USA believe that information technology and virtual developments will play an increasingly significant role in their cumulative growth over the coming decade [4] [5]. On the other hand, these activities will present companies with many new dangers, including cyber security threats [1].

As businesses increasingly leverage sophisticated new capabilities to drive innovation in cyber events, the nature of information technology threat intelligence is changing, with more effective strategic and complicated risks predominating. Recently, there has been a substantial shift in the characteristics of information technology security incidents and their implications [11]. Information security, core information technology, and new tools are mistakenly regarded as distinct business entities, complete with risk, regulation, and a secure environment rather than a collection of interconnected components [9]. Unlike 15 years ago, when an IS modifiable event might cause only minor "practical" problems, we today face a wide range of complex. These targeted cyber-attacks may cause significant disasters and incur significant overt and hidden costs [28]. A company's competitiveness and policy interests are affected by its actions.

According to research conducted by Pricewaterhouse Coopers, companies with network security incidents have lost around 2.1 percent of their value, resulting in a loss of over a billion dollars for each event published in 2012 [30]. Regarding the impact on enterprises, cybercrimes may significantly negatively influence people's lives (phishing scams, unauthorized access). Federal and state governments (government assaults, criminal organizations, network analysis methods on "smart" devices to access the network, control mechanisms, or critical national infrastructural facilities) are also included in this category [30]. However, it was less likely two decades ago, especially in infrastructure. Cyber-related catastrophes do not arise due to an "error" or "bad luck". Instead of insufficient data program setup and a scarcity of cyber security competence, the problem has arisen [6]. Inherent in any information management system are information technology protections enabling it to run non-disruptively, accurately, dependably, and productively. The more advanced the material handling system and processes an organization develops to recognize and prevent all cyber-attacks, the more likely the company will be exposed to computer hazards or be subjected to lower average risk [13].

5. Sample/Unit of Analysis

A systematic review is a preferred research method in scholarly articles; however, enterprise information security may be challenging to implement and man-

age in a data breach. Some researchers will address many sampling methods, including random (systematic, stratified, or cluster) and non-random (purposive or snowballing). Focusing on particular individuals and answering research questions is possible, relying on interviews and questionnaires. On the other hand, some scholars find inviting organizations and communities to obtain general data necessary. In the current topic, infrastructure cyber-attacks focus on citizens from different countries; therefore, international samples are preferred to gather, compare, and analyze data. Global and local models effectively contribute to understanding the future of infrastructure cyber-attacks in the USA since this country establishes relationships with different nations.

Regarding businesses, it is essential to remember that there is no such thing as a "one solution fits all" idea since each has its unique set of infrastructural and technical needs [11]. Therefore, it is not always possible to foresee when infrastructure cyber-attacks will occur, and the precautions used to protect a system from assaults may not be effective when the attacks do occur. However, there is valuable advice for handling cyber catastrophes; most targeted companies are caught off guard in crises, failing to provide proper safety protocols and reacting swiftly [8]. A significant problem for any government's cyber security program is electrical power generating difficulties in a world becoming more dependent on the Internet and, consequently, energy, such as healthcare and businesses [14]. The possible expansion of so-called "distributed generation" networks, which employ digital technology to permit two-way communication between utilities and their customers, would represent a huge step forward in developing reliable electricity supply and distribution. Additionally, since functional, administrative, and telecommunications technology barriers have been dismantled, baseload digitalization has increased its sensitivity to information security threats due to the factors above [14].

The merging of information technology and operational technology gave rise to the concept of cloud computing and a plethora of breakthroughs in critical infrastructure management (CI) [29]. Additionally, the development fosters a deep awareness of cybercrime since CI safety becomes increasingly difficult to apply from both an information technology and an operational technology viewpoint. According to the current national trend, significant energy infrastructure facilities will be one of the primary targets of computer hackers shortly [2]. Additionally, to enhance their protections and raise user engagement, considering the general paucity of resources for establishing an integrated security program for critical power transportation systems, the key priority should be improving their safeguards and increasing user involvement [26]. The analysis for this paper comprised multiple conceivable scenarios representing different cyber-attacks on Critical Power Systems and examining the firms' reactions and organizational mistakes throughout the planning and response process [27]. As previously stated, human factors play an essential role in information security: they are one of the leading sources of cyber-attacks, whether due to a lack of awareness or

improper behavior.

According to the study, due to the political nature of the conflict, the material was either kept from being shared ultimately or was removed entirely from the disclosures in all information security events [1]. The cause of failure and privacy issues represents the most severe threat to providing essential power services and infrastructure [12]. The result not only constitutes the honesty of the adversary establishment but also decreases the chance of cybercriminals planning to study the used malicious software or methodology and replicating it elsewhere [2]. Therefore, it is critical to discuss and coordinate cyber security crises on a national and international level to build an appropriate response [4] [5]. The technique provided in this section should provide more information on the issue of cyber-attacks on critical infrastructure.

Moreover, it should attempt to correctly evaluate a trade association or other organization [4] [5]. As a result of integrating information technology and operational technology settings, the reliability of electricity production requires additional planning and complexity. The results were compared against a realistic framework for measuring the information security degree of essential energy infrastructure, including the findings [9]. However, the calculations and the areas that have been specified still need to be satisfactory.

The agricultural business has recently made enormous strides in developing smart farming and precision technology in agriculture and its role as a critical component of the USA's infrastructure [14]. It is also vulnerable to cyber-attacks; however, most of those working in the business may be unaware of how these assaults occur. Regarding global productive capacity, agriculture accounts for 6.4 percent of total output [7]. As a result, they are developing in the current agricultural environment, and deploying modern technologies will have a more substantial economic impact than previous generations [7]. Additionally, the rapid increase in population has increased the need for agricultural food products. Therefore, conventional farming methods must be updated to fulfill this need [14]. Consequently, the food and agricultural manufacturing sectors have started using information and IoT technologies to increase the quantity and quality of farm products available today [3].

Increased productivity while retaining customer satisfaction may be possible with intelligent farming. Precision agriculture scenarios, such as controlled water distribution and groundwater surveillance at distinct levels, are used all around the globe to enhance agricultural yield, including in the USA [15]. A network of instruments may gather information and transmit it to the Internet. The knowledge acquired on present climatic variability is significant and provides an opportunity to develop a palm strategy for creative agricultural management [8]. As the IoT and connected infrastructures are integrated into farms, the farm sector will increasingly depend on many platforms and devices to monitor and improve operations. Integrating IoT technology into the agricultural business, on the other hand, raises the likelihood of multiple security threats

[28]. Due to minimal expenditures in cybercrime by property organizations, these threats still need to be addressed [26]. Despite the amount of research on cyberattacks in essential topics, the agricultural sector has yet to be managed by many investigators. Therefore, there is a need for more investigations.

Furthermore, the absence of financial resources and technical experience among public agricultural members will compound the situation. Foreign competitors and threats focus on emerging industries, which is a cause of concern for the agricultural business [10]. Through cyber-attacks on smart agricultural infrastructure, an adversary may be able to control and influence on-field gadgets and autonomous driving simultaneously. Attacks on suitable farms might make farming risky and unprofitable [12]. Agriculture may suffer from assaults that can cause widespread harm, such as flooding agricultural fields or overly spraying chemicals using intelligent robots. These kinds of attacks may result in poor nutrition and economic loss. Such large-scale orchestrated efforts, often called Cyber Agroterrorism, can potentially suffocate the country's agricultural productivity and economic development [29].

6. Findings

Cyberattacks such as the well-known "Night Dragon" attack demonstrate how an attacker might gain critical information from various petrochemical companies [2]. "Night Dragon" integrates social engineering and well-strategically planned targeting (see **Appendix A**). Another example is the harm done to a German steel factory by phishing scam hackers who got entry into the company's internal network and manufacturing activities [29]. Additionally, it seems unlikely that producers would recognize the potential loss and damage to crops that might result from the expanding number of World Wide Web devices [6]. Consequently, safeguarding a wide range of equipment in the precision agriculture environment has risen to the top of the agricultural industry's priority list. The Intelligence Community published a document underlining the relevance of intelligent farming and the privacy risks and dangers it presents to cyber-based infrastructures [1].

The article emphasizes the network security concept of authenticity, consistency, and accessibility in agriculture. It describes many precision agriculture systems, such as on-farm gadgets, position and distant inertial measurement units, and computer vision [1]. It also goes through the touched people, such as farmers, animal producers, and organizations that run or depend on agriculture. A potentially dangerous situation is also discussed in this article. Likewise, the safety concerns of using Sensing devices in agriculture have been thoroughly examined [1]. Attackers may launch various attacks, such as colossal disruption of services attacks with several IoT devices deployed on a slick farm. In 2016, the Mirai botnet launched numerous distributed denial-of-service attacks on connected home automation systems [1].

A successful attack on some of the world's most significant cities would have

had far-reaching repercussions globally [29]. Consequently, safeguarding massive online data centers is critical for ensuring reliable cyber-related connections and connectivity. However, perfectly logical and topographically distinct links may carry the same physiological connectivity via parallelism via a single optical fiber thread. The result is highly susceptible to the same harm agencies, even though they are perfectly logical and topographically distinct [6]. Consequently, a single attack may destroy several hundred thousand or even thousands of connections, thus removing many hubs from the system. Therefore, it is necessary to safeguard the regions where this may occur to maintain the stability of computer architecture [13]. As a result, this presents a massive challenge for seats critical to global defense but located in physically inaccessible regions.

The failure of an electric power grid seldom brings down a central Interfuses hub, and certainly not all of them simultaneously, especially since most centers are equipped with alternate sources of energy that can keep them working for lengthy periods [4] [5]. Most essential infrastructures in use today are experiencing substantial transformations due to technology and commercial advances [30]. With the increasing reliance on cyber technology to improve the effectiveness and efficiency of the foundation, the number of cyber-attack targets would inevitably expand. Legislators, programmers, and users have continuing difficulty [26]. All economically significant facilities invest in communication systems vulnerable to cyber-attacks [12]. The latter may be categorized by providing information and specialist skills to plan a conventional or computer hacker.

It is similar to corporate espionage strategies used to magnify the intentional damage caused by a violent attack [25]. For a brief time, these assaults hinder preventative or restorative responses, enabling them to harm major physiological components in the process. Consequently, this has proven to be the most challenging attack. It needs precise timing, similar performance, and a comprehensive and correct grasp of the organism's core microstructural and mechanical characteristics [15]. Complete decryption can significantly reduce the effectiveness of all online attacks on network infrastructure. In some cases, it can completely neutralize them, provided that operational staff with high concentrations of attentiveness and adherence are available and that protection subsystems are in place [27]. However, it is possible to exercise the opposite control in the design and operation of current technologies when considering the systematic approach of a hostile mind scheming computer hackers on these devices.

7. Future Research

Any extensive infrastructure network widely dispersed over a region would need many borderline mechanical hits on its most vulnerable networks to inflict long-term physical pain and damage to corporate strategy on the web [3]. For network providers and users on a community-wide scale, attacks on second hubs, power transmission lines, independent single-power turbines, crushers, and turbines may be cumbersome and costly due to service disruption. Still, they

only cause slight damage and significantly reduced reduction [10]. Furthermore, the destroyed Iranian centrifugal cascade's design and manufacturing were in bad condition, with defective components for such severely pressured equipment. It is unlikely that Stuxnet or any other computer malware would succeed over critical infrastructures that are designed and built to last [10].

Over the past twenty years, technical advancements in oil and gas management and computer technology networks have been followed by increased computer security incidents on more interconnected networks [25]. Attackers target vulnerable, exploitable devices or malware that attack networking applications to access critical facilities and technologies connected via networking [2]. Given the importance of the petroleum sector to the global economy and the diversity of critical systems often operated from remote locations, it is essential to understand and neutralize such attacks [2]. The US Department of Energy produced a Risk Management Guide for Power Generation, including the oil and gas industry [9]. Even though most of the methods are relevant to our notions, the article proposes a non-mandatory control measure for power generation that only sometimes connects with information security.

Some limitations prevented this item from reaching its full potential powers. For example, we selected to only look at articles published in English, French, and German during the searches rather than other languages. Furthermore, the search keywords used to locate relevant information may need to be narrower, failing to capture the whole body of knowledge in the context. Also plausible is that some bias exists in the media [12]. Any publication evaluation procedure is subject to reader bias, resulting in the inaccurate identification and deletion of relevant articles due to incorrect titles [6]. A decision was made to have group sessions to analyze various reports to avoid each material position dominating the discussion to cope with this situation. However, this, together with our attempts to include only books from large publishers and businesses that have reached an agreement, aims to reduce the likelihood of such issues [14].

Given the interdependence of numerous information-communications-technology (ICT) devices and other factors, the failure of one might have disastrous consequences for everyone else [14]. The government's responsibility for information security has been disputed in the USA for more than a year. However, developing a strategy is complex since municipal governments are the primary organizations responsible for implementing services for the people [15]. The necessary arrangements, like the Treatment, Works Owned Public-wise (POTWs), and water systems owned publicly (PWSs), should have required measures to avert or alleviate possessions on computer security. This study inspects both technical and methodological methods for shielding against computer hackers.

Most industrial businesses feel unlimited potential cyber security threats, making investing in protection against any other destructive attack unfeasibly expensive [4] [5]. Therefore, the current difficulty for this company is establish-

ing what remedies would be acceptable for promoting an appropriate exemption level in which they may provide proper functioning of their CPS with similar outcomes. However, while keeping their fundamental economic framework in mind, the A CPS in the industrial sector is necessary as a principal component analysis for assessing behavior across cyber security events [10]. The impact of participating in numerous managed protection tactics from the firm's viewpoint while having multiple protective features from the attacker's perspective is investigated in this study.

By the same token, it is reliable for studying the impact of specific scenarios in manufacturing technologies and enhancing business decisions; a comprehensive simulation model has been developed and considered for implementation [26]. As a result of many documented incidents in various industries in recent years, there has been a substantial increase in interest in determining the impact of computer hackers on industrial facilities [26]. [2] outlined several cybersecurity risks for industrial facilities and methodologies to evaluate such concerns. [9] emphasized the weaknesses of fabrication techniques, mainly when using STL documents in their operations, while [6] stresses the importance of changing the intended meaning of goods for manufacturing organizations.

In developing manufacturing hazards, scientists suggested a tree-based analysis technique for examining malware networks in the industrial sector. [10] proposed a simple monitoring method for improving product quality in Trojan-affected production facilities. Also recently investigated was the cyber security of SCADA firms in the high-tech sector, a growing concern [8]. Researchers have focused on the primary and ultimate aims of the attack and any potential flaws rather than assessing the repercussions. No general statistical methodology is available when analyzing information security trends in industrial settings [15].

8. Conclusions

Cyber-attacks are a danger to the USA's infrastructure, especially electricity production, a primary national concern. Information Security Studies offer integrated techniques to minimize cyber risks in the energy business in the USA, according to research published in the journal Information Security Studies [7]. This research aims to identify the goals, objectives, and tactics implemented to reduce the likelihood of power outages caused by cyber-attacks [7]. In our advanced technological society, sustainable power and electricity are necessary for critical processes in mobility, health, telecommunications, banking, food production, emergency workers, and more [6]. Any cyber-attack today can interrupt the electricity supply, cause damage to highly sophisticated equipment, and endanger human health and well-being.

The administration and cyberspace security components of cyber security holes are the most addressed as they are evident in two of the three situations studied. However, it is significant to remember that even with the supplied framework for identifying cybercrime model characteristics, more than six prin-

ciples are required to encompass all vital power generation features. The latter's uniqueness is due to the interconnectedness and convergence of IT and OT contexts required for complete system monitoring. Therefore, although no formulas exist that provide appropriate criteria for assessing the effectiveness of information security on essential power generation, this study may be used as an example of the many factors to examine.

Due to the seeming inability to manage participants' responsibility and the difficulty in authenticating the identities of competent adults, treaty commitments intended to resolve the problem have had only a limited impact [2]. According to some scientists, the improvement in data transmission and the necessity to communicate information swiftly and appropriately about attacks with damaged persons gives a solid foundation for constructing a system to prevent future attacks efficiently. However, only a few nations conduct this practice consistently [1]. Indeed, authorities, corporations, and individuals must make significant efforts to become more cyber-vigilant, which means anticipating and protecting against cyber-attacks and training employees.

In addition, corporations and governments must engage in more meaningful community cooperation to address the issue [14]. For example, Decree 13636 ("Enhancing Essential Infrastructures Computer Security"), signed by President Barack Obama in February 2013, called for the creation of a consensual possibility information security architecture between the public and private sectors, among other things and set forth several other requirements [14]. This methodology allows all government organizations in the USA to secure critical infrastructures using the most effective risk mitigation measures, regardless of their geographic location or cyber-security capabilities [3]. In this structure, the most significant feature is that it allows all those willing to communicate effectively and understand the hazards to do so effectively and grasp the threats, which is vital for establishing national and international cyber-security networks [2].

Most cyber-attacks have occurred in areas with developing infrastructure. Infrastructure remains the primary target for many computer hackers because they feel it is more productive than other targets [13]. As a result, it is difficult for academics to conduct a comprehensive study on the hazards presented to infrastructure by cyber-attacks, which is a perplexing task in and of itself. Researchers are forced to choose just one issue from the vast infrastructure information and discuss it due to this need [4] [5]. Since the subject is extensive, and many sub-topics still need to be addressed, it is recommended that aspiring researchers focus their studies on areas where prior studies have yet to be conducted [8]. Those exploring this subject in the future should do it on the current concerns discussed.

Acknowledgements

I want to express my special appreciation to my committee member and Chair, Dr. Ian A. McAndrew, FRAeS, Dean of Doctoral Programs and Engineering Faculty. I am grateful for Dr. McAndrew's timeless support in encouraging my

research and writing to continue developing as a scientist and pursuing a third doctorate. Dr. McAndrew's advice on research and academia remains priceless. I would also like to thank Carmit Levin for her enduring support-furthermore, thanks to my cousin, Ms. Maria Boston, whose academic inputs were invaluable.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Major, M., Romero-Mariona, J., Phipps, R., Tacliad, F., Slayback, S.M., Romero, E. and Hallman, R.A. (2020) Towards Quantifying Energy Resiliency through Return on Cyber Investment Modeling. 2020 *HICSS Symposium on Cybersecurity Big Data Analytics*, Hawaii, 7 January 2020.

[2] Plėta, T., Tvaronavičienė, M., Casa, S.D. and Agafonov, K. (2020) Cyber-Attacks to Critical Energy Infrastructure and Management Issues: Overview of Selected Cases. *Insights into Regional Development*, **2**, 703-715. https://doi.org/10.9770/IRD.2020.2.3(7)

[3] Hemsley, K. and Fisher, R. (2018) History of Cyber Incidents and Threats Involving Concern for Decision-Makers. In: Gardoni, P., Ed., *Routledge Handbook of Sustainable and Resilient Infrastructure*, Routledge, London, 359-374.

[4] Maglaras, L.A., Kim, K.H., Janicke, H., Ferran, M.A., Rallis, S., Frank, P., Cruz, T.J., *et al.* (2018) Cyber Security of Critical Infrastructures. *ICT Express*, **4**, 42-45. https://doi.org/10.1016/j.icte.2018.02.001

[5] Maglaras, L., Ferrag, M., Derhab, A., Mukherjee, M., Janicke, H. and Rallis, S. (2018) Threats, Countermeasures and Attribution of Cyber-Attacks on Critical Infrastructures. *EAI Endorsed Transactions on Security and Safety*, **18**, e1. https://doi.org/10.4108/eai.15-10-2018.155856

[6] Miller, T., Staves, A., Maesschalck, S., Sturdee, M. and Green, B. (2021) Looking Back to Look Forward: Lessons Learned from Cyber-Attacks on Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, **35**, Article ID: 100464. https://doi.org/10.1016/j.ijcip.2021.100464

[7] Chadwick, D.W., Fan, W., Costantino, G., De Lemos, R., Di Cerbo, F., Herwono, I., Wang, X.S., *et al.* (2020) A Cloud-Edge-Based Data Security Architecture for Sharing and Analyzing Cyber Threat Information. *Future Generation Computer Systems*, **102**, 710-722. https://doi.org/10.1016/j.future.2019.06.026

[8] Lamba, A. (2018) Protecting "Cybersecurity & Resiliency" of Nation's Critical Infrastructure—Energy, Oil & Gas. *International Journal of Current Research*, **10**, 76865-76876. https://doi.org/10.2139/ssrn.3535434

[9] Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A. (2020) Cyber Security Risks in Globalized Supply Chains: A Conceptual Framework. *Journal of Global Operations and Strategic Sourcing*, **13**, 103-128. https://doi.org/10.1108/JGOSS-05-2019-0042

[10] CIO (2011) Night Dragon Brings Security Vulnerabilities into the Boardroom. https://www2.cio.com.au/article/376330/night_dragon_brings_security_vulnerabilities_into_boardroom/

[11] Al-Abassi, A., Karimipour, H., Dehghantanha, A. and Parizi, R.M. (2020) An En-

semble Deep Learning-Based Cyber-Attack Detection in the Industrial Control System. *IEEE Access*, **8**, 83965-83973. https://doi.org/10.1109/ACCESS.2020.2992249

[12] Harry, C. and Vivek, S. (2021) Strategic Cyber Effects in Complex Systems: I understand the US Air Transportation Sector. 2021 13*th International Conference on Cyber Conflict* (*CyCon*), Tallinn, 25-28 May 2021, 111-131. https://doi.org/10.23919/CyCon51939.2021.9468293

[13] Bracho, A., Saygin, C., Wan, H., Lee, Y. and Zarreh, A. (2018) A Simulation-Based Platform for Assessing the Impact of Cyber Threats on Intelligent Manufacturing Systems. *Procedia Manufacturing*, **26**, 1116-1127. https://doi.org/10.1016/j.promfg.2018.07.148

[14] Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E. and Bonacina, S. (2021) Influence of Human Factors on Cyber Security within Healthcare Organizations: A Systematic Review. *Sensors*, **21**, Article 5119. https://doi.org/10.3390/s21155119

[15] Clark, R.M., Hakim, S. and Panguluri, S. (2018) Protecting Water and Wastewater Utilities from Cyber-Physical Threats. *Water and Environment Journal*, **32**, 384-391. https://doi.org/10.1111/wej.12340

[16] Koblentz, G.D. (2020) Emerging Technologies and the Future of CBRN Terrorism. *The Washington Quarterly*, **43**, 177-196. https://doi.org/10.1080/0163660X.2020.1770969

[17] Gupta, S., Starr, M.K., Farahani, R.Z. and Ghodsi, M.M. (2020) Prevention of Terrorism—An Assessment of Prior POM Work and Future Potentials. *Production and Operations Management*, **29**, 1789-1815. https://doi.org/10.1111/poms.13192

[18] Carroll, P. and Windle, J. (2018) Cyber as an Enabler of Terrorism Financing, Now and in the Future. *Journal of Policing, Intelligence and Counter Terrorism*, **13**, 285-300. https://doi.org/10.1080/18335330.2018.1506149

[19] Howcroft, J. (2018) The Future of Terrorism: The Practitioners' View. *Connections: The Quarterly Journal*, **17**, 77-81. https://doi.org/10.11610/Connections.17.2.06

[20] Schuurman, B. (2019) Topics in Terrorism Research: Reviewing Trends and Gaps, 2007-2016. *Critical Studies on Terrorism*, **12**, 463-480. https://doi.org/10.1080/17539153.2019.1579777

[21] Horgan, J.G. (2017) Psychology of Terrorism: Introduction to the Special Issue. *American Psychologist*, **72**, 199-204. https://doi.org/10.1037/amp0000148

[22] Okoye, I.E. (2018) Trends in Terrorism Incidents in Nigeria and the United States: Analysis of Data from 1980-2013. *International Journal of Criminal Justice Sciences*, **13**, 200-211.

[23] Bø, S. and Wolff, K. (2019) A Terrible Future: Episodic Future Thinking and the Perceived Risk of Terrorism. *Frontiers in Psychology*, **10**, Article 481506. https://doi.org/10.3389/fpsyg.2019.02333

[24] Coccia, M. (2018) The Relation between Terrorism and High Population Growth. *Journal of Economics and Political Economy*, **5**, 84-104. https://doi.org/10.15664/jtr.1469

[25] Albahar, M. (2019) Cyber-Attacks and Terrorism: A Twenty-First-Century Conundrum. *Science and Engineering Ethics*, **25**, 993-1006. https://doi.org/10.1007/s11948-016-9864-0

[26] Tonn, G., Kesan, J.P., Zhang, L. and Czajkowski, J. (2019) Cyber Risk and Insurance for Transportation Infrastructure. *Transport Policy*, **79**, 103-114. https://doi.org/10.1016/j.tranpol.2019.04.019

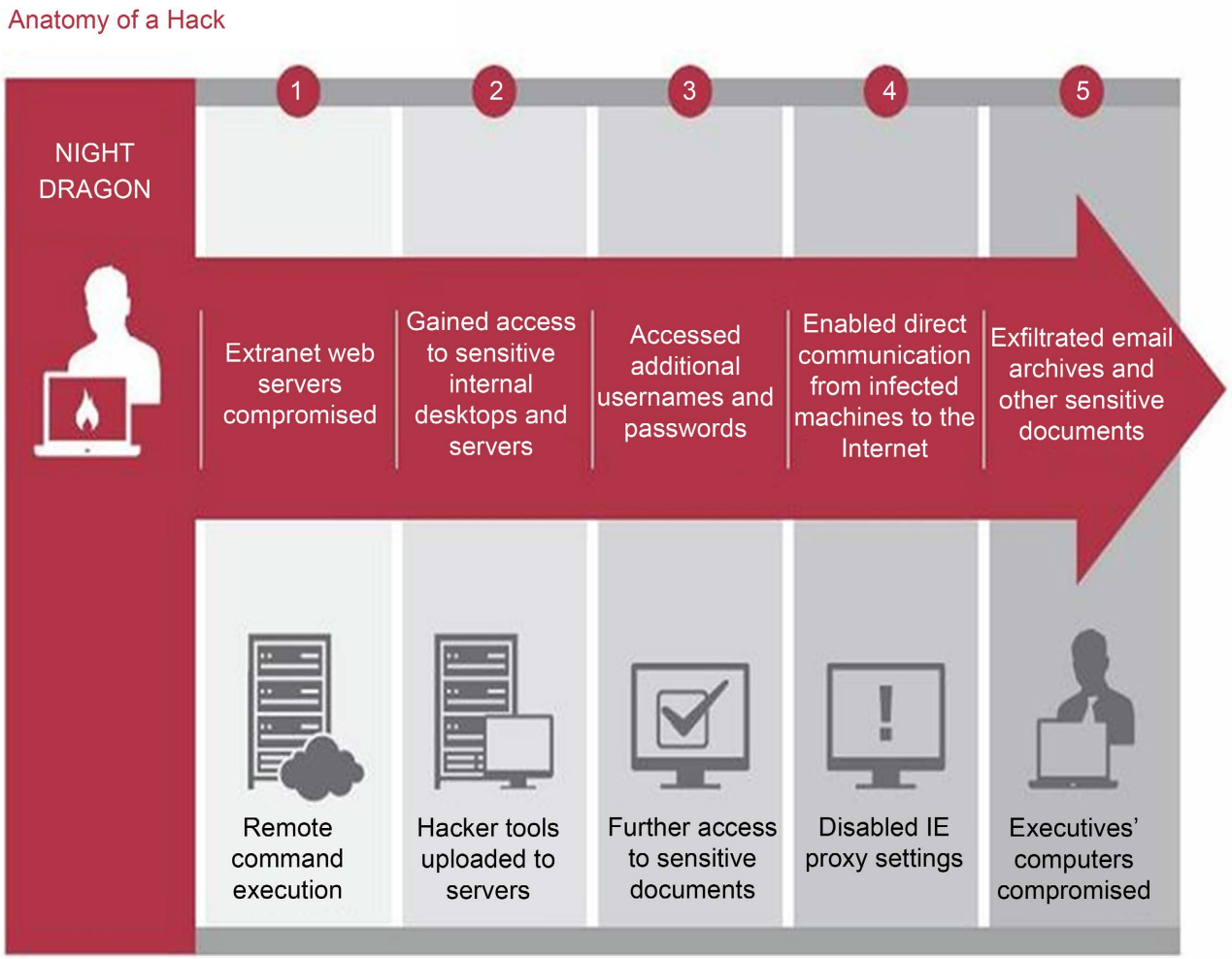
[27] Kammouh, O. and Cimellaro, G.P. (2018) Cyber Threat on Critical Infrastructure: A Growing Concern for Decision-Makers. In: Gardoni, P., Ed., *Routledge Handbook of Sustainable and Resilient Infrastructure*, Routledge, London, 359-374. https://doi.org/10.4324/9781315142074-19

[28] Alcaide, J.I. and Llave, R.G. (2020) Critical Infrastructures Cybersecurity and the Maritime Sector. *Transportation Research Procedia*, **45**, 547-554. https://doi.org/10.1016/j.trpro.2020.03.058

[29] Sontowski, S., Gupta, M., Chukkapalli, S.S.L., Abdelsalam, M., Mittal, S., Joshi, A. and Sandhu, R. (2020) Cyber-Attacks on Smart Farming Infrastructure. 2020 *IEEE 6th International Conference on Collaboration and Internet Computing* (*CIC*), Atlanta, 1-3 December 2020, 135-143. https://doi.org/10.1109/CIC50333.2020.00025

[30] Stergiopoulos, G., Gritzalis, D.A. and Limnaios, E. (2020) Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. *IEEE Access*, **8**, 128440-128475. https://doi.org/10.1109/ACCESS.2020.3007960

Appendix A. Anatomy of a Hack-Night Dragon



Note: Adapted from Night Dragon brings security vulnerabilities into the boardroom (2011, February 11). CIO. https://www2.cio.com.au/article/376330/night_dragon_brings_security_vulnerabilities_into_boardroom/.