Digital Innovations
& Contemporary Research in SCIENCE,
ENGINEERING & TECHNOLOGY
Vol. 10. No. 4, December 2022 – Special Issue on Cryptography & Security Mechanisms

Article Citation Format
Kwaku, T. (2022): Securing Critical National Infrastructure Against
Hacktivist. Journal of Digital Innovations & Contemporary Research in
Science, Engineering & Technology.
Vol. 10, No. 2. Pp 33-42
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N4P5

Securing Critical National Infrastructure Against Hacktivist

Kwaku Timothy
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: Kwaku.timothy@st.gimpa.edu.gh
Phone: +233244287747

ABSTRACT

The acts of hacktivists in today's modern world might have extremely negative repercussions for the order and peace of countries. Hacktivists, by the very nature of their methodology, invariably target important government installations. This research focuses mostly on investigating the myriad of approaches that may be taken to cyber-secure important national infrastructure against the maneuvers that can be carried out by hacktivists. Inferences are drawn in this study from hacktivism episodes that occurred in the past and were documented by a variety of sources, some of which may be verified. A four-point cyber security plan for important national infrastructure has been developed as a way to provide direction for the execution of cybersecurity measures by key state facilities. This scheme was inspired by the ideas presented previously.

Keywords: Critical National Infrastructure, Security, Hacktivists, Cyberspace, Hacking, Cybercrime

1. INTRODUCTION

The proliferation of internet access and internet compliant devices has increased the possibilities of various cyber-attacks. The internet in this modern era through the use of social media and others have been disruptive as a lot of political and economic uprising have been triggered. Cyberspace, as it is often known, has evolved into "a general-purpose technology that contributed almost 4 trillion US dollars to the world economy in 2016 and links nearly half of the world's population." (Joseph S. Nye Jr, 2017). Hacktivism refers to several types of online and computer activism, mostly on the Internet. The terms "hacker" and "activism" were combined to create the phrase. Although hacktivism has developed into a distinct area of study in activism, the phrase has not yet achieved complete acceptance. This is because, on the one hand, activism may use a variety of tools created by hackers, while, on the other side, hackers can further their own goals (Уринов et al., 2020).

The intents of these hacktivists are potentially unguided and could be a source of mayhem. By extension, for improved security state agencies and cybersecurity outfits are mostly challenged to monitor and curb any possible intrusion of such unscrupulous individuals. The term "Critical National Information Infrastructure" (CNII) refers to those resources—both actual and virtual—as well as systems and operations that are so crucial to a country's survival that their loss or destruction would be catastrophic on National economic strength, National image, National defense and security, Government capability to functions, and Public health and safety (MOC, 2014).

It is therefore imperative that all state machinations are garnered to ensure the security of critical national infrastructure. CNII's could be targets of anti-national agents and terrorists. In the context of the global threat environment, cyberattacks intended at critical national infrastructure represent a risk-element that is not only large but also diversified and quickly on the rise. Because of their high inherent worth and inherent weaknesses, critical infrastructures are susceptible to cyber-attacks. These attacks have the potential to cause extensive damage to the countries that they are directed towards. Threats to the cyber security of critical infrastructures can originate from a wide variety of potential actors, including state-sponsored espionage and sabotage, international terrorism, domestic militants, malevolent "hacktivists," and even disgruntled employees working for the targeted organization (Rudner, 2013). This research basically surveys and explores various technological interventions whose implementation will ensure improved security of critical national infrastructure.

Problem Statement

The vulnerability of critical infrastructure to cyber-attacks and technical failures has become a big concern. There have been various instances where critical national infrastructure became subjects of cyber-attacks leading to incalculable losses. The first reported power outage brought on by a hostile cyberattack occurred in December 2015. BlackEnergy virus infected three Ukrainian utility providers, cutting off the energy to hundreds of thousands of households for six hours. The malware, which was likely started by a phishing attempt, was targeted at the power companies' SCADA (supervisory control and data acquisition) systems, said cyber security company Trend Micro.

Two months after the blackout, the Israel National Electricity Authority was revealed to have had a significant cyberattack; however, damage was limited after the Israel Electricity Corporation shut down systems to stop the virus from spreading(Kovacevic & Nikolic, 2016). These cyber attacks accrue a lot losses across different sectors. According to IBM Security's annual Cost of a Data Breach Report, a health-care data breach now has a record-high price tag of $10.1 million on average (Lohrmann, 2022). There is therefore the need to explore the major critical national infrastructure attack, identify challenges and propose ways to improve the cyber security of critical national infrastructure.

Objectives

The underlying objective of this research is to explore the various ways to secure Critical National Infrastructure against the activities of hacktivists. By so doing, this research primarily:

1. Explores instances of various cyber attacks on critical national infrastructure
2. Establish lessons drawn from these cyber attacks
3. Propose ways to strengthen cybersecurity on various critical national infrastructure.

2. RELATED WORKS

As a result of the disruptive potential of new digital technologies, protecting vital infrastructure from cyber-attacks is a concern for policy. Since cybersecurity is typically a private work but a public obligation, governments must make a tough decision: Should they structure their capacities hierarchically or rely on partnerships with private businesses? Choices, according to (Weiss & Biermann, 2021), rely on the institutional environment and the nature of the situation.
Their comparison of France's system of state capitalism with that of the United Kingdom's system of market capitalism supports the notion that the former controls intermediaries more hierarchically and that both governments take a more assertive stance when defending against threats than when managing risks. According to (Ashrafuzzaman et al., 2018), a crucial national asset that is always at risk from cyberattacks is the electric power system. A number of crucial control procedures in a power transmission system are built on state estimate (SE). These control procedures can be interfered with by a fake data injection (FDI) attack on SE, which would cripple a power system and cause mayhem in the area. A cyber-attacker may create and carry out covert FDI assaults that are highly challenging to detect with knowledge of the system structure. For the SE of the power grid, statistical and, more recently, machine learning algorithms have been used to identify FDI assaults.

In their paper, they provide a Deep Learning (DL) based technique to precisely identify covert FDI assaults on the SE of the power grid. They contrast the effectiveness of the DL approach with three well-known machine learning algorithms: distributed random forests, generalized linear modelings, and gradient boosting machines (DRF). The IEEE 14-bus system simulation dataset was examined by all four approaches. The results suggest that these algorithms successfully identify covert FDI assaults on the smart grid, with the DL-based technique achieving the greatest results.

(Romagna & Jan van den Hout, 2017)analyses hacktivists' motives and methods qualitatively. Website defacers appear to have diverse ideological and psychological objectives. Although socio-political incentives seem to be the most influential, thrill-seeking and self-esteem boosts also matter. Hacktivists employ common weaknesses and methods, according to the report. They also design and use public tools. Targets seem to be picked depending on how simple they are to hack or how much attention the defacement would gain. Their study reviews the literature and interviews hacktivists and cybersecurity specialists. The researchers analysed forensic data from an ad hoc honeypot server and technical data from over 7 million defacements from the Zone-H Defacement Archive.

The primary goal of protecting vital infrastructure has often been to defend against environmental risks. The rise of cyber assaults, however, has shifted the emphasis; infrastructures now face a distinct threat that might have fatal repercussions and result in substantial financial losses. It is evident that the volume of novel and developing assaults is outpacing the effectiveness of traditional security measures. Infrastructure security needs new, flexible solutions. Critical infrastructures and the cyberthreats they face were examined in (Butts & Shenoi, 2014) article, which also offers insights on present and foreseeable infrastructure security measures. The specific measures are explored later on in this research as part of its literature inspiration.

3. METHODOLOGY

A literature review that makes use of several search indexes has been chosen as the approach to be utilized in this investigation. The search interest focused on key national infrastructure, cyber security risks, and interventions on state infrastructure and websites. Verifiable and standard sources of literature were sifted through in order to find relevant information. Google Scholar, the ACM Digital Library, IEEE Xplore, ResearchGate, and a multitude of other online databases were among the sources that were consulted.

4. CYBER-ATTACKS ON CRITICAL NATIONAL INFRASTRUCTURE

The concept of e-governance as adapted by most governments around the world has migrated a lot of essential government services to the web. Critical sectors such health care, recruitment, revenue collection and other functions have been moved to various online media. In this session, we chronicle a list of cyber attacks on government websites, the world and over based on established literature. This essentially gives a perspective for the better appreciation of government targeted cyber-attacks.

Prominent among these government website attacks was when Russia Numerous state government websites were taken offline as a result of a wave of cyberattacks that were claimed by Russian hackers. The politically driven cyberattacks that started on Wednesday, October 6th, had an effect on a number of states, including Colorado, Connecticut, Kentucky, and Mississippi. The hacktivist organization Killnet, which utilizes Distributed Denial of Service (DDoS) assaults to take its targets offline, is the cybercrime gang that took credit (Alicia, 2022). Another instance of hacktivism was the discovery of the Mysterious Team Bangladesh (MT) hacktivism organisation by the AI-driven cyber intelligence and threat detection firm CloudSEK, which was targeting servers and websites operated by the Indian government.The organisation allegedly conducted DDoS (Distributed Denial of Service) assaults against domains and subdomains of multiple state governments as well as an Indian government-hosted web server, according to CloudSEK.

Assam, Madhya Pradesh, Uttar Pradesh, Gujarat, Punjab, and Tamil Nadu governments' websites were impacted. The assaults were discovered after a Mysterious Team Bangladesh (MT) member going by the moniker "D4RK TSN" posted on Pastebin on July 12 claiming to have carried out an HTTP flood DDoS attack against Indian government websites. Similar posts may be seen on Facebook, Pastebin, and Telegram, among other sites(Pihu, 2022).

The security of government websites cannot be compromised due to the sensitive data and operations that they perform. Even in recent times, there have been targeted cyber attacks on various websites. Notable among these attacks was the cyber attack on Albania in September 2022. Albanian officials were forced to temporarily shut down the Total Information Management System, a programme used to track people entering and leaving Albania, as a result of Iranian hackers attacking Albanian computer networks. This strike came shortly after Albania decided to break diplomatic relations with Iran, as well as after NATO and the United States both denounced an Iranian cyberattack on Albania in July. Albanian government networks were subjected to a ransomware attack in July by Iranian attackers, which damaged data and interrupted government services (CSIS, 2022).

Critical National Infrastructure Security threats

As grounded in literature, this session outlines the myriad of security issues of government and critical national infrastructure.Rudner, 2013 addressed cyber threats to critical national infrastructure from an intelligence perspective. According to his analysis, there is a diverse group of potential attackers that pose a risk to the cyber-security of vital facilities. Some of the security threats listed were:

State-Sponsored Espionage and Sabotage:

A state-sponsored assault (SSA) is a cyberattack launched by hackers with ties to a certain government. Their objectives are threefold: to get financial gain, to gain intelligence, and to locate and exploit weaknesses in the nation's infrastructure.

International terrorism:

Violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations (state-sponsored).

Malevolent ‘‘Hacktivists,’’

An emerging concern is the malicious use of cybertechnology, sometimes known as "hacking," to target the computer systems of others. However, malicious hacking by cyber-activists, or "hacktivists," who target critical infrastructure assets can pose a serious threat to national security. Whereas most incidents of hacking into computers or computer networking appear to be motivated by criminality, protest, or an ipso facto technical challenge. For instance, international oil firms have warned that the more frequent and precisely targeted cyberattacks by hackers, who are typically driven by criminal or economic motives, might cause worldwide devastation by disrupting the supply of oil.

Due to health and human safety considerations, critical infrastructure firms have some of the highest uptime standards, making them even more available than banking or healthcare. Governments and regulatory agencies all around the world are paying close attention to security breaches in this industry because they may be so damaging to society. (Thales_Data_Threat, 2022) summarizes some of the most significant findings of the 2022 Thales Data Threat Report Critical Infrastructure Edition, which includes responses from 300 security leaders and practitioners within critical infrastructure organizations, and offer suggestions for lowering the risk of attacks like ransomware and malware in the closing paragraphs. Summarily, they listed the following as the cyber-security threats or issues to critical national infrastructure:

Remote Working Worsens the “Human Factor” Weakest Link

Unsurprisingly, the "human aspect" is cybersecurity's weakest link. Most malware and ransomware assaults start with human mistake. This involves utilising easy-to-guess passwords, phishing, and business email infiltration. Large-scale moves to "hybrid" working arrangements—a mix of working remotely and in regular offices—have aggravated this dilemma. The integration of IT and OT makes it simpler for attackers to move laterally through enterprises, converting IT problems into more serious OT system difficulties.

Malware and Ransomware Attacks Increase and Become More Complex

Malware (55%), followed by ransomware (53%), was the largest source of security assaults in critical infrastructure firms. Transportation businesses reported larger malware growth (65%) and lower ransomware (45%) than normal, whereas trucking and shipping reported significantly lower malware (32%) but much higher ransomware (64%). Compared to 20% overall, 19% of critical infrastructure responders reported ransomware attacks. Transportation and energy/utilities respondents reported even smaller ransomware assaults, 17% apiece.

Breaches and Failed Audits Are a Continuing Problem

In the previous year, cyberattacks have increased in volume, intensity, and/or breadth, according to 44% of respondents. A security breach affected more than one-third of respondents (39%) in the last year, which is 6% more than the average. A breach affected 51% of respondents at some time in the past, which is 3% more than the average.

Diverse Data Protection Strategies Need Better Alignment and Common Direction

In order to use the proper security safeguards, the first stage in a data protection plan is to determine where data is kept, followed by classification. An amazing 57% of respondents, which is 4% more than the norm, stated they are completely aware of or extremely sure that they are aware of where their data is held. However, just 28% of respondents—6% less than the average—said they could fully categorize their data, only 49%—6% more—believed they could identify at least half of it.

Zero Trust Adoption Continues, Particularly in Cloud Environments

Distributed warehouses, shipping ports, electricity lines, vehicles, transmission sites, and train assets are characteristic of critical infrastructure businesses. Zero trust can ensure "least privilege" access to massively dispersed, high-value data and assets. The move from proprietary, dedicated connections to IoT has substantially increased the size, complexity, and flexibility of underlying networks and raised attack surfaces. Zero trust works nicely in these contexts.

Cloud Apps and Data Continue to Grow, Increasing Attack Surfaces and Complexity

In a stacked survey question, respondents named cloud-based storage, databases, and apps as their top attack targets. 54% of respondents said that more than 60% of their cloud data is sensitive. Most respondents have several cloud (IaaS) providers, which might complicate cloud security.

5. THE FOUR (4-POINT) SECURITY SCHEME FOR CRITICAL NATIONAL INFRASTRUCTURE

From the series literature considerations and appreciation of the nature of cyber attacks on critical national infrastructure, this research proposes a 4-point security scheme to guide the implementation of cyber security policies.

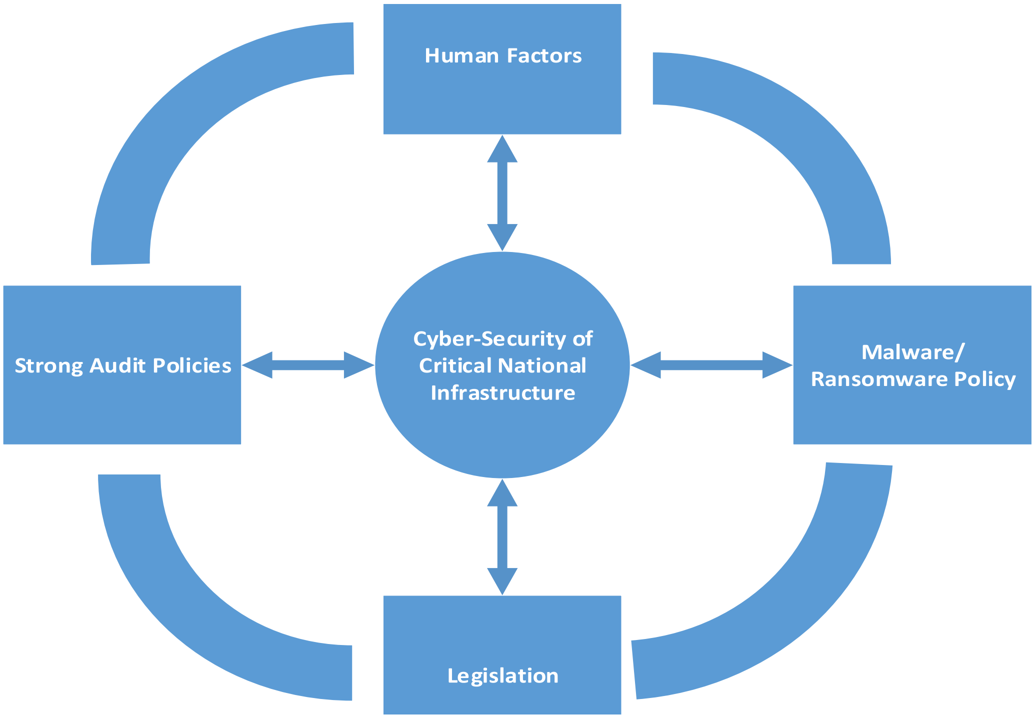
Human Factors
Strong Audit Policies
Cyber-Security of Critical National Infrastructure
Malware/ Ransomware Policy
Legislation

Fig.1 The four-point cyber security scheme for Critical National Infrastructure

Figure 1 represents a conceptual overview of the 4-point Security Scheme for Critical National Infrastructure. It should be noted that a coordinated harmony of these factors will necessarily make any national cyber-security police for critical national infrastructure more robust and reliable.

Human Factors

As stated previously, the carelessness of a human user could be the weakest link in an otherwise extremely powerful and comprehensive cyber-security system. This is because human users are fallible. There are users who can use easy passwords, leave their workstations unlocked, and a whole lot of other things. Users of state systems should be required to go through training that is both rigorous and comprehensive in nature. Users of important government systems need to have their hands-on expertise properly covered by the training, which should include realistic simulated exercises and situations that have been well planned out. Training and retraining of both necessary and non-essential staff at such national sites should be included as part of the human factors component of the four-point cyber-security system. This training should take place on a regular and periodic basis.

Malware/Ransomware Policy

The consequences of malware and ransomware attacks on cyber-systems can be very costly and posses a risk of huge data leaks and breaches. A ransomware assault carried out by the cybercriminal group DarkSide was responsible for the recent suspension of the Colonial Pipeline, which halted the flow of 2.5 million barrels of oil product. This incident received a lot of media attention.

This incident took place during the beginning of May 2021 and resulted in a ransom payment of $4.4 million that was made entirely in cryptocurrency. After some time, a portion of the ransom was paid back (Unearth, 2022). Organizations should implement the following common safeguards as they promote a culture of cybersecurity:

Malicious software is eliminated by anti-malware software after scanning your devices for dangers. SIEM (Security Information and Event Management): Guards against malicious software and keeps track of network activities and access. A firewall is a digital barrier that analyses, assesses, and filters incoming communication between internal systems and the outside world. Trust Zones: Extra firewalls created for your internal network to safeguard critical data that needs more protection. Encrypt data on your devices and the communications between them, which is especially important for IoT systems like smart grids and smart metres. Employees must enter a network or system using more than just a password when using multi-factor authentication.The corporation may decide to work with a cybersecurity firm or consultant as well. Big data and AI are also increasingly being utilised to monitor networks. If you've already implemented these best practises, start executing a cogent Zero Trust approach that treats internal risks as if they have already been compromised.

Strong Audit Policies

A cybersecurity audit is a technique for ensuring that your company has security procedures in place to handle all potential dangers. Internal staff members might conduct an audit to get ready for an outside organization. You will need to hire an external auditor to confirm compliance and obtain a certification if your organization is subject to legal requirements like the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), or ISO 27001.

A cybersecurity assessment isn't the same as a cybersecurity audit. An assessment evaluates the risk to see how well it is executed, whereas an audit uses a checklist to confirm you have addressed a particular risk. The methodology that ensures a strong audit policy includes the following:

- Develop a security policy.
- Review and cross-check your cybersecurity policies.
- Strengthen your network structure.
- Review and apply business compliance standards.
- Review and apply employee workplace standards.
- Conduct and internal cybersecurity audit.

Legislation

Cyber laws are in place to safeguard customers from being defrauded when shopping online. They are designed to prevent crimes committed online, such as the theft of credit card information and identity. Thefts of this nature can result in criminal charges being brought against the perpetrator at both the state and federal levels. Various countries have passed legislation to ensure proper usage of internet facilities. The penalty for breaking such laws are strategically crafted to deter Hacktivists from pursuing any unscrupulous activity. Act 1038, also known as the Cybersecurity Act of 2020, was passed in Ghana in order to assist in the development of cybersecurity and to respond to difficulties in this area. The Cyber Security Authority, also known as the CSA, was established in advance of the law's going into effect in order to ensure that it is followed and to maintain order within the country's cybersecurity ecosystem.

6. RECOMMENDATIONS

All businesses today should have an end-to-end strategy for their critical infrastructure's cyber resilience, especially if they are part of one of the 16 industries that CISA has designated or are connected to those industries. This entails putting an emphasis on risk reduction, being proactive, and making sure that the business can react quickly to any threat or threatening situation. A variety of technologies and services, such as secure cloud architecture, disaster recovery, cyber recovery, data protection, privacy protection, and more, may and should be included in end-to-end cybersecurity for critical infrastructure. Consider the following key attributes, developments, and abilities:

Secure cloud architecture: One key step in lowering risk for critical infrastructure is the ability to control all cloud resources from a single unified plane. The organization's cloud security and networking rules are ensured by having a single operational centre for all clouds, allowing IT teams to identify, defend, detect, respond, and recover with more confidence, speed, and knowledge. Organizations may validate people, devices, applications, data, and transport sessions using a zero trust architecture before allowing them access to the network, other users, apps, data, or the cloud. Accelerate and Simplify Your Journey to a Zero Trust Architecture, a related article.

Solutions and services for modern data security and cyber recovery are necessary to ensure the vital infrastructure is resilient to successful assaults and other possible catastrophes. Having systems and services in place to recover rapidly with the least amount of harm to data, systems, and applications is also important.

Consider solutions like Dell Technologies PowerProtect Cyber Recovery, which provides a cyber recovery vault and uses an automatic operational air gap to maintain a backup that is both physically and logically separated from any incursions, in order to address these difficulties. security that is inherent to all supply chains and ecosystems. Supply chain assurance is the first step towards intrinsic security. For instance, the manufacturing procedures used by Dell Technologies include several levels of controls to reduce any hazards that may be introduced into the supply chain. Dell SafeID is another illustration; it isolates user credentials from the operating system and memory. Make sure the servers you use have robust security measures, such as protected component verification and protection against BIOS modification. Moreover, safeguard your users' and your devices' endpoints with an integrated endpoint security solution like VMware Carbon Black Endpoint.

Automation and intelligence are used to drive detection, inquiry, and reaction. Any contemporary cybersecurity plan for critical infrastructure must include unified threat detection and response technologies, secure networking options like SD-WAN and Secure Access Service Edge (SASE), and other components. In order to keep security up to date, solutions should be able to continually update threat information and give end-to-end visibility and actionable insight throughout your whole ecosystem. Utilizing a service-based paradigm for extended disaster recovery security and real-world, actionable threat intelligence, enterprises can monitor, identify, analyse, and respond to threats across the whole IT environment with a solution like Dell Technologies Managed Detection and Response. State agencies summarily, must invest heavily in any robust framework or policy that ensures adequate protection of critical national infrastructure.

REFERENCES

Alicia, H. (2022, October 12). *Russian Hackers Shut Down Dozens of State Government Websites in DDoS Attacks - CPO Magazine*. CPO Magazine. https://www.cpomagazine.com/cyber-security/russian-hackers-shut-down-dozens-of-state-government-websites-in-ddos-attacks/

Ashrafuzzaman, M., Chakhchoukh, Y., Jillepalli, A. A., Tosic, P. T., De Leon, D. C., Sheldon, F. T., & Johnson, B. K. (2018). Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning. *2018 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018*, *June*, 219–225. https://doi.org/10.1109/IWCMC.2018.8450487

Butts, J., & Shenoi, S. (2014). Critical infrastructure protection VIII: 8th IFIPWG11.10 international conference, ICCIP 2014 Arlington, VA, USA, March 17-19, 2014 revised selected papers. *IFIP Advances in Information and Communication Technology*, *441*(February 2018). https://doi.org/10.1007/978-3-662-45355-1

CSIS. (2022). Significant Cyber Incidents | Center for Strategic and International Studies. In *Center for Strategic and International Studies*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Joseph S. Nye Jr. (2017). Deterrence and Dissuasion in Cyberspace. *International Security 41*, *24*(1), 7–53. https://doi.org/10.1162/ISEC_a_00266

Kovacevic, A., & Nikolic, D. (2016). Cyber Attacks on Critical Infrastructure. In *Civil and Environmental Engineering* (pp. 448–465). https://doi.org/10.4018/978-1-4666-9619-8.ch018

Lohrmann, D. (2022). *Cyber Attacks Against Critical Infrastructure Quietly Increase*. LOHRMANN ON CYBERSECURITY. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-attacks-against-critical-infrastructure-quietly-increase

MOC. (2014). *Ghana National Cyber Security Policy and Strategy*. *March*, 1–49.

Pihu, Y. (2022). *Hacktivist Group From Bangladesh Launches Cyber Attack On Indian Government Websites*. CNBC. https://www.cnbctv18.com/technology/hacktivist-group-from-bangladesh-launches-cyber-attack-on-indian-government-websites-14782721.htm

Romagna, M., & Jan van den Hout, N. (2017). Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats P. *Proceedings of the 27th Virus Bulletin International Conference*, *October 2017*, 41–50. https://www.researchgate.net/publication/320330579

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3), 453–481. https://doi.org/10.1080/08850607.2013.780552

Thales_Data_Threat. (2022). *2022 Thales Data Threat Report*.

Unearth. (2022). *5 Ways to Prevent Cyberattacks on Critical Infrastructure*. https://www.unearthlabs.com/blogs/cybersecurity-critical-infrastructure

Weiss, M., & Biermann, F. (2021). Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform*, *00*(00), 1–18. https://doi.org/10.1080/17487870.2021.1905530

Уринов, Н. Т., Сайидова, Н. К., & Юлдашев, Х. Д. (2020). CYBER THREATS AND VULNERABILITIES. *EPRA International Journal of Research and Development (IJRD)*. https://doi.org/10.36713/epra2016