NEWPORT INTERNATIONAL JOURNAL OF SCIENTIFIC AND EXPERIMENTAL SCIENCES (NIJSES)

Volume 6 Issue 1 Page 31-47, 2025

©NIJSES PUBLICATIONS
Open Access

ONLINE ISSN:2992-5819
PRINT ISSN:2992-6149

https://doi.org/10.59298/NIJSES/2025/61.3147

Safeguarding National Critical Energy Infrastructure using Cybersecurity Frameworks and Collaborative Approach for a Resilient Energy Future

Wesley O. Odumu[1], Barnabas I. Gwaivangmin[2] and Ademola P. Adewoye[3]

[1]**Department of Computer Engineering, School of Engineering Technology Plateau State Polytechnic, Barkin ladi Plateau State. (writeodeh@yahoo.com, +2348035988003)**
[2]**Department of Electrical and Electronic Engineering, Abubakar Tafawa Balewa University Bauchi, Bauchi State. (gwaivangminb@gmail.com, +2348027093429)**
[3]**Meglope Nig. Ltd, Zarazon New Layout, Jos Pateau State. (adewoyepeterademola@gmail.com, +2348055551473)**

ABSTRACT

The government heavy reliance on information communication technology for their daily activities and administration to drive the operations of critical infrastructures cannot be overemphasized. This is evident largely in industrial control systems (ICS) among which the supervisory control and data acquisition (SCADA) system is used to monitor and manage essential operations exposing it to cyber threats and attacks. Cyber threats and attacks on critical infrastructure result to denial of service, vandalism, theft or manipulation of data and even physical harm which can lead to catastrophic national security and economic downturn. These are attributed to the integration and increasing interconnectivity of enterprise information technology and operational technology with standard solution instead of proprietary protocol and software. This paper presents analysis of threat: environment, classification and their attributes and cyber-security frameworks to guard against threats and attacks on critical energy infrastructures using case study approach to demonstrate practical applications in real-world scenarios. The emphasis is on supervisory control and data acquisition (SCADA) system for remote controlling switches, pumps and surveillance systems. This is for government to shape the cyber-security outlook of the critical energy infrastructures to be more secured, resilient, adaptive and sustainable. This will help government make meaningful informed decisions on the cyber-security solutions most appropriate to meet their specific needs and challenges. Besides, it will promote collaboration and knowledge sharing amongst professionals and stakeholders in government, energy companies, regulators, and cyber-security experts for greater innovation and advancement.

Keywords: Cybersecurity Framework, Critical Infrastructure, Cyber Threat, Energy, Supervisory Control and Data Acquisition Systems (SCADA), Collaboration.

INTRODUCTION

Government the world over is striving to find innovative ways to curb the exponential and sophisticated growing cyber-attacks on critical infrastructures. This is because her day to day administration is heavily reliant on technology which is essential for the swift operation of critical infrastructure which is the focus now of government as they channel their operations to e-governance, which is expected to be the best practice for the future of all nations [1]. According to the draft Cyber Security Act of 2012, an industry can be defined as "critical" if damage or unauthorized access to that system could reasonably: i) result in the interruption of life-sustaining services, ii) cause catastrophic economic damages, or iii) cause severe degradation of national security. The transportation system,

banking and finance, energy, heath and emergency, defense, and government sectors and many others use conventional information technologies. Critical infrastructure and information technologies have strong relationships in many different ways and at many different levels. Today, major parts of critical sectors use cyber system for control and monitoring for example, the Supervisory Control and Data Acquisition (SCADA) systems. It is a computer system used to gather and analyze real-time data. These systems use standard hardware, software, operating system and protocol that are connected to corporate networks and even to the internet by wired and wireless means. They utilize standard solutions which make them vulnerable and exposed to cyber threats. Typically, the hardware, software, and communication interfaces of these devices are developed utilizing commercial off-the-shelf components [2]. The critical infrastructure community comprises of public and private owners and operators, and other entities whose role is securing the nation's infrastructure. The members' functions are supported by technology which includes information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices like the internet of things (IoT). These make critical infrastructure exposed to cyber threats and attack maliciously exploited by hackers to cause harm to them by changing their working operations either for sabotage, espionage, financial gain, or ideological motives. According to [2], the sector is a prime target for cyber-attacks due to its reliance on complex networks and digital technologies. Their security is of great concern to government and organization as any cyber-attack on them has far-reaching consequences like: disruption of services, economic sabotage, death, and so on. This paper is aimed at exposing the multifaceted threats and threat actors be-deviling the energy infrastructure, vulnerabilities brought about by the use of the (SCADA) system, examining real-world examples of noteworthy cyber-attacks and emphasizing the employment of cybersecurity frameworks and standards, and collaborative approaches like partnership as measures to fortify the resilience of the critical energy infrastructure.

Cyber Threats, Actors, and Classification

As a prefix, the term 'cyber' dates back to the 1940s, and was first used in the concept of 'cybernetics' relating to the communication and control interfaces between living things and machines [3]. Since this date the term has been used widely in the context of futuristic technology. The term has undergone a rapid evolution. To Internet users of the mid to late 1990s, the term 'cyber' was used to describe the practice of conducting intimate relationships online [4]. Yet in a relatively short time, the term has become closely associated with security and attacks against computing systems. The origins of this evolution lie in the 1960s use of the term 'cyberspace' to refer to environments outside of normal experience. Over time this notion of a separate domain came to be used to refer to the space created by the network of connected computing systems that comprises the internet [5].

NATO defines cyberspace as:

The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data [6]. Hence, the 'cyber domain' is a potentially contested space which is equivalent to the traditional militarily contested environments of the land, sea, and air [7]. Following this logic, in the same way that there is an army to fight on land, a navy to fight on the sea, an air force for air battles, a cyber capability is required to defend and project national interests within this new domain [8]. Cyber threats have evolved beyond simple viruses and now encompass a sophisticated array of attacks [9]. Malware, ransomware, phishing, and advanced persistent threats (APTs) are among the arsenal of tools employed by cyber adversaries. In the face of evolving threats, organizations and individuals alike must adopt proactive defense measures. Continuous monitoring, threat detection, and vulnerability management are essential components of a robust cybersecurity strategy. Rapid incident response and recovery plans ensure resilience in the event of a successful attack. While technological solutions are paramount, the human element remains a critical factor in cybersecurity. According to [9], cyber-attacks may be used to manipulate public opinion, influence elections, or destabilize political environments. This can involve spreading disinformation, conducting social engineering campaigns, or compromising political figures' communications. Some cyber-attacks involve extortion, where threat actors demand payment from individuals or organizations under the threat of exposing sensitive or embarrassing information. This can occur through threats of data leaks or distributed denial-of-service (DDoS) attacks. As technology continues to advance, so do the tactics of cybercriminals. Thus, threats can limit the ability of organizations to innovate, compete, and increase the reputation of customers [10], (NIST). The new realization of threats and attacks increases the interest in the following areas [11]:

a. Increasing dependence to the emergence of technology.
b. The establishment of organizations on collaboration and trust.
c. The business ecosystems include information and data ubiquity.
d. Multiple parties are involved in transactions and operations.

e. The new technological reality encompasses new and advanced threats.

The new attacks enforce current security community in full attention and interesting as never before since the incidents and risks associated with cyber-attacks are increasing [12].

Cyber Threat Actors

Threat actors can be an individual or group of individuals whose task is to cause an adverse reaction in the computer system. They can range from individuals working on their own who attack systems for no other motivation than to have fun or to demonstrate their technical prowess, to teams of salaried government employees who launch attacks to further the geopolitical aims of a nation state.

Profiling threat actors involves understanding the characteristics, motivations, and tactics employed by various groups engaging in cyber activities. Threat actors fall into the following categories:

a. *Script kiddie* – An unsophisticated individual with low expertise and low resources who conducts attacks for personal gratification, or to demonstrate prowess within a peer group.

b. *Hacktivist* – A collective of individuals united by shared interests or ideology who may have some degree of technical competence, and who may be able to muster significant resources, in order to conduct attacks to further their ideology. Hacktivist groups are driven by ideological, political, or social motivations. They aim to advance a particular cause, raise awareness, or protest against perceived injustice. Their attacks often have a public-facing element to draw attention to their agenda. Hacktivist groups typically possess moderate to advanced hacking skills, focusing on defacement, data breaches, or disruptions of online services. Entities perceived as adversaries to their cause, such as governments, corporations, or organizations that go against their ideological beliefs.

c. *Criminal* – A catch-all term used to refer to any group that is motivated by illicit financial gain. Some criminal gangs may be relatively unsophisticated with little expertise or resources, using tools developed by others to conduct attacks. Other criminal groups may be highly organised crime groups with access to significant technical expertise and large quantities of resources.

d. *State sponsored* – Some threat actor groups exhibit great expertise and clearly have access to many resources, yet do not appear to be financially motivated. The victims they target often appear to point towards the group conducting espionage, or seeking to support the geopolitical aims of a nation state.

e. *APT (advanced persistent threat)* – This term is often used synonymously with state sponsored to refer to threat actors that are supported by a nation state. However, it was first used to refer to threat actors that were highly sophisticated and well resourced, who carefully target their victims and are patient and persistent in launching attacks. As such, the term can be used to refer to both state-sponsored and the most sophisticated criminal groups who may have levels of expertise and resources at least equal to those of many state-sponsored threat actors.

f. *Insider* – An individual who may have legitimate access to a system, or deep knowledge of a system gained through legitimate access, who chooses to use these to the detriment of the legitimate system owner.

These are not the only possible taxonomies of threat actors. The criminologist, David Wall classified threat actors according to their behaviour types:

1. *Cyber-trespass* or *hacking* – Transgressing computer boundaries to intrude in spaces that are owned by others.

2. *Cyber-deceptions/thefts* – Acquisitive crime over the internet, including the abuse of financial instruments or details to obtain monetary gain, and the unauthorized obtention of digital property, such as music piracy.

3. *Cyber-pornography/obscenity* – The acquisition and distribution of illegal pornographic material, including images of child abuse.

4. *Cyber-violence* – Using networked systems to inflict psychological harm on others. This term includes activities such as publishing hate speech or cyberstalking where a perpetrator seeks to affect another through persistent tracking or sending unwanted communications.

Understanding the motivations and profiles of these threat actors is crucial for organizations and cybersecurity professionals. It enables the development of targeted defense strategies, threat intelligence sharing, and international cooperation to mitigate the impact of cyber threats. As the cyber landscape evolves, staying vigilant and adapting defenses are essential to counter the diverse range of threat actors. Some of the attributes of the threat attributes are found in Table 1.

Table 1: Threat actor attributes

Attribute	Description
Target	The nature of the targets of the threat actor. Some threat actors preferentially target individuals, other companies, or governments.
Expertise	The technical capability of the threat actor. Less sophisticated threat actors are only able to launch attacks using tools written by others, the most sophisticated develop their own malicious tools and may identify previously unknown vulnerabilities.
Resources	The budget and time available to the threat actor. Even threat actors with relatively little expertise may be able to assemble and coordinate large networks of computers under their control as part of a botnet.
Organisation	The nature of relationship between individuals within a group. Threat actors may be 'lone wolves' acting without coordinating with others, may be part of a tightly disciplined military-like structure, part of a flexible gang united by personal relationships and trust, or members of a collective united by shared interests.
Motivation	The reason the threat actor is conducting an attack. For the majority of attacks, the reason is illicit financial gain. However, some attacks may be due to personal reasons such as for self-gratification or due to holding a grudge, or due to furthering an ideology, or to support geopolitical aims.

Cyber Threat Classifications

Threat taxonomies help to facilitate in identifying threats that can affect an organization and in organizing those that are already in existence. Using the many threats listed in a threat taxonomy an organization can possibly know the threat it's likely to be faced with. Earlier standard ISO/IEC 7498-2:1989 classified threats simply as either accidental or intentional, and active or passive. Accidental threats are those that exist with no premeditated intent, whereas intentional threats have a purposeful motive. Passive threats do not modify any information within the system; active threats change the state of a computing device in some way (ISO 1989) (Figure 1). Jouini *et al.*'s threat classification model considered the source of the threat, the threat agent, motivation, and intention; showing that similar outcomes of a threat impacting such as the disclosure or destruction of information could have very different aetiology [13].

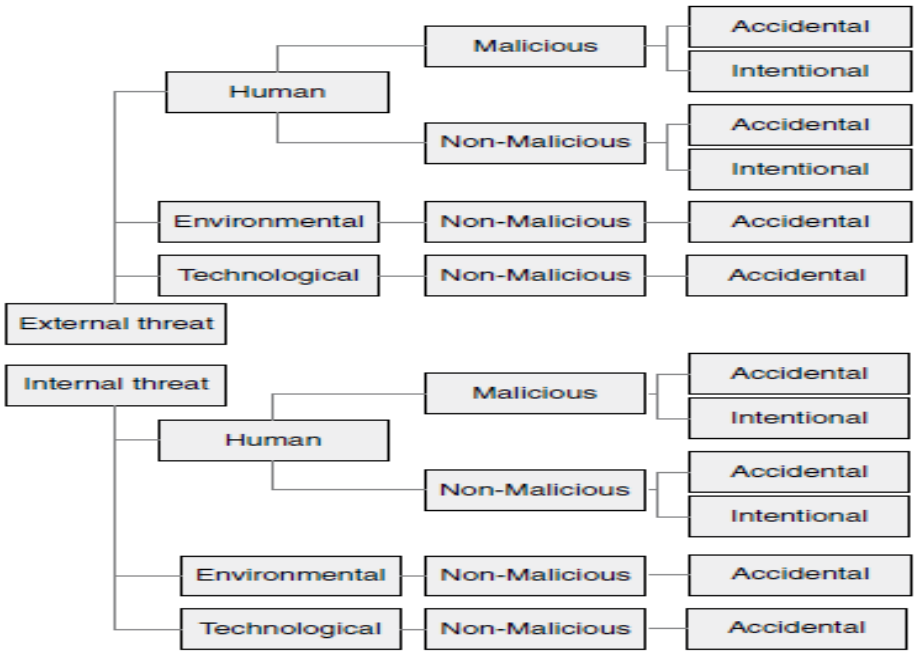

Figure 1: Taxonomy of threats [13].

The taxonomy of threats can be more detailed than the one above as seen in The European Network Information Security Agency (ENISA) which divides possible threats into eight high-level categories, then further subdivides into many more. The eight highest level categories consist of:

a. Physical attack (deliberate/intentional)
b. Unintentional damage/loss of information or IT assets
c. Disaster (natural, environmental)
d. Failures/Malfunction
e. Outages
f. Eavesdropping/Interception/Hijacking
g. Nefarious Activity/Abuse
h. Legal

Microsoft STRIDE taxonomy of threats approach only considers threats against systems that fall under one of six categories:

a. Spoofing – Impersonating something or someone else.
b. Tampering – Modifying data or code.
c. Repudiation – Claiming not to have performed an action.
d. Information disclosure – Exposing information to someone not authorised to see it.
e. Denial of Service – Deny or degrade service to users.
f. Elevation of Privilege – Gain capabilities without proper authorisation.

What is Critical Infrastructure?

All critical infrastructures are dependent on computer information infrastructures for management, control, and communications. The government defines a critical infrastructure as, …systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety… [14]. Critical infrastructure includes any element of a system that is required to maintain societal function, maintain health and physical security, and ensure social and economic welfare. Widely accepted examples of critical infrastructure are energy and utilities, financial systems, food, transportation, government, information and communications technology, health, and water purification and distribution. However, these elements do not operate in isolation today. Increasingly, connectivity and interdependencies between such systems increase the complexity of managing critical infrastructure and modelling the risks of cybersecurity threats [15]. Indeed, [4], state that "the computerization and automation of critical infrastructures have led to pervasive cyber interdependencies". And [11], discuss the difficulty in assessing the effects that failures in communications networks may have on municipal

infrastructures such as hospitals and emergency services. They further stated that cyber-interdependencies comprise a fundamental class of interdependency in critical infrastructure networks.

Threats to Critical Infrastructure

It is becoming increasingly clear that cyber-attacks continue to increase in frequency and sophistication and traditional cybersecurity methods are also increasingly insufficient to detect and respond to new types of attacks [15]. As the complexity and interdependencies of critical infrastructure increase, providers of critical infrastructure must cope with increasing vulnerability of their management systems to cyber-threats. As outlined in the *US National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* [16], three effects may constitute vulnerability on a system:

1. *Direct infrastructure effect*: Cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function.
2. *Indirect infrastructure effect:* Cascading disruption and financial consequences for government, society, and economy through public and private sector reactions to an attack.
3. *Exploitation of infrastructure:* Exploitation of elements of a particular infrastructure to disrupt or destroy another target.

The increasing complexity of such system vulnerabilities, and the complexity of the threats themselves, necessitates cooperation between the industry and the government. These existing and emerging trends lead to a requirement for the consistent implementation of cybersecurity by industry stakeholders, key infrastructure providers, and government in order to protect critical infrastructure vital to financial, commercial, and social wellbeing.

The evolution of cyber threats has been a dynamic and multifaceted phenomenon. The European Union Agency for Cybersecurity (ENISA Threat Landscape 2020 — ENISA, n.d.) highlights the need to comprehensively address the historical trajectory of cyber threats to understand their nuances and adapt cybersecurity strategies accordingly.

Notable Cyber Threats

The two landmark cases that help to redefine the cyber landscape and the invaluable insights they offer as seen in Table 2.

Table 2: Some notable cyber threats

Year	Attack	Impact	Example	References
2012	Stuxnet	Targeted Iran's nuclear program, manipulating centrifuges and causing physical damage.	i) ICS vulnerability: Exposed alarming weaknesses in industrial control system ii) Zero-Day Exploits: Highlighted the importance of vulnerability management and patching. iii) International Collaboration: Emphasized the need for global cooperation in combating sophisticated threats.	[17] [18]
2015	Ukraine Power Grid attack	Caused widespread power outages through remote manipulation of control system	i) Cyber-Physical Convergence: Demonstrated the convergence of cyber and physical threats. ii) Targeted Tactics: Showcased the need for tailored defenses against specific attack vectors. iii) Resilience and Recovery: Provided valuable lessons in building cyber resilience.	[19]; [20]

Evolving Cyber Threats

The evolution of cyber threats includes the rise of sophisticated Advanced Persistent Threats (APTs), often orchestrated by nation-state actors. Notable groups like APT28 and APT29 have been implicated in cyber espionage campaigns targeting critical infrastructure, emphasizing the geopolitical dimension of cyber threats [21]; [22]. Table 3 depicts some evolving cyber threats and their impacts.

Table 3: Some evolving cyber threats

Threat Trend	Description	Impact	Example Attacks	References
Ascendance of APTs	Well-organized groups, often backed by nation-states, engage in intricate cyber espionage and data theft.	Threat to national security, global stability, and critical infrastructure	APT28 (targeting critical infrastructure) APT29 (industrial espionage)	[21] [22]
Weaponization of Ransomware	Ransomware evolves from individual extortion to targeting critical services like healthcare and municipal systems.	Widespread disruption, financial loses, and potential physical harm	WannaCry (hospital disruptions), NotPetya (infrastructure shutdown)	[5] [23],
Shifting Tactics And Techniques	Adversaries constantly adapt, using zero-day exploits, supply chain attacks, and social engineering.	Increased difficulty and defense, evolving vulnerability	SolarWinds supply chain attack, ; Log4j vulnerability exploitation.	[24] [25]
Other emerging trends	Cryptocurrency theft, disinformation campaigns, and deepfakes pose new challenges.	Social and political disruptions, economic instability, erosion of trust.	Crypto exchange hacks, fake news campaigns, manipulated videos.	[26]; [27]; [28]

Energy Resources and Threat to Energy Infrastructure

Energy is regarded as a main critical infrastructure and energy security (ES) is important part of national security [29]; [30]. Energy security and energy infrastructure is important and an essential commodity in the world market that is reliant on a worldwide system of production and delivery. It is the fuel that drives the global economy and keeps our societies working. As the economies of the world grow and societies develop, so does the importance of infrastructures that produce and supply this energy. The U.S. National Counterterrorism Center counts 2750 terrorist incidents on energy infrastructure occurring between 2004 and 2011 [31]. According to [32], the sector is a prime target for cyber attacks due to its reliance on complex networks and digital technologies. Moreover, the interconnectivity of energy systems has a multiplier effect on the cybersecurity risk. A breach in one sector can cascade through interconnected systems, leading to widespread disruptions and economic losses. Power grids, for instance, are highly susceptible to cyber-attacks that have the potential to disrupt electricity generation and distribution, leading to widespread ramifications. Oil and gas facilities, on the other hand, heavily rely on intricate automation and control systems, making them vulnerable to cyber threats that could compromise their operational integrity. Components of power management systems and their main vulnerabilities and cyber threats are considered in. Electric power management systems include two levels: the physical component of control system, and supporting infrastructure, which includes software, hardware and communications networks. The main types of threats for these systems are:

1) The threat to corrupt the content;

2) The threat to introduce a time delay or denial in the communication with received measurements or control messages, de-synchronization, timing attacks. The main consequences from cyber-attacks implementation are loss of load or violations in system operating frequency and voltage, or other negative influence [33]. [7], noted that outdated software, insecure communication protocols, and insufficient security controls present significant risks to the integrity and reliability of energy systems. Many energy organizations rely on aging systems that were not designed with cybersecurity in mind, making them vulnerable to cyber threats. Moreover, the convergence of

operational technology (OT) and information technology (IT) networks introduces new attack surfaces. Additionally, the rapid adoption of new technologies, such as smart grids and IoT devices, introduces new vulnerabilities that adversaries can exploit. Furthermore, legacy infrastructure and outdated security practices pose significant challenges for the energy sector. Many energy organizations rely on aging systems that were not designed with cybersecurity in mind, making them vulnerable to cyber threats [34]. Additionally, the rapid adoption of new technologies, such as smart grids and IoT devices, introduces new vulnerabilities that adversaries can exploit [6]. This clearly tells us that threat to energy infrastructure is among the most serious security and economic challenges today and in the future. The limitation is not on few nations alone, but the spread of the attacks ranges from refineries or pipelines, power stations to attacks on oil companies executives. The complex and highly networked system for example, power grids, oil and gas pipelines, and renewable energy facilities, switches and pumps stations that are controlled by SCADA systems make use of either radio signals or internet connectivity to control the flow of energy resources. Also, the interdependent and interoperability of energy infrastructure and internet of things (IoT) to other infrastructures like transportation networks and facilities, information and communication infrastructure cutting across wide open areas or dense urban environments makes them vulnerable and prime targets for malicious cyber attacks.

Examples of threats to Critical Energy Infrastructures

Adversaries can leverage open-source public resources to perform GPS spoofing attacks against phasor measurement units (PMUs) [34]. By introducing small undetectable timing delays (in the micro second range) in the measurement signals (within the IEEE standard limits for synchrophasors C37.118 (Revision IEEE Standard C37.118, 2005), the phase differences between actual and measured angles can be significantly altered exceeding allowed limits, tripping circuit breakers (CBs), sectionalizing parts of the electric power systems EPS, and causing power outages (e.g., brownouts, blackouts) [35]. Moreover, in [36], researchers introduced a coordinated load redistribution attack affecting power dispatch mechanisms. By attacking generators or transmission lines while falsifying load demand and line power flows, system operators are misled into increasing load curtailment. Furthermore, in [37], the authors investigated two types of DoS attacks along with their impact on EPS. The first attack is assumed to be a stealthy false data injection attack false data injection attack (FDIA) performed to mask the attack impact from detection algorithms. The second, assumed as a non-stealthy attack, aims to maximize the damage on power system operation by targeting the most vulnerable transmission line, impeding power dispatch, and causing load shedding. Attacks targeting supervisory control and data acquisition SCADA-controlled switching devices or monitoring devices impeding situational awareness (in an integrated T&D system model) are evaluated in [38]. The authors in [19], investigated cyber-attacks on IoT-enabled grid deployments. They discuss how advancements in IoT technologies can drive the power grid modernization process, but at the same time increase the system's threat surface given its interconnected topology encompassing millions of IoT nodes. Researchers in [39], examine the security of modern power systems from the viewpoint of interconnection with micro-grids. In addition, [18], provides a complete overview of the cyber-threats encountered on the infrastructure, network protocols, and application levels of power systems. Furthermore, attacks targeting the data availability, integrity, and confidentiality of micro-grids are discussed in [40]. Stuxnet in 2010 targeted supervisory control and data acquisition (SCADA) systems. It utilized zero day vulnerabilities to infect air-gapped systems and set a precedent for state sponsored cyber attacks, specifically aimed at disrupting Iran's nuclear program. In 2017, the malware *Triton* was discovered in Saudi Arabia, attacking a petrochemical plant by disabling instrumented safety systems [41]. The cyber attack on Ukraine's power grid in 2015 where threat actors successfully compromised industrial control systems (ICS) and disrupted electricity distribution to thousands of customers [42]. The Ukraine power grid cyber attack highlighted the importance of securing critical infrastructure assets and systems against sophisticated cyber threats, particularly in the energy sector. The Colonial Pipeline ransom-ware attack: the attack shut down Colonial Pipeline's operations for approximately five days, causing localized shortages of gasoline, diesel fuel, and jet fuel. Panic-buying became rampant across the southeastern United States as consumers feared gas would run out.

Nigeria's Energy and the Electrical Grid System and Threat

Energy is amongst Nigeria's most critical infrastructure, as it is a fundamental part to every aspect of life in Nigeria. The entire economy is reliant on energy that is mainly produced by the electrical grid system and oil and gas system. There are quite a number of state regulations and organizational standards that provide standard recommendations to protect the power grid from cyber threats [43]. The energy infrastructure in Nigeria is fundamentally organized around two principal sectors, electricity and oil and natural gas. The production of electricity consists of three major components: generation, transmission, and distribution. The generation of electricity is through the use of hydroelectric dams, and fossil fuel plants while the transmission and distribution

systems are linked to the electrical grid system. The distribution systems manage, control, and distribute the produced electricity into businesses, government organizations, and homes. The energy system has become a natural target for terrorists due to the fact that it cannot be stored once it is produced. Recently, in Nigeria there had seen national grid collapse, thefts which vary from small petty theft to large grand theft, illegal tapping of power lines or oil pipelines, vandalism which can cause small loses that serve as vulnerabilities that can be as well exploited. In "Thenigeriavoice newspaper" of 11th July, 2024, the Defence Headquarters raised an alarm that terrorists are planning to destroy some critical infrastructures in many parts of the country. The Director, Defence Media Operations Edward Buba quoted as "we are aware of some of the plans to target some critical infrastructures in the country. Accordingly, we have emplaced measures to forestall such plans. He added that "security agencies responsible for securing critical infrastructures and facilities have also been placed on alert. Accordingly, some of such plans have been frustrated." The report stated that attacks on critical infrastructures and facilities, particularly on electricity infrastructures, especially in some parts of North-East, have been on geometric rise in the recent time, causing a black out in the affected areas. For instance, three electricity towers, T193, T194 and T195, were destroyed on December 28, 2023, by terrorists who used improvised explosive devices in Borno State. Similarly, in June 2024, two towers T193, and T194 along the 330 kilovolts single circuit transmission line were destroyed by vandals. The protection of the electrical grid system from cyber-attack must ensure the monitoring and awareness of new advances being made in cyber weapons. Also, the protection of the Supervisory Control and Data Acquisition (SCADA) systems using improved security such as firewalls, use of encryption, and more refined measures for detecting cyber intrusion. Intelligent agent-based networks designed to monitor and respond to cyber threats will also be necessary if we hope to better protect our systems. Also, an area where additional R&D is required centers on ways to detect a cyber-attack from internal sources such as disgruntled employees. Thus, our critical infrastructures must be protected not only from terrorists but also from the very people we entrust to regulate and protect our valuable resources. The nation's energy infrastructure is dependent also on the management of our oil and natural gas sector. In general, the nation's electrical grid system and the oil and natural gas systems are all critical to the total functioning of almost every aspect of our economy, and any disruption in these services will result in grievous consequences. This is coming up because the protection of these systems from terrorist attacks is largely the inter-dependent of these industries on cyber computer systems and to forestall such industries which are yet to experience sophisticated cyber-attacks, and have not fully integrated computer security and intrusion analysis programs to offset and protect themselves from this type of terrorist targeting.

Cybersecurity Frameworks for Improving Critical Infrastructure

A framework according to the Collins English Dictionary is the use of a complete set of rules, ideas or guidelines to describe a problem or determine what to do [44]. Cybersecurity framework therefore, is a general guideline that covers many components or domains that can be adopted by businesses/companies/institutions, which does not specify the steps that are required to be taken [45]. In fact, organizations can refer to cybersecurity frameworks to realize guidelines in the successful implementation of cybersecurity standards to be better equipped to identify, detect, and respond to cyberattacks [46]. The main goal of a cybersecurity framework is to reduce the risk of cyber threats through learning from the best practices [47]. A cybersecurity strategy cannot be implemented effectively without the right cybersecurity framework [48] and cybersecurity standards as guidelines or techniques for protecting the environment or cyber organizations, including best practices that can be used for business or industry. Cybersecurity frameworks are flexible and can provide users with the freedom to choose some parts or the whole model, methods, or technical practices, offering general and adoptable guidelines, as well as offering suggestions to be applied within the organization [49]. Implementation costs can be reduced as a result of the flexibility of cybersecurity frameworks. This can be effective to protect the infrastructure against cyber threats and secure critical sectors in the nation and economy. CSFs are very flexible and can reduce implementation costs, help protect and secure infrastructure, and other sectors (private or government) that are important to the economy and national security [50]; [51]. There are many different types of cybersecurity frameworks and standards that have been developed to address the unique challenges of the energy sector. The NIST Cybersecurity Framework [51], for instance, provides a comprehensive set of guidelines for managing cybersecurity risks. Similarly, the ISO/IEC 27001 standard offers a framework for establishing, implementing, maintaining, and continuously improving an information security management system [52]. Industry-specific standards, such as the NERC CIP standards (NERC, 2020), further enhance the resilience of critical energy infrastructure. The Cyber Kill Chain framework, introduced by Lockheed Martin, provides a structured approach to understanding and mitigating cyber threats [53]. This framework delineates various stages of a cyber-attack, including reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives, guiding cybersecurity professionals in identifying and disrupting attacks at each stage. The MITRE ATT&CK framework is a knowledge

base of adversary tactics and techniques based on real-world observations [54]. It provides a comprehensive framework for mapping and categorizing cyber threats, enabling organizations to identify gaps in their cybersecurity defenses and prioritize remediation efforts effectively. These cybersecurity frameworks and standards play a crucial role in guiding energy organizations for the enhancement of cybersecurity posture and mitigate risks to critical infrastructure and also provide comprehensive guidelines, best practices, and recommendations for the implementation of an effective cybersecurity measure that is tailored towards the unique challenges and requirements of the energy sector. Organizations or private sectors can adopt this framework into best practice for securing their own critical organization [54]. Businesses that seek to successfully implement cyber security standards are dependent on cybersecurity frameworks to harmonize policy, business, and technological approaches that are effective to mitigate cybersecurity issues and address cyber risks [55]. Therefore, cybersecurity frameworks (CSFs) have been developed by academic institutions, international organizations, countries, and corporations to ensure cyber resilience [56]. Thus, to ensure the protection of data and the infrastructure in organizations, businesses, and governments, cybersecurity standards and frameworks are required [57].

The following points are major examples of the implementation of common cyber security visions, goals, and strategies [57]. The framework should address:

a. The increasing cooperation and focusing inside the security community to motivate active participation of all players and at all levels.
b. The leverage and expansion of current best practices of cyber security measures in the research and education fields.
c. The emerging of proper related government agencies into this domain.
d. The creation of a general framework for identification of the next generation of cyber security controls.
e. The establishment of coordinative and collaborative strategies, plans, and policies in terms of cybersecurity trends.

National Institute of Standards and Technology (NIST) Framework

President Obama, in February 2013, commissioned NIST to establish a "Cybersecurity Framework." The framework is voluntary. Organizations or private sectors can adopt this framework into best practice for securing their own critical organization or [55]. It is one of the popular and widely accepted and adopted cybersecurity frameworks in the energy industry. The NIST CSF provides a flexible and risk-based approach to cybersecurity, comprising five core functions: Identify, Protect, Detect, Respond, and Recover [51]. It is comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure. The leveraging on [58], by energy organization will help them to make an assessment of their current cybersecurity posture, make adjustment and improvement to areas that are lacking and develop a tailored cybersecurity strategies that is in alignment with industry standards and best practices. The core framework has several functions: identify, protect, detect, respond, and recover [58] as depicted in Figure 2.

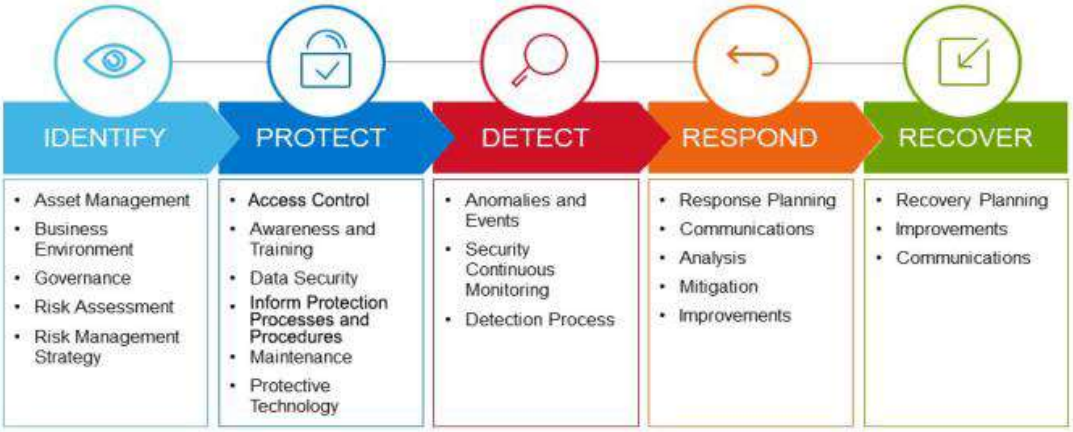

Figure 2: NIST Cybersecurity Framework version 1.0 [58]

Table 4 : Functions of the cyber security function [58].

Function	Description
Identify	Develop and identify the requirements, processes, and people necessary to provide cyber security; the assets that require protecting; the existing cyber security capabilities; and the threats that may impact the organisation.
Protect	Develop and implement the necessary protections in order to protect assets against threats, and to be able to contain the impact of potential cyber security events.
Detect	Develop and implement the necessary processes, systems, and people in order to detect cyber security events.
Respond	Develop and implement the capability to respond appropriately to cyber security events and incidents.
Recover	Develop and implement the ability to be able to restore business functionality that may be impaired by a cyber security incident.

Currently, the newly developed NIST Cybersecurity Framework (CSF) 2.0 is to also help organizations manage and reduce their cybersecurity risks as they start or improve their cybersecurity program. This guide is a supplement to the NIST CSF and is not intended to replace it [58].
The NIST CSF 2.0 is organized by six Functions—**Govern, Identify, Protect, Detect, Respond,** and **Recover.** Together, these Functions provide a comprehensive view for managing cybersecurity risk. The new function introduced in version 2.0 is **GOVERN** here, the organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Figure 3: Cybersecurity Framework (CSF) 2.0 [58]

The framework provides risk management principles and best practices to small and large businesses alike, regardless of focus, sector, or nation [58]; [59];[60] to increase the vital infrastructure's dependability and security. The NIST Framework not only has the potential to shape a standard of care for domestic critical infrastructure organizations but also could help to harmonize global cybersecurity best practices for the private sector [13].

ISO/IEC/27001:2014 Framework

A framework called ISO/IEC 27,001 [61], addresses ISMS requirements for organizations of all sizes, types, and industries (including retailing, defense, banking, education, healthcare, and government), as well as for businesses of all dimensions (from tiny corporations to giant corporations) (including businesses, governments, and non-profit organizations). It is another prominent cybersecurity framework relevant to the energy sector which is the series of standards developed by the International Organization for Standardization [51] and the International Electro-technical Commission (IEC). ISO/IEC 27001 provides a systematic approach to managing information security risks, encompassing policies, procedures, controls, and other measures to protect sensitive information [61].

Energy organizations can use ISO/IEC 27001 certification to demonstrate compliance with international cybersecurity standards and enhance trust and confidence among stakeholders and customers. The ISO27001 (Information Technology-Security Techniques-Management System Requirement) is an industry best practice standard that has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). An ISMS is a group of policies, practices, instructions, and related activities and resources that a corporation provides to keep its systems safe, in accordance with ISO/IEC 27,000:2018 (ISO/IEC, 2018). The ISO 27K family of specifications, as well as other IT specifications, consider the plan-do-check-act (PDCA) paradigm as a continuous improvement process paradigm, as illustrated in Figure 5 [62].

Figure 4: Sequence of PDCA in ISO 27,000 [63]

Sector-Specific Guidelines and Standards

In addition to these frameworks, energy organizations may also refer to sector-specific cybersecurity guidelines and standards developed by regulatory agencies and industry associations. For example, the North American Electric Reliability Corporation (NERC) and Critical Infrastructure Protection (CIP) standards outline cybersecurity requirements for the electric power industry in North America, focusing on the protection of critical assets and systems (NERC, 2021). Similarly, the European Union Agency for Cybersecurity (ENISA) provides guidance and recommendations for enhancing cybersecurity resilience in the energy sector through initiatives such as the Energy Infrastructure Protection (EIP) guidelines.

Distributed Cybersecurity Framework

[64]; [65]; [66]; [67], examine the current situation of distributed cyber-security systems. Using dynamic models, the survey [65] evaluates the literature on distributed filtering and control techniques in industrial CPS environments.[67],explores recent work into cyberattack countermeasures within distributed systems. The adoption and implementation of these cybersecurity frameworks and standards, by energy organizations can help in the establishment of a robust cybersecurity foundation to mitigate risks concerning critical infrastructure, and to safeguard the reliability, availability, and security of energy systems. In furtherance to this, adhering to recognized cybersecurity frameworks and standards facilitates regulatory compliance, cultivates and promotes a culture of collaboration and information sharing among stakeholders, which leads to continuous improvement in cybersecurity practices across the energy sector.

Collaboration between Public and Private Sectors

This fortification cannot be accomplished in isolation. Public-Private Partnerships bridge the gap between government agencies like the Department of Homeland Security (DHS) and private sector entities. Through information sharing, joint exercises, and coordinated response efforts, these partnerships create a unified front against cyber threats, enhancing the overall cybersecurity posture of critical infrastructure. Cross-Sector initiatives, like the Cross-Sector Cybersecurity Working Group, further bolster this collaborative spirit, fostering shared strategies and insights across different sectors. Cyber threats transcend national borders, necessitating international collaboration to address the global nature of cyber-attacks [68]. Nations, organizations, and

cybersecurity entities collaborate on information sharing, joint threat investigations, and the development of international cybersecurity norms and agreements facilitates a unified response to cyber threats, pooling resources and expertise strengthens collective defense against nation-state-sponsored attacks and transnational cybercrime.
Proactive defense measures involve anticipating and preventing cyber threats before they can manifest [55]. Organizations implement continuous monitoring, vulnerability assessments, and regular security audits. Anticipating future trends is crucial in preparing for emerging cyber threats. The U.S. Senate Committee on Homeland Security and Government Affairs (Office, 2023) emphasizes the significance of regulatory frameworks, industry best practices, and collaborative endeavors between public and private sectors. This approach can enable planners to reflect on the many factors for consideration like – designation & grouping of infrastructures by sectors, historical analysis of the most likely intelligence threats, available resources, prioritization of infrastructures, ownership (public-and private sector) of infrastructures, criticality criteria, stakeholders associated with infrastructures, existing vulnerabilities of infrastructures, consequences associated with damage or destruction of infrastructures, available resources and overall risk management. The intent is to apply the available resources to the most-likely threat. Due diligence should be taken in appropriating funds for the protection of critical infrastructures from federal, state, and private sectors since such funds are grossly inadequate and unavailable. The protection efforts today should be multidimensional rather than the traditional one with armed guards and barriers securing either a building or system. Considerations and prioritization should be given to both human, physical and cyber considerations. The process should be dynamic and not a passive one. Collaborative initiatives also extend to public-private partnerships, where governments, industry stakeholders, and cybersecurity experts collaborate to address shared challenges. These partnerships foster information sharing, joint research, and the development of cybersecurity practices that are adaptive to the evolving threat landscape. By combining the expertise and resources of both the public and private sectors on a global scale, these partnerships contribute to a more comprehensive and effective defense against emerging cyber threats.

Examples of Collaboration seen in some Countries

The prioritization of cyber-security by some nations of the world has even gone to the extent of by which government is providing guidelines for private and public sectors. Netherlands has a public private partnership (PPP) taskforce to improve the quality and breath of ICT education in all academic level, from primary to professional education. This taskforce is a public private partnership between the industry and the government. The success of the taskforce is to ensure that the skills of the children are honed as early as secondary, in order to ensure the continuity of talent to top degree programs [69]. In Finland, there is a centre of excellence to spur a robust national cybersecurity cluster. The centre of excellence and the cluster play roles to increase the cybersecurity knowledge and know-how in the nation through education and R&D. Finland also believes in collaboration between government, businesses and non-governmental organisations (NGOs) to develop comprehensive cybersecurity programs to impact the society. In Norway, the authorities provide skills advisory by surveying level of competency of the general public and businesses. Public authorities lead public initiatives to cultivate and sustain the culture of cybersecurity in the nation. Saudi Arabia established the National Cybersecurity Authority (NCA) in 2017 to centralize cybersecurity controls. Concurrently, the National Cyber Security Center (NCSC) was established to serve as the arm for the technical and operational component of the NCA. The NCSC monitors supervisory control and data acquisition systems among government entities, specifically in the sectors of energy and industry [70]. The Government of Gambia in conjunction with the World Bank West Africa Regional Communication and infrastructure Program developed the Gambian National Cybersecurity strategy. The strategy aims at making the Gambian cyberspace as an essential pre-requite for allowing the economic and social development of Gambia and its people to fully benefit from the digital transformation (GNCSS, 2016). The strategy is focused on five priority goals of building capacity, the establishment of institutional frameworks, resilience and protection. The Nigerian government through the office of National Security Adviser developed and launched her national cybersecurity strategy in 2014 with the vision of becoming safe, secured, a vibrant and resilient and trusted community that provide an opportunity for the citizenry, safeguard national assets and interest, promote peaceful interactions and proactive engagement in cyberspace for national prosperity. The vision is to be achieved through ten specific objectives among which are the establishment of an institutional framework, national capabilities, awareness, local, regional and international cooperation etc. While the strategy assumes cyberspace as a platform for global competitiveness and socioeconomic development, it however lacked in-depth policy guidance on innovative technology and cultural peculiarities that may impede practice. The US Department of Commerce, led by NIST, builds partnerships between academia, the private sector, and governments, by promoting secure networks and cybersecurity education ecosystems, in the form of training, and the Cybersecurity Framework - National Initiative for Cybersecurity Education (NICE) [5]. The Electricity Subsector Coordinating Council

(ESCC), collaboration between industry leaders and government representatives, exemplifies successful security implementation in the energy sector. Through joint initiatives, the ESCC has implemented robust cybersecurity measures, conducted grid resilience exercises, and shared threat intelligence, bolstering the security of the electric grid (ESCC - Home, n.d.). The international collaboration has become an effective mitigation strategy against cyber threat for an adaptive, robust, responsive and resilient cybersecurity ecosystem. This is imperative to foster global cooperation through exchange of threat intelligence; best practices and collaborative effort against challenges pose by cybersecurity. This is achieved by establishing or setting standardization, guidelines and frameworks on a global scale to address cyber threats using bodies like International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). One prominent example of international collaboration is the Budapest Convention on cybercrime. This is a treaty that is adopted by some countries to facilitate international cooperation in the investigation and prosecution of cybercrime. It establishes common definitions, procedures, and legal frameworks, fostering a harmonized approach to addressing cyber threats across borders. Such conventions exemplify the growing recognition that effective cybersecurity requires a coordinated response that transcends national boundaries [72]. Therefore, safeguarding the integrity, confidentiality, and availability of the critical energy infrastructure has become paramount to ensure uninterrupted energy services and preservation of trust among users and stakeholders. Involving governments, businesses, and individuals to collaborate is now a shared responsibility and a necessity for the security of cyber information systems and to keep abreast of cyber threats evolvement.

CONCLUSION

Employing a layered defense strategy instead of a single line of defense gives a practical collaborative approach which is a preventive, detective, and responsive measure. Also, it leverages on automating the processes and the use of artificial intelligence (AI) technologies to enhance threat detection and response capabilities. Automation can streamline routine tasks, allowing cybersecurity teams to focus on more complex and strategic aspects of risk mitigation [72]. AI, with its ability to analyze vast amounts of data and identify patterns, contributes to a more proactive and adaptive defense against emerging threats. The adoption of standardized cybersecurity frameworks, such as the NIST Cybersecurity Framework [51] or [61] provides a structured approach to managing and mitigating cyber risks. Satisfactory cybersecurity protection can be achieved by adopting a cybersecurity framework that describes the scope, implementation, and evaluation processes, and also provides a general structure and methodology for protecting critical digital assets [73]. In fact, organizations can refer to cybersecurity frameworks to realize guidelines in the successful implementation of cybersecurity standards to be better equipped to identify, detect, and respond to cyberattacks [42]. Collaborative initiatives also extend to public-private partnerships, where governments, industry stakeholders, and cybersecurity experts collaborate to address shared challenges. These partnerships foster information sharing, joint research, and the development of cybersecurity practices that are adaptive to the evolving threat landscape. By combining the expertise and resources of both the public and private sectors on a global scale, these partnerships contribute to a more comprehensive and effective defense against emerging cyber threats. Furthermore, it fosters collaboration between cybersecurity experts, data scientists, network engineers, and other stakeholders to align AI-driven cybersecurity initiatives with business objectives and operational needs [74]. Implement mechanisms for ongoing monitoring and evaluation of AI-driven cybersecurity solutions to assess their performance, identify areas for improvement, and adapt to evolving threats.

REFERENCES

1. Asiabaka, *C.C. (2014) Imperatives of egovernment and the future of Nigeria.Owerri: FUTO. Accessed July 4, 2014 from www.softwareclubnigeria.org/.../FUTO%20VC%20E- Gov%20Imperatives%20)*
2. McLaughlin, S. et al. (2016) 'The cybersecurity landscape in industrial control systems,' *Proc. IEEE*, vol. 104, no. 5, pp. 1039_1057.
3. Coe, T. (2015) 'Where does the word cyber come from?', *OUP Blog* (28 March). https://blog.oup.com/2015/03/cyber-word-origins.
4. Newitz, A. (2013) 'The bizarre evolution of the word 'Cyber'. *Gizmodo*. https://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487 (accessed 13 January 2023).
5. Strate, L. (1999). 'The varieties of cyberspace: problems in definition and delimitation,' *Western Journal of Communication* 63 (3): 382–412. https://doi.org/10.1080/10570319909374648.
6. NATO Terminology Office (2017b) *Cyberspace*. NATOTerm, The Official NATO Terminology Database. https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en (accessed 13 January 2023).
7. Crowther, G.A. (2017) 'The cyber domain', *The Cyber Defense Review* 2 (3): 63–78.
Lee, M (2023) *Cyber Threat Intelligence*, First Edition.© John Wiley & Sons, Inc.

8. Ferdinando, L. (2018) *Cybercom to Elevate to Combatant Command.* US Department of Defense Press Release. https://www.defense.gov/Explore/News/Article/Article/1511959/cybercom-to-elevate-to-combatant-command (accessed 13 January 2023).
9. Emmott, R. (2018). NATO cyber command to be fully operational in 2023. *Reuters* (26 October). https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9 (accessed 13 January 2023).
10. NIST, (2014) 'Framework for Improving Critical Infrastructure Cybersecurity,' In Cybersecurity Framework; *National Institute of Standards and Technology:* Gaithersburg, MD, USA; p. 41.
11. Kaplan, J.M. *et al.*, (2015) *Beyond Cybersecurity: Protecting Your Digital Business* John Wiley & Sons.
12. Choo, K.K.R. (2011). *The cyber threat landscape: Challenges and future research directions.* Computers & Security, 30(8), pp.719-731.
13. Jouini, M., Rabai, L.B.A. and Aissa, A.B. (2014) *Classification of security threats in information systems* Procedia Computer Science, 32, pp.489-496.
14. DHS (2012) *Enhanced cybersecurity services.* Available from DHS: http://www.dhs.gov/enhanced-cybersecurity-services. Accessed 20 Sep 2013
15. Rahman, H. A., Marti, J. R., and Srivastava, K. D. (2011) 'A Hybrid Systems Model to Simulate Cyber Interdependencies between CriticalInfrastructures,' *International Journal of Critical Infrastructures*, 7(4): 265–288. http://dx.doi.org/10.1504/IJCIS.2011.045056
16. Office, U. G. A. (2023). *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods.* https://www.gao.gov/products/gao-23-105468
17. Langner, R. (2011) 'Stuxnet: Dissecting a cyberwarfare weapon', *IEEE Security and Privacy*, *9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67
18. Mohee, A. (2022) *A Realistic Analysis of the Stuxnet Cyber-attack.* https://doi.org/10.33774/apsa-2022-qs797
19. Ren, J. *et al.* (2019) 'Smart Grid and Electric Power Informatization,' *Journal of Physics: Conference Series*, *1187*(2). https://doi.org/10.1088/1742-6596/1187/2/022017
20. Whitehead, D. E. *et al.* (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *70th Annual Conference for Protective Relay Engineers, CPRE 2017.* https://doi.org/10.1109/CPRE.2017.8090056
21. Cherqi, O. *et al.* (2021) 'Leveraging Open Threat Exchange (OTX) to Understand Spatiooral Trends of Cyber Threats: Covid-19 Case Study,' *Proceedings - 2021 IEEE International Conference on Intelligence and Security Informatics, ISI 2021.* https://doi.org/10.1109/ISI53945.2021.9624677
22. Mwiki, H. *et al.* (2019). Analysis and triage of advanced hacking groups targeting western countries critical national infrastructure: APT28, RED October, and Regin. *Advanced Sciences and Technologies for Security Applications*, 221–244. https://doi.org/10.1007/978-3-030-00024-0_12
23. Ghafur, S. *et al.*(2019) 'A retrospective impact analysis of the WannaCry cyberattack on the NHS', *Npj Digital Medicine 2019 2:1*, *2*(1), 1–7. https://doi.org/10.1038/s41746-019-0161-6
24. Juvonen, A. *et al.*, (2022) 'On Apache Log4j2 Exploitation in Aeronautical, Maritime, and Aerospace Communication', *IEEE Access*, *10*, 86542–86557. https://doi.org/10.1109/ACCESS.2022.3198947
25. Zetter, K. (2023) *The Untold Story of the Boldest Supply-Chain Hack Ever.* WIRED. https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/
26. Balaban, D. (2023) *Inside The World Of Crypto Exchange Hacks.* Forbes. https://www.forbes.com/sites/davidbalaban/2023/05/20/inside-the-world-of-crypto-exchange-hacks/?sh=b8a453f2915f
27. Clemons, E. (2018) *Why Fake News Campaigns Are So Effective - Knowledge@Wharton.* https://knowledge.wharton.upenn.edu/article/build-fake-news-campaign/
28. Feingold, S. (2022) 'Four key ways disinformation is spread online | World Economic Forum', *World Economic Forum.* https://www.weforum.org/agenda/2022/08/four-ways-disinformation-campaigns-are-propagated-online/
29. Kondratev, A. (2012) 'The current trends in research of Critical Infrastructure in foreign countries', *Foreign Military Review*, no. 1, 19 - 30.
30. Massel, L. V. *et al.* (2016) 'Cyber Danger as one of the strategic threats to Russia's Energy Security', *Cybersecurity issues*, no. **4**(17) 2□10.
31. National Counterterrorism Center, (2013) *Counterterrorism 2013 calendar,* at http://www.nctc.gov/site/index.html (accessed 09 OctOber 2013)
32. Lee, L.H. *et al.* (2012) *Context-Aware Web Security Threat Prevention.* https://doi.org/10.1145/2382196.2382302

33. Gaskova, D.A and Massel, A.G (2018) 'Methods to Analyze Critical Facilities in Energy with Regard to Cyber Threats Vth International workshop Critical Infrastructures: Contingency Management, Intelligent, Agent-based, Cloud Computing and Cyber Security' (IWCI 2018) *Advances in Intelligent Systems Research, volume 158*
34. Keliris, A. *et al.* (2018) 'Lowbudget energy sector cyberattacks via open source exploitation," in *Proc. IFIP/IEEE Int. Conf. Very Large Scale Integr. (VLSI-SoC)*, pp. 101_106.
35. Konstantinou, C. (2017) 'GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment,' *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 4, pp. 180_187.
36. Xiang, Y. Wang, L. and Liu, N. (2017) 'Coordinated attacks on electric power systems in a cyber-physical environment," *Electr. Power Syst. Res.*, vol. 149, pp. 156_168.
37. Tian, J. *et al.* (2020) 'Coordinated cyberphysical attacks considering DoS attacks in power systems," *Int. J. Robust Nonlinear Control*, vol. 30, no. 11, pp. 4345_4358
38. Zografopoulos, I. *et al.* (2021) 'Security assessment and impact analysis of cyberattacks in integrated T&D power systems,' *arXiv:2102.03215*. [Online]. Available: http://arxiv.org/abs/2102.03215
39. Canaan, B.; Colicchio, B. and Abdeslam, D. Ould (2020) 'Microgrid cybersecurity: Review and challenges toward resilience," *Appl. Sci.*, vol. 10, no. 16, p. 5649.
40. Nejabatkhah, F. *et al.* (2020) 'Cyber-security of smart microgrids: A survey,' *Energies*, vol. 14, no. 1, p. 27.
41. Vegesna, V.V. (2024) 'Cybersecurity of Critical Infrastructure' *International Machine learning* journa*l and Computer Engineering* Vol.7 No.7 2024
42. ENISA, (2019) 'European Union Agency for Network and Information Security', *Threat Landscape Report 2018*. 15 Top Cyberthreats and Trends.
43. Leszczyna, R. (2018) 'Standards on cyber security assessment of smart grid,' *Int. J. Crit. Infrastruct. Prot.* 22, 70–89.
44. Dictionary, C. E. (2020) 'Collins Dictionary online,' *Collins*.
45. Oxford University Press (2014) *Oxford Online Dictionary*. Oxford: Oxford University Press, [Online]. Available: http://www.oxforddictionaries.com/definition/english/Cybersecurity
46. Ozkan, B.Y.; van Lingen, S. and Spruit, M. (2021) 'The Cybersecurity Focus Area Maturity (CYSFAM) Model. *J. Cybersecur.* 1, 119–139.
47. Baron, J. *et al.*, (2019) 'Making the Rules. The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights'; Publications *Office of the European Union*: Luxembourg.
48. Dedeke, A. and Masterson, K. (2019) 'Contrasting cybersecurity implementation frameworks (CIF) from three countries,' *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 373–392.
49. Donaldson, S. *et al.* (2015) *Enterprise Cybersecurity: How to Build a Successful Cyber defense Program against Advanced Threats* Apress: Berkeley, CA, USA.
50. NIST, (2018) 'NIST Releases Version 1.1 of its Popular Cybersecurity Framework,' *NIST*, [Online]. Available:https://www.nist.gov/newsevents/news/2018/04/nist-releases-version-11-its-popularcybersecurity-framework.
51. NIST Cybersecurity Frameworks 2.0 https://www.nist.gov/cyberframework
52. ISO/IEC, (2015) "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services," *ISO/IEC 27017*.
53. Straub, J. (2020) 'Modeling attack, defense and threat trees and the cyber kill chain, att&ck and stride frameworks as blackboard architecture networks,' *In 2020 IEEE International Conference on Smart Cloud* (SmartCloud) (pp. 148-153). IEEE.
54. Al-Sada, B., Sadighian, A., and Oligeri, G. (2023) 'Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database', *IEEE Access*.
55. Shackelford, S.; Russell, S. and Haut, J. (2015) *Bottoms up: A comparison of voluntary cybersecurity frameworks*. UC Davis Bus. Law J. 16, 217.
56. Azmi, R.; Tibben, W. and Win, K. (2018) *Review of cybersecurity frameworks: Context and shared concepts*. J. Cyber Policy, 3, 258–283.
57. Sommestad, T. (2012) "A framework and theory for cyber security assessments" (*Doctoral dissertation, KTH, Royal Institute of Technology* Stockholm, Sweden)
58. NIST Cybersecurity Frameworks 2.0 https://www.nist.gov/cyberframework
59. Kissel, R. (2019) 'Glossary of Key Information Security Terms,' *NISTIR 7298*.

60. Krumay, B.; Bernroider, and Walser, R. (2018) 'Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework,' *Secure IT Systems*, vol. 11252, pp. 369–384
61. ISO/IEC, (2018) "Information technology — Security techniques — Information security management systems — Overview and vocabulary," *ISO/IEC 27000*.
62. Disterer, G. (2013) 'ISO/IEC 27000, 27001 and 27002 for Information Security Management,' *Journal of Information Security*, vol. 4, no. 2, pp. 92-100.
63. Xue, K. *et al.* (2018) 'Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Trans. Inf. Forensics Secur,' *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2062 - 2074.
64. Mohamed, A., Kashif, K., Qi, S. and William, H. (2017) "Intrusion prediction systems," *in Intrusion prediction systems, New York, Springer*, pp. 155 - 174.
65. Ding, *et al.* (2019) 'A Survey on Model-based Distributed Control and Filtering for Industrial Cyber-Physical Systems,' *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, vol. 15, no. 5, pp. 2483–2499.
66. Lin, H. *et al.* (2018) "A Survey on Network Security-Related Data Collection Technologies," *IEEE*, vol. 6, pp. 18345 - 18365.
67. Nespoli, P. *et al.* (2018) "Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 20, no. 2, pp. 1361-1396.
68. Love bugged! (2000) *Network Security*, *6*. https://doi.org/10.1016/S1353-4858(00)06015-3
69. ESCC - Home. (n.d.). *Retrieved January 22, 2024*, from https://www.electricitysubsector.org/
70. Al-Janabi, S. and Al-Shourbaji, I. (2016) 'A Study of Cyber Security Awareness in Educational Environment in the Middle East', *J. Inf. Knowl. Manag.* 15, 1650007.
71. MGBACHI, T.V. (2024) 'Navigating Cybersecurity Beyond Compliance: Understanding Your Threat Landscape and Vulnerabilities. *Boston University, Metropolitan College, Boston* IRE Journals | Volume 7 Issue 7 | ISSN: 2456-8880
72. Couretas, J. M. (2022) 'Cyber Analysis and Targeting', *An Introduction to Cyber Analysis and Targeting*, 1–12. https://doi.org/10.1007/978-3-030-88559-5_1
73. Antunes, M. *et al.* (2021) 'Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal', *J. Cybersecur.* 1, 219–238.
74. Shah, V. (2021) 'Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats,' *Revista Espanola de Documentacion Cientifica*, *15*(4), 42-66.

CITE AS: Wesley O. Odumu, Barnabas I. Gwaivangmin and Ademola P. Adewoye (2025). Safeguarding National Critical Energy Infrastructure using Cybersecurity Frameworks and Collaborative Approach for a Resilient Energy Future. NEWPORT INTERNATIONAL JOURNAL OF SCIENTIFIC AND EXPERIMENTAL SCIENCES, 6(1):31-47. https://doi.org/10.59298/NIJSES/2025/61.3147