ISSN: 2756 – 4118 *African Journal of Science Policy and Innovation Management* Volume 1, Issue 2. December, 2020
ajspim.oauife.edu.ng

CYBER SECURITY ASSESSMENT OF NIGERIA'S ELECTRIC POWER INFRASTRUCTURE

Ibikunle O. Ogundari[1*], Funso A. Otuyemi[2], Abiodun S. Momodu[3] and Babatunde O. Salu[4]

[1] *African Institute for Science Policy and Innovation, OAU, Ile-Ife*
[2] *School of Computing and Engineering, University of Huddersfield, UK*
[3] *Centre for Energy Research and Development, OAU, Ile-Ife*
[4] *African Regional Centre for Space Science and Technology Education - English*
*Corresponding author email: ibikhunle_ogundari@oauife.edu.ng

ABSTRACT

The evolution of the Nigerian electric power system from a traditional centralized grid to an integrated cyber-physical system inevitably makes cyber-attacks inevitable. It is imperative to analyse these cyber-security concerns of Nigeria's electric power system as an input to critical energy infrastructure policy development. The study relied on primary and secondary sources of information including policy documents such as the Energy Sector Reform Act (2005), the Nigerian National Cybersecurity Policy draft document (2015), the World Bank project appraisal document on Nigeria's electricity transmission project, as well as journal articles on Nigeria's electric power system, and cyber-threats to critical energy infrastructure in the world. In addition, a technology foresight analysis framework comprising content analysis and strategic foresight was also used. The study ascertained that the national power infrastructure were old and obsolete technologies known as legacy equipment, and the new cyber-physical system included digital metering devices, and automated power flow control systems amongst others. The national power infrastructure indicated higher susceptibility to cyber-attacks upon and by the electric power system compared to cyber-attacks through the electric power system, and was susceptible to cyber-attacks by classification and methods such as phishing, malware and data breaches amongst others. These cyber-threats were considered possible across the generation, transmission and distribution systems. A robust, effectual, and formal cyber-security system revolving around three critical resources – People, Processes, and Technology/Systems, were postulated for the national electric power system, entailing the development of an Incident Response Plan comprising documented instructions detailing four critical components or strategies, namely, preparation; detection and analysis; containment, eradication and recovery; and post–incident activity.

1.0. INTRODUCTION

The electric power supply system in Nigeria is a critical infrastructure which is necessary for the proper functioning of the State. The electric power system is significant as its availability or adequacy is critical to the effective and efficient performance of the Nation's economy, and indispensable to socio-economic development (Ogundari and Otuyemi, 2019). Globally, critical infrastructure planners are aware of the need to maintain and protect valuable national critical infrastructure in order to promote and sustain national development (Ogundari and Otuyemi, 2019). With the increasing dependence of critical infrastructure such as a nation's electric power structure on computer information systems and networks, critical infrastructure

planners, globally, have noted their susceptibility to cyber vulnerabilities and threats, and have made the safety and protection of the electric power structure to be a national security priority.

Cyber vulnerabilities and threats refer to the forms or measures state and/or non-state actors may target computer information systems, infrastructure or computer networks by malicious means. These vulnerabilities and threats may allow access to valuable information, disrupt essential services, and/or damage equipment (Ngoma, 2012; Alese *et al.*, 2014; Lin and Tom, 2016). Cyber threats became pronounced as public threats in Nigeria in the late 1990's consequent to an increase in awareness and availability of computing and information systems, the domestic licensing of Global System for Mobile Communication (GSM), providers, advancement in internet service provision, increase in internet service providers, improvement in technology for internet access, and increase in capabilities to purchase and acquire these services and technologies (Alese *et al.*, 2014; KPMG, 2016).

In the recent past, electric power systems around the world have been reported to be faced with an increased number of cyber operating systems threats (Yin *et al.*, 2015), with the vulnerability of the power system going beyond mere physical system security to being a matter of cyber security. This highlights the vulnerability of electric power systems and electric markets as a whole to cyber-attacks which may result in loss of revenue and ineffective/inefficient power networks.

Reforms in the Nigerian electric power sector in recent years have brought in new players, funding and technology whose focus includes the modernisation and modification of the national power infrastructure. The integration of new Information Technology (IT) and Operational Technology (OT) into the national power infrastructure inevitably makes increased vulnerabilities to cyber-attacks inevitable. It is imperative to address these issues by identifying these potential problems and taking preventive or corrective measures to improve or reduce this risk.

1.1 Statement of the Problem

Nigeria's electric power system, which is a critical infrastructure, is supposedly expected to operate efficiently and effectively in a secure environment and protected from threats physical or cybernetic in nature. The reality however, is that the Nigerian electric power system is plagued by inefficiency and ineffectiveness, and the physical and cybernetic vulnerabilities of its operational environment are numerous and more often than not, complex and not clearly defined. The recent reforms in Nigeria's electric power system have created opportunities for increased privately-owned management and funding leading to the modification and modernization of the sector, and the injection of new power and networking technologies including electronic-compatible energy management and control systems into the three key sectors of power generation, transmission and distribution. Inopportunely, the government policies that drive these reforms such as the Electric Sector Reform Act (2005), and other energy policy documents (such as the Renewable Energy Master Plan drafts and the National Energy policy (2003), were developed before cyber security concerns became a prominent national policy issue. Thus, these policies reflect a dearth of strategies to address the concerns.

Arguably, one of Nigeria's first official responses to cyber-security concerns is the National Cyber Security Policy and Strategy document which was only prepared in 2014 and launched

in 2015 (Galadima, 2016). This document focused on the national security and defence sector, and although the national cyber-security policy document does have a section (7.5) that identified critical infrastructure sectors including energy and power, there is no specific section that shows an in-depth assessment on cyber threats in that sector, nor specific strategies to mitigate these concerns. Although the Nigerian government had become aware of the issue of cyber-security concerns on the National electric power system (Osho and Onoja, 2015), specific government policy initiatives toward these concerns are inadequate due to their very limited understanding of the issues. Since the launch of the national cyber security policy document, there has been increased integration of modern cyber-physical systems into the three key sectors of power generation, transmission and distribution for increased operational effectiveness and efficiency. However, policy guidelines that underscore clear understanding of the phenomenon, and appropriate strategies to mitigate the cyber threats to these cyber-physical systems are still not readily available. Enhancing the chances of cyber-attacks on Nigeria's electric power system may cause considerable, irredeemable damage to the sector, and nullify the hard-earned gains of the reforms in the national electric power system. Other challenges may include huge loss of strategic investments and revenues, job losses in the sector and allied sectors, increased felonious disruptions of electric power supply, and the total collapse of the system.

It is undisputable that there is limited understanding on the cyber threats to the national electric power system, and unless greater understanding is obtained, policy formulation and implementation for and in the sector may eventually become inadequate, inappropriate or ineffective. This may have long-lasting adverse effects on Nigeria's electric power system. Many main-stream energy policy scholars and analysts are hampered by the complex technical nature of cyber-physical systems analysis and this probably adds to the limited policy briefs on cyber-security analysis of the electric power systems. Against this backdrop, it becomes imperative for the energy sector in general and the electric power sub-sector specifically to review cyber-security threat possibilities and mitigation strategies to curtail these cyber-threats. The strategic objective of this paper is to provide an energy technology foresight analysis critical to strengthening cyber-security strategy development in Nigeria's electric power sector. This strategic objective can be achieved by examining Nigeria's electric power infrastructure, examining the potential cyber threats that may affect the electric power infrastructure, and assessing mitigation strategies to minimize these cyber threats.

2.0 Methodology

The study relied on both primary and secondary sources of information. The primary source of information includes the Energy Sector Reform Act (2005), the Nigerian National Cybersecurity Policy draft document (2015), the National cyber-security strategy document of 2014, and the World Bank project appraisal document on Nigeria's electricity transmission project 2018. Secondary sources of information included journal articles and internet portable document format (pdf) files. The internet search entailed an exploration of literature on Nigeria's electric power system, Information Technology and Operations Technology in Nigeria's electric power infrastructure, cyber threats/cybersecurity concerns to electric power infrastructure in the world, and information technology threats to critical infrastructure in the world. A technology foresight analysis framework comprising content analysis and strategic foresight was used for the study.

3.0 Historical background and Structure of the electric power system in Nigeria

Awosope (2014) noted that electricity production commenced in Nigeria in 1896 with the installation of a power plant in Marina, Lagos. The Electricity Corporation of Nigeria (ECN) was established in 1951, while in 1962, the Niger Dams Authority (NDA) was established for the development of hydroelectric power. In 1972, these two institutions were merged to create the National Electric Power Authority (NEPA) on 1stApril 1972. NEPA had the integrated responsibilities for the generation, transmission and distribution of electricity in Nigeria. In 2005, NEPA metamorphosed into Power Holding Company of Nigeria (PHCN) through the Electric Power Sector Reform (EPSR) Act, 2005 (Folorunso and Olowu, 2014). Pursuant of the EPSR Act 2005, further restructuring took place, with the PHCN broken into three major components – generation, transmission, and distribution. The generation and distribution components were privatized, while the transmission component was placed under the control of the Federal Government, albeit under private sector management. Since 2006, Nigeria's electric power system has consisted of six generation companies, eleven distribution firms and a transmission company (Onochie *et. al.* 2015). Nigeria's power system is made up of three distinct sectors, namely, generation, transmission and distribution (Momodu, 2012; Onochie *et al.*, 2015).

Generation

Electricity generation in Nigeria is from two major plant types – thermal and hydro plantsAs shown in Table 1, thermal power plants dominate the Nigerian electric power generation terrain, with an estimated 84% of installed generating capacity. The hydro power type accounts for only 16% of installed power generating capacity (Momodu, 2012; Folorunso and Olowu, 2014).

Transmission

The Transmission Company of Nigeria (TCN) was created as a successor company of PHCN after the unbundling of the sector. The company is publicly owned and privatelymanaged. The national electricity transmission capacity is made up of about 5523.8 km of 330KV line and 6801.49 km of 132 KV line (NESO, 2017). The principal obligation of the System Operator is to operate the transmission system and the connected installed generation in a safe and reliable manner without any system failure (KPMG, 2016). Figure 2 shows the existing transmission line system in the country is limited across large swathes of the North East and the Middle Belt of the country.

Distribution

Distribution companies (or Discos) are responsible for marketing and sales of electricity to customers. The eleven Power Distribution Companies (Discos) and their covered states are shown in the Table 2.

Nigeria's electric power infrastructure is characterised by old power plants and inadequate power generation, severely limited network coverage, overloaded and defective transformers and feeder pillars, inferior and deficient distribution lines, and a billing system that is ineffectual.

ISSN: 2756 – 4118 *African Journal of Science Policy and Innovation Management* Volume 1, Issue 2. December, 2020
ajspim.oauife.edu.ng

Table 1: Names and nominal installed capacities of Generation Companies in Nigeria

S/N	Generation Company	Year Commissioned	Plant Type	Nominal Capacity (MW)
1	Afam Power Plc (I-V)	1962	Thermal	987.2
2	Egbin Power Plc	1985	Thermal	1320
3	Kainji/Jebba Hydro Electric Plc	1968	Hydro	1330
4	Sapele Power Plc	1978	Thermal	1020
5	Shiroro Hydro Electric Plc	1989-1990	Hydro	600
6	Ughelli Power Plc	1966	Thermal	924
7	Calabar Thermal Power Station	2014	Thermal	561
8	Ijora Thermal Power Station	1956	Thermal	60
9	Geregu Power Station	2007	Thermal	148
10	Delta Power Station	1966	Thermal	116
11	Shell Afam Generation Company	2008	Thermal	450
12	Omotosho Generation Company	2007	Thermal	500
13	Jebba Generation Company	1985	Thermal	570
14	Ibom Power Station	2009	Thermal	190
15	Nigeria Electricity Supply Company (NESCO)	1923-1950	Hydro	30
16	Oji river Generation Company	1956	Thermal	10
17	AES Generation Company	2001	Thermal	270
18	Omoku Generation Company	2006	Thermal	250
19	Olorunsogo Generation Company	2007	Thermal	335
20	Benin Generation Company Limited	2012	Thermal	450
21	Okpai Power Station	2005	Thermal	480
22	Ihovbor Power Station	2012-2013	Thermal	450
23	Alaoji Power Station	2012-2015	Thermal	1074
24	Aba Power Station	2012	Thermal	140
	Total			12,265.2

Source: (Momodu, 2012; Folorunso and Olowu, 2014)

Table 2: Electricity Distribution Companies and States Covered in Nigeria

	Electricity Distribution Company	States Covered
1	Abuja Electricity Distribution Company	FCT, Niger, Nassarawa, Kogi
2	Benin Electricity Distribution Company	Edo, Delta, Ekiti, Ondo
3	Enugu Electricity Distribution Company	Imo, Anambra, Ebonyi, Abia, Enugu
4	Eko Electricity Distribution Company	Lagos State (Victoria Island, Lekki, Lagos Island, Apapa, Epe, Ikoyi, etc.)
5	Ibadan Electricity Distribution Company	Oyo, Ogun, Osun, Kwara
6	Ikeja Electricity Distribution Company	Lagos State (Ikeja, Surulere, Ikorodu, etc.)
7	Jos Electricity Distribution Company	Plateau, Bauchi, Benue, Gombe
8	Kaduna Electricity Distribution Company	Kaduna, Sokoto, Kebbi and Zamfara
9	Kano Electricity Distribution Company	Kano, Jigawa and Katsina
10	Port Harcourt Electricity Distribution Company	Rivers, Bayelsa, Cross Rivers, Akwa Ibom
11	Yola Electricity Distribution Company	Adamawa, Borno, Taraba and Yobe

The relationship between staff and customers is at best contentious, and logistic facilities, including telecommunication equipment, are insufficient in quantity and questionable in effectiveness (Oshevire *et al*., 2013; Vincent and Yusuf, 2014; Amuta *et. al.*, 2018; Olagoke *et al.*, 2018; Ogundari and Otuyemi, 2019).

Nigeria's electric power system is a traditional, conventional grid system with its consequent limitations in operations. The grid is a centralized system with one-way communication and where power flows in one direction – from the generation systems through the transmission and distribution infrastructure to the consumer. Typically, power generation is done in a location an extensive distance from where the end-users live, requiring significant transmission capabilities (Vincent and Yusuf, 2014; Amuta *et. al.*, 2018). The power system, under its various organisational manifestations (ECN, NEPA, PHCN), exhibits a rigid hierarchical structure, which is unable to self-monitor, and depends on manual restoration during disturbances. The electric power system has limited Supervisory Control and Data Acquisition System (SCADA) sensors, and other computing and information communication technologies necessary to monitor the performance of the power system, and/or ensure reliable power delivery (Amuta *et. al.*, 2018; Olagoke *et al.* 2018).

Furthermore, the system has inadequate interaction with its customers, generally limiting customer information to bill of servicers consumed on a month-to-month basis (Oseni, 2011). Metering is mainly electromechanical where available, as most customers do not have meters in their residences and are thus subject to estimated billing, derogatorily called 'crazy billing' Onohaebi, 2014). The Nigerian electricity customers have no choice on distribution systems as they are subject to monopolies (they are restricted to the distribution company in their area of location). The unreliable power grid is prone to failures and cascading outages, with operations and maintenance dependent on manual equipment checks (Vincent and Yusuf, 2014; Olagoke *et al.* 2018). The national electric power system exhibits low efficiency, with significant transmission and distribution losses (about ten percent of power generated is lost in the transmission/distribution lines) (Amuta *et. al.*, 2018).

Vincent and Yusuf (2014), Amuta *et al.* (2018) and Olagoke *et al.* (2018) further clarified that the technologies used in the ECN/NEPA/PHCN era before the current wave of reforms, modernization and modification were legacy equipment including Radio-phones (for exchange of system information between engineers and technicians on the network), manual circuit relays which switch high voltage circuits on and off; limited SCADA systems for monitoring system parameters like voltage, frequency etc; electromechanical metering devices (used on the distribution part of the network for determining customer consumption for billing purposes), and electrostatic meter for measuring high voltage. Others are blind monitoring systems which can detect faults on the network, distribution panels, transformers, feeder pillars, and other analogue metering equipment.

Post reforms, some of the equipment have been upgraded, and a hybrid configuration consisting of legacy equipment and digital automatic systems has been in place (Emodi *et al.,* 2014; Amuta *et. al.*, 2018; Olagoke *et al.*, 2018). This hybrid system is to evolve into a fully automated system as the sector modernises. The typical electric power system is complex, consisting of two key parts – the electric power infrastructure and the information infrastructure (Yin *et. al.*, 2015; Draffin, 2016). The electric power infrastructure (or primary power system) consists of power generation, transmission and distribution, while the information

infrastructure (or secondary power system) consists of power monitoring, telecommunication, data networking and the control operation of the power grid (Goetz *et. al.*, 2002). These two parts are operated by sensitive monitoring and control systems which should maintain the quality and the dynamic stability of the grid as well as guarantee systems delivery.

The new equipment being incorporated into the national electric powers structure includes a cyber-physical system consisting of electronic field devices, communication networks, substation systems and control centres that are embedded throughout the physical grid for efficient and reliable generation, transmission, and distribution of power. The new equipment includes digital metering devices, automated power flow control systems, automated pro-active protection devices, two-way electronic communication devices, and self-monitoring systems which are capable of automatic fault correction responses amongst others (Vincent and Yusuf, 2014; Amuta *et. al.*, 2018; Olagoke *et al.*, 2018). They are codified as the Energy Management System (EMS) (system of computer-aided tools used to monitor, control, and optimize generation or transmission system performance), the Supervisory Control and Data Acquisition (SCADA) systems (control systems comprising computer/information systems, networked data communications and graphical user interfaces (GUIs) for advanced process supervisory management), Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC) (Institute for Security Technology Studies, 2002; Watt, 2003; Negrete-Pincetic *et. al.*, 2009; Seissa *et. al.*, 2017).

The inculcation of automated, cybernetic information and communication systems to the national power infrastructure either by hybridization with or total replacement of the hitherto legacy equipment, inevitably increases the susceptibility of the national power infrastructure to various security violations from cyberspace (Koledoye *et al.*, 2013; Alese *et al.*, 2014; KPMG, 2016). Cyber-attacks can be focused on any of these distinctive systems or a combination of them, either from local points or from remote locations. For example, in a SCADA network, an attacker could try to disrupt the communications between the EMS and the Remote Terminal Unit (RTU) thereby sending spurious packets in the network and breaking communication between the two components (Ten *et. al.*, 2008). An understanding of the potential threats that these new technologies may expose the national power infrastructure to and possible alleviation initiatives is critical to mitigation strategy development.

Figure 4 depicts the final evolution of the Nigerian electric power supply grid infrastructure with its embedded cyber-physical infrastructure. The cyber system consists of electronic field devices, communication networks, substation systems and control centres that are embedded throughout the physical grid for efficient and reliable generation, transmission, and distribution of power.

4.0 Electric Power Systems and Cyber-Attack Types and Classifications

Cyber-attacks on electric power systems may be described by types or classifications. Three types of cyber-attacks electric power systems are susceptible to are those upon the power system, those by the power system, and those through the power system (Amin, 2002). Two classifications of cyber-attacks are those by location (local, remote and pseudo-remote) and those by attack mechanism (denial service attack, replay attack, middle attack and reprograming the device) (Alves-Foss and Heckendorn, 2002; Malladi *et al.*, 2002; Gu and Liu, 2007; Negrete-Pincetic *et. al.* 2009; Yin *et. al.*, 2015).

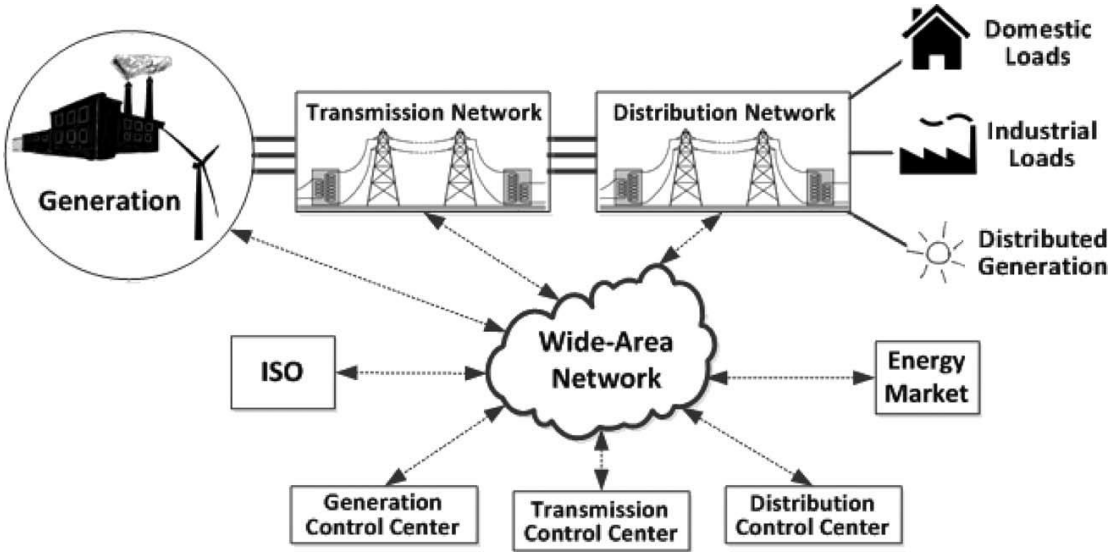

Figure 4: Electric power supply grid cyber-physical infrastructure
Source: (Sridhar *et. al.*, 2012).

4.1 Cyber-attacks by Type

i. **Cyber-attacks upon the electric power system:** the objective here is to hit the central electric power system(s) and render them incapacitated. This would have strategic implications for any nation's electricity market especially if it is a unified transmission grid (Knake, 2017).
ii. **Cyber-attacks by the electric power system:** the nation's electric power infrastructure would be compromised and weaponised against the country's populace. An example would be compromise power plant cooling towers and use them to disperse chemical or biological agents.
iii. **Cyber-attacks through the electric power system:** electric power system infrastructure could be compromised, and using the regional or national online networks, electromagnetic pulses through the grid may be used to impair regional or national computer or telecommunications infrastructure (Watts, 2003; Awosope, 2014).

The consequences of these types of cyber-attacks are far-reaching and may include deterioration in the reliability of the electric power system and its services, destruction of sensitive electrical industrial appliances, loss of revenue, national security considerations, and national embarrassment.

Nigeria's power infrastructure would appear to be most susceptible to cyber-attacks upon and by the electric power system. It is important to note that Nigeria's electric power system is a traditional, conventional, centralized grid system which although initially made up of legacy equipment, has had equipment up-grade to hybrid configuration consisting of legacy equipment and digital, automatic systems. Thus, it may be argued that a cyber-attack upon the electric power system, especially the centralized transmission system, would have significant impact on electricity supply, most likely leading to blackouts or brown-outs across the country. Cyber-attacks by the power system, whereby the nation's electric power infrastructure would be compromised and weaponised against the country's populace are also feasible. Knocking out the national power infrastructure for an extended period of time could be crippling for the economy, as the necessary electric power needs of various sectors of the economy would be

cut off, possibly leading to reduced commercial and industrial output, and increased consumption of more expensive, environmentally-polluting alternative power. Cyber-attacks through the electric power system may be considered the least likely to occur as the national electric power infrastructure lacks the necessary technology capabilities to achieve such levels of attack.

4.2 Cyber-attacks by Classification

i. **By location of attack:** Cyber-attacks premised on location may be considered local, remote or pseudo-remote (Yin, Xiao and Lv, 2015). Local attacks, as the name suggests, are in close proximity to the mark and take place in the Local Area Network (LAN). Remote attacks are launched outside the proximity area of the mark, and can invade computer/Information and Communication technology (ICT) networks in critical nerve centres, and impair critical equipment via system vulnerabilities and security limitations (Baigent *et al.*, 2011). Pseudo-remote attacks comprise internal saboteurs and external attacks causing what is called external invasion phenomenon. In an IT network, remote attacks have the highest occurrence probabilities while pseudo-attacks have the least due to their need of internal saboteurs (Zhang, 2011).

ii. **By attack mechanism:** cyber-attacks premised on attack mechanism may be classified as denial-of-service attack (DOS), replay attack, middle attack and reprograming the device. Denial of service (DOS) attack occurs when attackers take up excessive communication resources such that there is severely limited access for information availability to end-users (Gu and Liu, 2007; Negrete-Pincetic *et. al.*, 2009). Replay attacks entail breeching system security protocols using multiple false message intercept replays thereby fooling the end-user into thinking they have successfully completed the protocol run (Malladi *et. al.*, 2002). Attackers can also identify and intercept breaker tripping control instruction by network monitoring and replaying this instruction when necessary, resulting in breaker malfunction (Yin *et. al.*, 2015). In middle attacks, the attackers inject themselves surreptitiously between two communicating nodes, deceiving both nodes on their true identity and compromising information reception or dispatch between two communicating nodes (Negrete-Pincetic *et. al.*, 2009). An attacker can be a middleman between Remote Terminal Unit (RTU) and control centres, intercepting emergency fault information sent by RTU and replacing such with normal or alarm information, so that the system does not act in case of failure (Yin *et. al.*, 2015).

4.3 Cyber-attacks by Methods

Various methods for cyber-attacks on electric power systems are explained below:

i. **Data breach**: this type of attack is one of the most common types of cyber-attacks and entails stealing of sensitive information via a data breach. Files and information may be copied in a passive attack form without the attacker making his presence known.

ii. **Semantic attack**: incorrect information is used to damage the credibility of target resources or to cause direct or indirect harm. Examples include defamation (slander and libel), propaganda and stock manipulation schemes. These types of attacks are difficult to detect and catch.

iii. **Malware**: Short for "malicious software", it is the shared name for a several malicious software or computer programs (computer viruses, worms, Trojan horses,

adware, scareware, rogue software, ransomware and spyware) which are intentionally designed to infiltrate and extensively damage computers and data, without the users consent, or gain unauthorised access to a network.

iv. **Distributed Denial of Service**: this is an attack type where multiple compromised computer systems attack a target (e.g., a server, website or network service) and prevent this target from providing legitimate services to end users by flooding the target with superfluous messages which force it to slow down or shut down.

v. **Phishing**: this is the cyber-attack method where hackers attempt to obtain sensitive personal information from individuals (e.g., usernames, passwords or credit card numbers), by sending electronic communication purported to be from reputable companies.

Nigeria's power infrastructure, with its equipment upgrade to hybrid configuration consisting of legacy equipment and digital, automatic information and communication systems, would be susceptible to cyber-attacks by classification and cyber-attacks by methods. The cyber-physical systems present in the extant hybrid power infrastructure and the potential future cyber-physical system-based power infrastructure consist of equipment capable of routine cyber-attacks. National power supply disruptions due to typical and inexplicable information and communication/control systems failures at the various control centres have been reported (Alese *et al.*, 2014; KPMG, 2016; Vincent and Yusuf, 2014; Amuta *et. al.*, 2018; Olagoke *et al.*, 2018). The possibilities that these systems failures have been caused by cyber-attacks have not been ruled out.

4.4 Global Instances of Cyber-attacks on Electric Power Infrastructure

Cyber-attacks on critical infrastructure, especially on electric power systems, have globally been reported to be high in frequency and complexity (Yin *et. al.*, 2015; Desarnaud, 2017). This is in contrast to the perceived notions that such cyber-attacks would be low due to the absence of complex internet connections in electric power systems on the one hand, and the limitations on expert knowledge and skills for control systems architecture and executive operations on the other (Yin *et. al.*, 2015). Perceived low statistics on cyber-attacks on electric power critical infrastructure may be attributable to under-reportage due to fear of responsibility, fear of corporate image damage or the possibility of corporate competition. Furthermore, information on cyber-attacks on electric power systems may be suppressed as they may have substantial impact on national socio-economic activities (Yin *et. al.*, 2015; Desarnaud, 2017).

Several countries, such as, the United States, Japan, Georgia, Iran, Ukraine, Germany, Israel and Australia as well as the European Union have reported increases in the frequency and complexity of cyber-attacks on their electric power systems. Internal threats usually include human error, disgruntled employees or unscrupulous contractors, while external threats coming from nation-states and organized crime are also becoming more pronounced. Some incidents of cyber-attacks on electric power systems world-wide are presented in Table 2.

4.5 The Vulnerabilities of Nigeria's Restructured Electric Power System to Cyber-attacks

The inclusion of advanced cyber-physical systems in the national electric power system may increase operational effectiveness and efficiency. However, a significant drawback is that it opens up the electric power system to interferences from cyberspace. The potential impacts to Nigeria's power grid due to the damage, disintegration, alteration or exploitation of the advanced cyber-physical systems include:

Table 2. Incidents of Cyber-attacks on Electric Power Systems around the World

S/N	Country	Publication	Case Summary	Cause
1	USA	2001	SCADA system 2-week shutdown for repair	Insufficient access protection of VPN connection system for contracted vendors
2	USA	2003	SCADA system 2-week shutdown for repair	Intrusion and infection of slammer worm through VPN connection used by a contractor vendor
3	EU	2003	3-day loss of management functions of several power distribution/transformation stations	Malware infection of distributed SCADA system
4	Japan	2005	Leak of atomic power plant's confidential information via file sharing software	Malware infection of an employee's home PC storing confidential info.
5	Japan	2006	Leak of thermal power plant's confidential information via file sharing software	Malware infection of an employee's home PC storing confidential information
6	USA	2006	Loss of control of re-circulated water pump at Browns Ferry Nuclear power plant	Malfunction of Siemens Perfect Harmony VFD controller due to excessive traffic on power plant's integrated ICS network
7	USA	2007	Simulated cyber-attacks at Aurora power plant control system replica, changing the generator's operation trajectory and causing the generator to self-destruct	Invasion of SCADA system
8	USA	2007	Vulnerability test of power grid computer systems. Damage of browser, intrusion into power plant control network, and monitoring of power production and distribution.	Invasion of SCADA system and download of file record via cyber-attack
9	Brazil	2005 & 2007	Blackout across the nation	Hacker's cyber-attack against the power control system
10	Georgia	2008	Shutdown of Hatchpower plant for 48 hours	Computer patch in corporate network
11	USA	2009	Shutting down of power grid services	Usage of software tools by foreign cyber spies and hackers
12	USA	2010	Gas leak from pipeline due to computer malfunction	Computer malfunction (cause unknown)
13	Iran	2010	Destruction of centrifuges at Natanz uranium enrichment facility by malware Stuxnet	Malware infection
14	USA	2012	Malware infection of computers in control system environments of two power plants, causing 3-week restart delay for one and operation limiting for the other.	Malware infections of work USB drives

Sources: Negrete-Pincetic *et. al.*, 2009; Yin *et. al.*, 2015; Desarnaud, 2017)

Table 2 Contd. Incidents of Cyber-attacks on Electric Power Systems around the World

S/N	Country	Publication	Case Summary	Cause
15	USA	2014	Information leak due to attacks targeting as US/Canadian aero-defence firms/air carriers and energy businesses including EU ones	Malware (Havex) infection of SCADA systems due to attacks by Dragonfly hacker group
16	USA	2015	Large-scale DoS attack of FirstEnergy Corp. (no damage)	Unknown
17	Ukraine	2015	A few hours of power outage in western Ukraine (Ivano-Frankivsk Oblast)	Cyber-attack using malware Black Energy 3
18	Israel	2016	2-day shutdown of part of computer system for dealing with cyber-attack.	Malware infection by phishing attack
19	Germany	2016	Publication of confusion produced by a cyber-attack in around 2013 or 2014	Unknown
20	Ukraine	2016	Approximately 1-hour power outage of 1/5th pf power supply destinations in Kiev.	Cyber-attack using malware Industroyer/Crash Override
21	Ukraine	2017	Infection of malware NotPetya or radiation monitoring system at Chernobyl nuclear power plant forcing manual control	Malware infection (ransomeware)

Sources: Negrete-Pincetic *et. al.*, 2009; Yin *et. al.*, 2015; Desarnaud, 2017)

i. The Generation System: Electricity generation depends on local control of output and wide-area control (Automatic Generation Control, AGC). A cyber-attack on the local control system may be achieved by remote access or through the introduction of malware. Wide-area control depends on SCADA systems; hence, an attack on AGC could impact seriously on generation power stability or the physical destruction of physical equipment amongst other attacks (INL, 2016, Sin *et al.*, 2018; Dagoumus, 2019).

ii. The Transmission System: the major components here are substation transformers which step-up or step-down voltage over long distances for efficient delivery, transmission towers to connect power lines, and control centres to manage power delivery to distributed system loads. These components are most at risk to cyber-attacks, especially as their damage would require significant time and cost for replacement. Cyber-attacks may be launched through malware or other malicious software introduced to computers and devices, by local or remote access (Desarnaud, 2017; Mrabet *et. al.*, 2018).

iii. The Distribution System: this system is made up of distinct operators with independent areas of operation; hence networks and interconnectivity of systems across operators do not exist. Cyber-attacks here may affect the individual operators independent of each other, or may have backward implications to the transmission and generation systems. Cyber-attacks may be through malicious software to gain access to IT and OT infrastructure or hijack the SCADA system. Other cyber-attack methods may include phishing or DDoS. Cyberattacks could also affect market operations such as the billing systems for issuing invoices to consumers. These

systems use desktop computers, cloud services, or blockchain technology, which are vulnerable to cyberattacks, and could considerably affect cash flows and market viability (Jarmakiewicz *et al.*, 2015; Sin *et al.*, 2018; Dagoumus, 2019).

In order to launch cyber-attacks on Nigeria's electric power system, threat actors may likely seek to exploit networks, communication systems, devices, remotely accessible equipment and mobile devices, as well as third party services and supply chains. Attacks may then be launched through the cyber-attack types, classification and methods discussed earlier.

4.6 Cyber-security Strategies for Nigeria's Electric Power System Infrastructure

Cyber-security entails the protection of systems, networks, programs, devices and data from cyber-attacks by the usage of technologies, processes and controls (ONSA, 2014; Daffin, 2016). Thus, the main aim of cyber-security is the reduction of the risk of cyber-attacks. The scope of cyber-security activities is vast, ranging from simple personal-level changes to organization-wide business strategy. A robust, effectual cyber-security system is expected to be active and operative in an environment where cyber-attacks occur. Furthermore, such a system should have the capabilities to reduce an attacker's access to the computing and information systems of any critical infrastructure, provide appropriate and adequate diagnosis and treatment of cyber threats when required, and provide in-depth cyber-defence capabilities over multiple layers of protection (ONSA, 2014; Daffin, 2016). This robust, effectual cyber-security system revolves around three critical resources – People, Processes, and Technology/Systems (Watt (2003); ONSA (2014); Seissa *et. al.* (2017).

a. **People:** Although emphasis of cyber-attacks on electric power systems are principally centred on technical and procedural security loopholes, human factors such as ignorance, negligence, inordinate desire for personal gain, or lack of motivation can adversely affect national electric power grid security and integrity. The Nigerian electric power sector is replete with reports on the low entry qualifications, poor training, poor remuneration and rampant casualisation of employees (Oshevire *et al*., 2013; Vincent and Yusuf, 2014; Amuta *et. al.*, 2018; Olagoke *et al.*, 2018; Ogundari and Otuyemi, 2019). The sector needs to strengthen the welfare and motivation of its workforce as a strategic input into its cyber-security arsenal. Personnel should also have appropriate knowledge on the available security measures, adhere to accessible safety efforts, and update their cyber security skills and qualifications regularly.

b. **Processes:** The effective deployment of a cyber-security strategy in the electric power industry requires an appropriate and adequate process of implementation. This implementation process should be robust and detailed on how different activities and actions would be executed at minimum risks. As a public entity, the Nigerian electric power industry had a reputation for chaotic business operations (Ejumudo and Ejumudo, 2014; Ikekpeazu, 2018). Consequently, the establishment of appropriate, adequate and effective security controls and processes that can mitigate identified cyber-attacks can go a long way to making electric power infrastructure a hard target.

c. **Technology/Systems:** Technology is critical to an effective cyber-security program that identifies cyber-risks and develops appropriate control measures that prevent or mitigate the impact of those risks (Seissa *et. al.*, 2017). Although unbundling the Nigerian power sector has led to technology developments and the acquisition of

modern computing (Ajumogobia and Okeke, 2015), computing/IT logistics support has been inadequate (Oshevire *et al*., 2013; Vincent and Yusuf, 2014; Amuta *et. al*., 2018) and the local development of appropriate security protocols has been limited. The implementation of security protocols ideally should restrict access of cyber-threats into industrial control systems and computers (James, 2013).

The Nigerian electric power system lacks a robust formal cyber-security system to enhance national strategic readiness for its protection (ONSA, 2014). As the system evolves from the legacy equipment through the hybrid stage to a total automated system, it is imperative that a sustainable, proactive cyber-security system is institutionalised. The development of such a system would include an organized approach to cyber-attack prevention known as Incident Response Planning (IRP) (Collier, 2017). An incident not detected and controlled at the time of incursion usually worsens to a more harmful occurrence such as data infringement or system failure Thus, a robust incident response plan should quickly limit damage, restore services and minimize losses. This robust incident response plan should comprise printed documented instructions for the organization detailing four critical components or strategies, namely, preparation; detection and analysis; containment, eradication and recovery; and post–incident activity (ONSA, 2014; Draffin, 2016; Collier, 2017).

i. Preparation: This stage or strategy incorporates prevention and early warning systems. It prepares stakeholders to critically examine the operational environment of the energy infrastructure computer and network systems, and to understand the procedures for handling computer security incidents at the electric power infrastructure. Furthermore, this stage entails prevention activities (developing, evaluating and enhancing physical security measures at generation, transmission, and distribution substations to prevent malicious attacks), and the reduction of attackers' access to computer and network systems.
ii. Detection and Analysis: This stage or strategy provides for appropriate diagnosis and treatment. The robust cyber-security system should be able to adequately establish the cyber-attack specifications on a system, prioritize impact response, and organize the incident report.
iii. Containment, Eradication and Recovery: This is the Reaction stage or strategy which provides for cyber defence in coordinated layers of protection. In the containment protection layer, the malicious malware is kept under control or within limits to prevent its expansion or escalation and limit its impact on the system or infrastructure. In the eradication protection layer, the malicious malware and affected systems are totally eliminated from the infrastructure computer and information system, while in the recovery protection layer, there is the retrieval and restoration of lost data and systems and the elimination of threats to the network.
iv. Post-Incident Activity: This stage or strategy entails an incident autopsy, establishing the cause and circumstances of the cyber-attack incident, and detailing the organization's reactions and non-reactions in order to adjust and enhance the organization's incident response plan.

The cyber-security strategies and incident response plan for the national energy systems infrastructure may be presented in a Cyber Security Life Cycle as shown in Figure 7 (Draffin, 2016). Vulnerabilities need to be assessed and reduced, attacks prevented when possible,

effective speedy response when attack occurs, and a thoughtful plan to recover and restore operations.

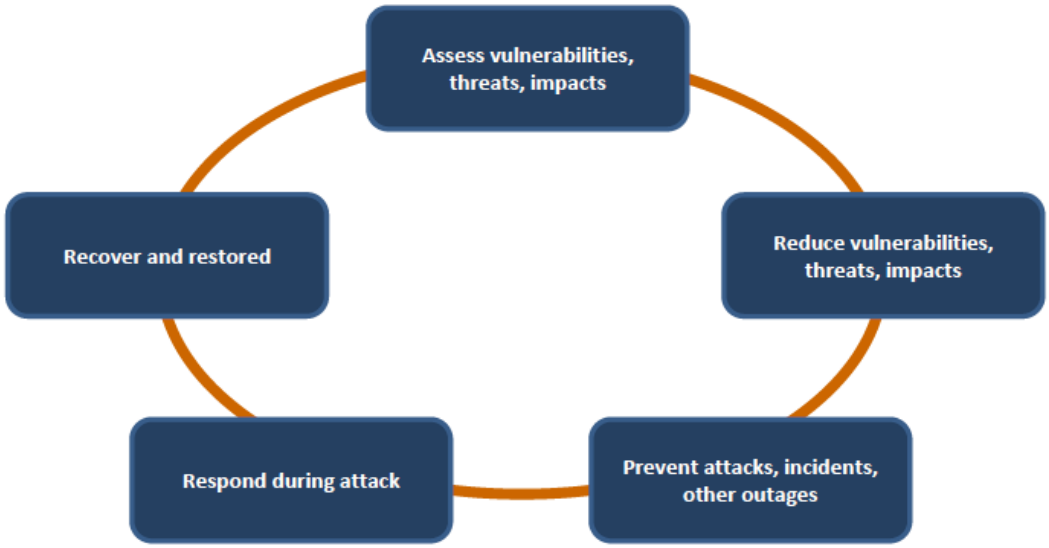

Figure 7: Cyber security life cycle
Source: (Draffin, 2016).

5.0 Summary and Conclusion

This paper focused on a cyber-security assessment of Nigeria's electric power system as an input to critical energy infrastructure policy development. A technology foresight analysis framework comprising content analysis and strategic foresight was used. The strategic assessment established that Nigeria's electric power system is a traditional, conventional, centralized grid system with old, obsolete technologies known as legacy equipment like radio-phones, manual relay circuits, limited SCADA systems and other analogue metering systems. The assessment further ascertained that the reforms, modernization and modifications in the national power sector were leading to an evolution from the legacy equipment to a hybrid configuration consisting of legacy equipment and digital, automatic systems as a prelude to a fully automated system. The new equipment includes a cyber-physical system consisting of digital metering devices, automated power flow control systems, automated pro-active protection devices, two-way electronic communication devices, self-monitoring systems amongst others. The study ascertained that the legacy equipment had limited susceptibility to cyber-attacks, but this vulnerability increased with the integration of the new cyber-physical equipment.

Out of the cyber-attacks types, classifications and threats, the national power infrastructure indicated greater susceptibility to cyber-attacks upon and by the electric power system. Cyber-attacks upon the electric power system, especially the centralized transmission system, would have significant impact on electricity supply, most likely leading to blackouts or brown-outs across the country. Cyber-attacks whereby the nation's electric power infrastructure could be weaponised against the nation are feasible especially where extended brownouts or blackouts could affect commercial and industrial output, and increased consumption of more expensive, environmentally-polluting alternative power. Cyber-attacks through the electric power system are least likely to occur due to the limited technologies in the national electric power infrastructure. The power infrastructure was considered to be susceptible to cyber-attacks by

classification and cyber-attacks by methods such as phishing, malware and data breaches, amongst others. These cyber-threats were possible across the generation, transmission and distribution systems of the hybrid electric power infrastructure. A robust, effectual, formal cyber-security system revolving around three critical resources – People, Processes, and Technology/Systems, were postulated for the national electric power system, entailing the development of an Incident Response Plan comprising documented instructions for the organization detailing four critical components or strategies, namely, preparation; detection and analysis; containment, eradication and recovery; and post–incident activity.

REFERENCES

Adegbulugbe, A. O. and Adenikinju, A. (2011) Energizing Vision 20:2020 in A. Iwayemi, W. Iledare, and A. Adenikinju (eds.) Proceedings of the 2010 NAEE Conference Book Merit Publishers, Ibadan.

Akinbami, J-F. K (2001). Renewable energy resources and technologies in Nigeria: present situation, future prospects and policy framework. *Mitigation and Adaptation Strategies for Global Change*. 6 (2), 2001, 155-182.

Akinwumi, I. O., Moses, R., and Akinbami, J-F. K. (2006) "Electric power supply strategies and productivity in selected manufacturing industries in Nigeria". *Resources, Energy, and Development*, 3(2); 107-128

Ajumogobia, O. (2015). Nigerian Energy sector legal and regulatory overview. http://www.ajumogobiaokeke.com/assets/media/2b13946e4257859eb7988150d1c620a2.pdf Accessed 14/03/2017

Alese, B. K., Thompson, A. F., Owa, K. V., Iyare, O., and Adebayo, O. T. (2014). Analysing Issues of Cyber Threats in Nigeria. In Proceedings of the World Congress on Engineering (Vol. 1).

Amin, S. M. (2002). Security challenges for the electricity infrastructure. Computer, 35(4), Pp supl8-supl10.

Amin, S. M. (2010). Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems. In *Power and Energy Society General Meeting, 2010 IEEE* (pp. 1-5). IEEE.

Amin, S. M., and Giacomoni, A. M. (2012). Smart grid, safe grid. *IEEE power and energy magazine*, *10*(1), 33-40.

Amuta, E., Wara, S., Agbetuyi, F., and Matthew, S. (2018): Smart Grid Technology Potentials in Nigeria: an Overview, *International Journal of Applied Engineering Research*, Volume 13, Number 2, pp. 1191-1200

Arya, A. K., Chanana, S., and Kumar, A. (2013). Role of smart grid to power system planning and operation in India. In *Proc. of Int. Conf. on Emerging Trends in Engineering and Technology*.

Atoyebi, A., Ogundari, I.O., and Akinwale, O.Y. (2013). Comparative techno-economic analysis of a grid and off-grid electric power supply for a new housing estate development in North Central Nigeria". Seminar presented at the National Centre for Technology Management (NACETEM), Federal Ministry of Science and Technology (FMST)

Awosope, C. A. (2014). Nigeria Electricity Industry: Issues, Challenges and Solutions. Covenant University 38th Public Lecture, 3(2).

Babatunde, M.A. and Shuaibu, M. I. (2008). The demand for residential electricity in Nigeria:
A bound testing approach.

Baigent, D., Adamiak, M. and Mackiewicz, R. (2011) IEC61850 Communication Networks and Systems in Substations: An Overview for Users. http://www.sisconet.com

Chhaya, L., Sharma, P., Bhagwatikar, G., and Kumar, A. (2017). Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control. *Electronics*, 6(1), 5.

Collier, J. (2017). Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom. In Ethics and Policies for Cyber Operations (pp. 187-212). Springer International Publishing.

Cyril W. and Draffin, Jr (2016). Cyber-security White Paper. MIT energy initiative utility of the future, https://energy.mit.edu/wpcontent/uploads/2016/12/CybersecurityWhitePaper_MITUtilityofFuture_-2016-12-05_Draffin.pdf Accessed 23/05/2017

Dagoumas, A. (2019): Assessing the impact of cybersecurity attacks on power systems, *Energies*, 12, 725; doi:10.3390/en12040725

Dán, G., Sandberg, H., Ekstedt, M., and Björkman, G. (2012). Challenges in power systeminformation security. IEEE Security & Privacy, 10(4), 62-70.

Desarnaud, G. (2017). Cyber-attacks and Energy Infrastructures: Anticipating Risks. *Etudes de l'Ifri,* https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf Accessed 02/01/2018

Development in Nigeria (2013). A paper presented at the 6th Annual NAEE/IAEE International Conference held at Sheraton Hotel, Lagos, from April 22-23.

Ejumudo, T. F. and Ejumudo, K. B. O. (2014): The operations of the Power Holding Company of Nigeria and discriminatory monopoly, Journal of energy Technologies andPolicy, Vol 4, No 6, pp 60 – 68.

Emodi, V. N., Yusuf, S. D. and Boo, K. J. (2014), The necessity of the development of standards for renewable energy technologies in Nigeria, *Smart Grid and Renewable Energy*, 5(11), pp. 259–274, 2014. https://doi.org/10.4236/sgre.2014.511024

Folorunso, O., and Olowu, T (2014). The Nigerian Power System till Date: A Review. *International Journal of Advance Foundation and Research in Science & Engineering*, 1(5).

Galadima, H. (2016). New security architecture for Nigeria: a holistic approach to rebuilding the nation-state. Being a paper presented at the National Institute for Policy and Strategic Studies (NIPSS), Kuru, Nigeria. https://savannahcentre.org/paper-new-security-architecture-for-nigeria/ Accessed on 8/8/2017.

Gu, Q., and Liu, P. (2007). Denial of service attacks. *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications*, *3*, 454-468.

Ibitoye, F., and Adenikinju, A. (2007), Future demand for electricity in Nigeria; *Applied Energy*, Volume 84, Issue 5, Pages 492-504

Ijewere, A. A. (2011). The Management of Electricity Power Supply in Nigeria Problems and Prospects. *Journal of Research in National Development*, 9(2), 173-185.

Ikekpeazu, F. O. (2018): Towards systems Management in the electric power sector for physical facilities in Nigeria: Issues, challenges and new directions, *PM World Journal*, Vol VII, Issue IV

INL (2016): Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector; Idaho National laboratory: Idaho Falls, ID, USA,

Iwayemi, A. (2008). Nigeria's dual energy problems: Policy issues and challenges. *International Association for Energy Economics*, pp 17-21.

Jarmakiewicz, J., Ma´slanka, K., and Parobczak, K. (2015): Development of Cyber Security Testbed for Critical Infrastructure. In Proceedings of the 2015 International Conference on Military Communications and Information Systems, Cracow, Poland, 18–19 May.

Knake, R. K. (2017): A Cyberattack on the U.S. Power Grid, http://www.iaem.com/documents/CFR-Contingency-Planning-Memo-Krake-Apr2017.pdf

Koledoye, T. O., Abdul-Ganiyu, J. A. and Phillips, D. A. (2013): The Current and Future Challenges of Electricity Market in Nigeria in the Face of Deregulation Process. *African Journal of Engineering Research*, 1, 33-39

KPMG Nigeria (2016): A Guide to the Nigerian Power Sector.

Lewis, J. A. (2013). Raising the Bar for Cyber-security. Centre for strategic and international studies. https://csis-prod.s3.amazonaws.com/s3fspublic/legacy_files/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf Retrieved 4th of April, 2017

Lin, Tom C. W., Financial Weapons of War (2016). Minnesota Law Review, Vol. 100, p. 1377, 2016; Temple University Legal Studies Research Paper No. 2016-25. Available at SSRN: https://ssrn.com/abstract=2765010

Liao Y (2013): Transformation of Electric Power Grid into Smart Grid. *Int J Adv Innovat* Thoughts Ideas 2: 149. doi: 10.4172/2277-1891.1000149

Lionel, E. (2013): The dynamic analysis of electricity supply and economic development: Lessons from Nigeria. *Journal of Sustainable Society*, *2*(1), 1-11.

Malladi, S., Alves-Foss, J., and Heckendorn, R. B. (2002): On preventing replay attacks on security protocols. IDAHO UNIV MOSCOW DEPT OF COMPUTER SCIENCE.

Momodu A. S. (2012): Evaluation of long term performance of electric power system in Nigeria. Ph.D. Thesis, Obafemi Awolowo University, Ile-Ife, Nigeria

Mrabet, Z. E., Kaabouch, N., Ghazi, H. E., Ghazi, H. E. (2018): Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng*. 2018, 67, 469–482.

Negrete-Pincetic, M., Yoshida, F., and Gross, G. (2009): Towards quantifying the impacts of cyber-attacks in the competitive electricity market environment. In PowerTech, 2009 IEEE Bucharest (pp. 1-8). IEEE.

Nnaji, B. (2011): Power sector outlook in Nigeria: government renewed priorities. *presentation at Securities and Exchange Commission, Abuja, June*.

Ogundari, I. O., Akinwale, Y. O., Adepoju, A. O., Atoyebi, M. K., and Akarakiri, J. B. (2017): Suburban Housing Development and Off-Grid Electric Power Supply Assessment for North-Central Nigeria. *International Journal of Sustainable Energy Planning and Management*, *12*, 47-63.

Ogundari, I.O., O.R. Olaopa, O.A. Jesuleye, I.G. Nwosu, and W.O. Siyanbola, (2011): An Analysis on Electric Power Requirements for Techno-Economic Development in Nigeria. A paper presented at the 2011 National Solar Energy Forum „NASEF 2011" of the Solar Energy Society of Nigeria, Sokoto Energy Research Centre, Usman Dan Fodio University, Sokoto, November 14-18.

Olagoke, A. S., Dahiru, A. B. and Salawu, A. (2018), Assessing the integration and automation of energy systems in Nigeria, *Int. J. of Energy Prod. & Mgmt*., Vol. 3, No. 3, pp. 191-200

Ogundari, I. O., Akinwale, O. Y., Olaopa, O. R., Akarakiri, J. B. and Siyanbola, W. O (2014): An Analysis on Electric Power Supply, Electricity Sectoral Allocation and Off-Grid Power Supply Technologies for Sustainable development in Nigeria, In Adenikinju, Iwayemi and Iledare (Eds) Energy Resource Management in a Federal System Challenges constraints and strategies.

Olaopa O., Ogundari, I. O., Awoleye, M., and Siyanbola, W. O. (2009): "The politics and policies of oil deregulation in Nigeria: Implications and policy suggestions". Contending Issues in the Niger Delta Crisis of Nigeria. JAPSS Press Inc, Houston, 203-256.

Onochie, U. P., Egware, H. O., and Eyakwanor, T. O. (2015): The Nigeria Electric Power sector (opportunities and challenges). *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, 2(4).

Onohaebi, S. O. (2014), Smart Grid and Energy Management in Nigeria Integrated Power System, *International Journal of Engineering Innovation & Research*, Volume 3, Issue 6, ISSN: 2277 – 5668

Oseni, M. (2011): An analysis of the power sector performance in Nigeria, *Renewable and Sustainable Energy Reviews*, 15(9), pp. 4765–4774.

Oshevire, P., Oladimeji, T. T., and Onohaebi, S. (2013): Smart grid technology and its possible applications to the Nigeria 330 kV Power System. *Smart Grid and Renewable Energy*, 4(05), 391 – 397.

Sambo, A. S. (2005): "Renewable Energy for Rural development: The Nigerian perspective". ISESCO: Science and Technology Vision, Vol. 1.

Sambo, A. S. (2008). Matching electricity supply with demand in Nigeria. International Association for Energy Economics (IAEE) Newsletter, Fourth Quarter.

Seissa, I. G., Ibrahim, J., and Yahaya, N. (2015) Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review, *International Journal of Science and Research*, Volume 6 Issue 1

Sun, C. C., Hahn, A., and Liu, C.C. (2018): Cyber security of a power grid: State-of-the-art, *Int. J. Electr. Power Energy Syst.*, 99, 45–56.

Sridhar, S., Hahn, A., and Govindarasu, M. (2012). Cyber–physical system security for the electric power grid. Proceedings of the IEEE, 100(1), 210-224.

Ten, C. W., Liu, C. C., and Govindarasu, M. (2008). Cyber-vulnerability of power grid monitoring and control systems. In Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead (p. 43). ACM.

The Edison Electric Institute (2014). The Electric Power Industry's Commitment toProtecting Its Critical Infrastructure.

PwC (2016). Powering Nigeria for the future. Retrieved [online] on 23rd of May, 2017 from https://www.pwc.com/gx/en/growth-markets.../pdf/powering-nigeria-future.pdf,

Trustees of Dartmouth College (Institute for Security Technology Studies) (2002) Cyber security of the electric power industry.Accessed from www.ists.dartmouth.edu/library/218.pdf on 23 May 2017

Ublock (N. D.): The Looming Threat of a Cyber Attack, https://ublock.org/cybersecurity-essentials/the-looming-threat-of-a-cyber-attack/

Vellaithurai, C., Srivastava, A., Zonouz, S., and Berthier, R. (2015). CPIndex: cyber-physical vulnerability assessment for power-grid infrastructures. *IEEE Transactions on Smart Grid*, *6*(2), 566-575.)

Vincent, E. N. and Yusuf, S. D. (2014): Integrating Renewable Energy and Smart Grid Technology into the Nigerian Electricity Grid System, *Smart Grid Renew. Energy*, Vol. 05, No. 09, pp. 220–238.

Watts, D. (2003). Security and vulnerability in electric power systems. In 35th North American power symposium (Vol. 2, pp. 559-566).

Yatsu, M., and Aihara, T. (2013). Power System Technologies for Reliable Supply of Electric Power and Wide-area Grids. *Hitachi Review*, *62*(1), 53.

Yin, H., Xiao, R., and Lv, F. (2015). Analysis of Causes and Actual Events on Electric Power Infrastructure Impacted by Cyber Attack. Journal of Power and Energy Engineering, 3(04), 77.

Zhang, Y. Q. (2011): Network Attack and Defence Technology. Tsinghua University Press, Beijing, 59-65.