

Threats and Challenges of Smart Grids Deployments - A Developing Nations' Perspective

Abdulrahaman Okino Otuoze^{1,2*}, Mohd Wazir Mustafa¹, Oladimeji Ibrahim², Sani Salisu^{1,3}, Olatunji Obalowu Mohammed^{1,2}, Abdulkarim Ayopo Oloyede⁴ and Zubairu Salisu Gaya³

¹School of Electrical Engineering, Universiti Teknologi Malaysia, 81310 UTM Skudai, Johor, Malaysia

²Department of Electrical and Electronics Engineering, University of Ilorin, Ilorin, Nigeria

³Department of Electrical Engineering, Ahmadu Bello University, Zaria, Nigeria

⁴Department of Telecommunication Science, University of Ilorin, Ilorin, Nigeria

*Corresponding author: ooabdulrahaman2@live.utm.my

Abstract: Considerable efforts in huge investments are being made to achieve a resilient Smart Grids (SGs) deployment for the improvement of power delivery scheme. Unsurprisingly, many developing nations are making slow progress to the achievement of this feat, which is set to revolutionize the power industry, own to several deployment and security issues. Studying these threats and challenges from both technical and non-technical view, this paper presents a highlight and assessment of each of the identified challenges. These challenges are assessed by exposing the security and deployment related threats while suggesting ways of tackling these challenges with prominence to developing nations. Although, a brief highlight, this review will help key actors in the region to identify the related challenges and it's a guide to sustainable deployments of SGs in developing nations.

Keywords: Challenges, Developing Nations, Deployment, Smart Grid, Threats.

© 2019 Penerbit UTM Press. All rights reserved

Article History: received 30 July 2019; accepted 17 August 2019; published 31 August 2019.

1. INTRODUCTION

Adequate access to improved and sustainable electricity has remained a mirage, especially in developing nations, in addition to operating a very old conventional and overloaded power network which also lack reliability, resiliency and robustness as well as very slow pace of renewable energy integrations [1-3]. Electricity thefts, infrastructural thefts and decay, associated operational inefficiencies, and manipulations by various stakeholders are notable factors plaguing these conventional grid systems [2, 4, 5]. The conventional power systems often do not provide consumers with adequate knowledge of their consumptions and energy efficiency in general. Also, the little information they are provided come with no incentives to help adapt customers' demands which could be a considerable advantage to utility companies [6, 7].

In most settings, the customers are made to suffer overbillings as a result of unmetered or estimated billings [8, 9]. The regular power outages by extension inflict heavy damages on the economy, hence lowers the growth of the countries, especially in terms of GDP [10]. For instance, industrial activities have been on the low in several developing nations due to erratic power supplies. More than 30 African countries currently experience irregular power supplies [11] with a large percentage of its population having no access to electricity.

The inefficiencies result on the account of low investment in the power sector, employees' ineptitudes,

lack of proper maintenance, vandalism, social vices and poor policies' formulations and implementations. Furthermore, many developing nations struggle to meet its electricity demand and as such blackouts have become not only very popular but a normal situation to which the citizens must adapt despite several hours of power outages on daily basis [10] with its associated economic and human developmental losses. Provision of basic infrastructure for quality water, efficient health care delivery systems, efficient digital marketing structure, and general provision of other basic facilities such as housing, roads, rails etc. remain associated lingering issues. This is a major concern for these nations because every critical sector relies on stable and efficient power supplies.

Being a critical infrastructure, the power grid imparts directly on all aspects of the economy hence, considered a key driver of the societal growth and development. This necessitates the dare need for its security to be guaranteed [5]. Therefore, adequate, optimized and a well-secured power delivery scheme must be deployed in any economy to help it overcome energy crises [12]. In developing nations, an estimated quarter of the urban poor populations reportedly lack access to electricity [11]. This is worsened by the ever-growing electricity demand due to rapid social-economic development being recorded worldwide driven by modern and digital economies which increasingly depend on electricity hence, subjecting the existing grid to heavy pressure in satisfying the growing demands [13].

The securities of the grid systems are quite essential given its high capital-intensiveness both in human and capital strengths. Hence, necessitating distinct imaginative and state-of-the-art solutions for a sustainable system. However, achievement of a cost-effective, secured and reliable power supplies has posed dare challenges to the present day global economy as many concerns such as lack of access to the grid at reasonable and controllable prices, high costs of primary energy sources, high installation cost of renewable energy systems, increasing greenhouse gas emissions [14, 15] etc. are yet to be substantially addressed. Worldwide, about 1.1 billion people reportedly lack access to electricity as at 2017 with a compounding scenario of associated huge cost of connecting many remote areas to the grid [16-21].

Since no nation triumphs, if its larger population lack quality access to electricity [22], the imminent challenges such as old systems which are no longer suited for power operations of the 21st century must therefore, be comprehensively studied [23]. To achieve this, energy efficiency has become the basis of current and future researches, demanding the deployment of energy-efficient technologies at various levels of power delivery schemes [7]. As suggested in [24], every energy efficient process can be evaluated using the four A's of energy security namely, availability, accessibility, affordability, and acceptability; and this leads to the concept of smart Grids (SGs) although with more requirements for security concerns.

SGs are improved power networks providing intelligent and multidirectional digital communication by interconnecting, monitoring and controlling the various components of the schemes for efficient and secure delivery of sustainable power supplies [5, 25-31]. This grid system is highly amenable to integration of renewable supplies using enhanced and automated controlled communication technologies with all the components interacting via communication sensor nodes and paths to achieve the multidirectional flow and interoperability and hence, increases the efficiency of operations as well as environmentally friendly system [23, 32-34].

However, the deployment of this enhanced grid system has come under several challenges with both technical and non-technical dimensions. These problems are faced by both developed and developing economies but given the gross underdevelopment of most of the developing nations with myriads of issues, this paper focuses on the challenges facing the developing nations. It assesses these challenges based on the technical and non-technical views but only highlights some selected aspects of these factors based on the security threats and solution approaches presented in literature. This work is an extension of the review presented in [35]. Next, section II highlights briefly, the general overview of the deployment challenges with emphasis on the technical and non-technical aspects explained in section III. While some of the selected challenges are assessed in sections IV through section X, section XI concludes the paper.

2. SMART GRIDS DEPLOYMENT CHALLENGES

SGs deployments are aimed to improve the efficiency, flexibility, reliability, resiliency, and security of the power delivery scheme [5, 7, 25, 27, 36]. This is achieved by efficient data collection, analysis and actuation of various monitoring and control mechanisms for a multidirectional communication flow and detection of faults to allow for self-state assessment and healings [7, 32]. The various aspects of SGs deployment to enhancing the grid's infrastructure, requirements for future planning and expansions include smart metering (SM) via advanced metering infrastructure (AMI), incorporations of distributed generations (DGs), integration of renewable energy systems (RES), smart distribution management (SDM), introduction of electric vehicles (EVs), demand-side management (DSM) and demand response (DR), smart energy storage (SES) systems, emission monitoring and regulations (EMRs), network reconfigurations (NRs), advanced electricity marketing (AEM) [13, 27, 37, 38] etc. the advanced metering infrastructure (AMI) is central to all the components and most crucial aspect of the SGs, hence, SGs deployments mostly begin with the metering unit at all components of the power delivery schemes.

The United States (US), European Union (EU), and China are in the lead by setting up extensive Research and Development (R&D) program in SGs while equally investing heavily in it [39]. China, Russia, India, and Brazil are a few of the developing nations making significant strides with a proper roadmap for huge deployment [29, 40]. From 2014 to 2016, SGs investments went up by 12% despite a low growth rate of 3% recorded in 2017 for smart distribution networks [41]. Many countries are making momentous efforts in smart electricity meters (SEMs) distribution, though, it is highly uneven across all regions, but a reflection of committed investments made by each region.

About \$200 billion was earmarked to be invested in SG infrastructure between 2010 and 2015 worldwide, according to Pike research report [7]. In 2013, a Navigant research estimated SG deployment will nearly double by 2020 to about US\$73 billion and US\$461 billion in annual revenue and cumulative profit, respectively [31]. Fig. 1 [41] shows SG deployment by region across the world from 2015 to 2017. From 1990, China's residential electricity consumption surged from about 48 billion kWh to 718 billion kWh in 2014 [42] following a concerted investment in SG deployment. Thailand planned a 15 year deployment to the tune of about US\$ 13 billion as confirmed by the Provincial Electricity Authority (PEA) [29].

Between 2004 and 2012, India recorded 15% increase in its populations' access to electricity from 59% to 74% but also has to deal with growing demand put at 5% per annum through 2030 [43]. As an action plan, India established a National Smart Grid Mission and budgeted over USD 5.8 billion for the period from 2012 to 2017 to deploy SGs [44]. In Malaysia, SGs investment went up from \$35.2 million to \$109.0 million between 2011 and 2016 with the country targeting an expansion in its renewable energies' supplies to 2080 MW and 4000 MW by 2020 and 2030 respectively. Malaysia currently runs a

pilot programme of SG deployment with US \$60 billion commitment to run through 2030 in its ancient city of Melaka [45]. The country has been able to achieve 100% electricity access [46] and with 5% power consumption growth per annum projected for the next five years which is even forecasted to double in the next 20 years [29], the country is considered as an emerging economy in the comity of developing nations.

Aside the involvement of its huge investments engulfing billions of United States dollars, SGs deployment just as any cyber-physical systems, comes with enormous security issues, challenges and vulnerabilities despite its numerous advantages. Physical damages to infrastructure, possibilities of customers' privacy breaches, general unauthorized access in form of malicious software or hardware attacks, lack of stable policies or poor implementations of formulated policies [31, 47] are a few possible threats.

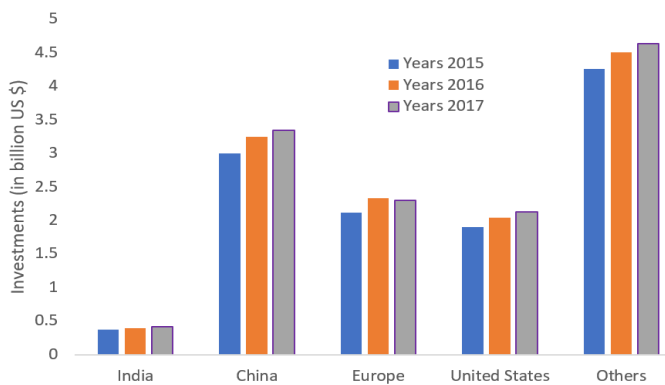


Figure 1 SGs investments by region from 2015 to 2017

Therefore, the deployment must follow a laid regulatory framework by international standard and must follow a well-structured business and technical model for a smooth operation and increased economic returns for the benefits of all players to ensure consumer protections and incentives [30, 48].

As the deployment widens, the reliability grows to be of major concerns, hence, requiring new analytical tools from research outputs [49] and advances in flexible renewable integration [12, 50] leading to reduced environmental emissions and increased energy efficiency [29]. However, they must be examined from all standpoints to ensure a successful deployment. Challenges abound worldwide in SGs deployments but those of the developing nations have special dynamics only peculiar to them. These challenges presented from both technical and non-technical standpoints are highlighted in the next following sections.

3. THE TECHNICAL AND NON-TECHNICAL CHALLENGES

The related SGs deployments' challenges to developing nations have raised so many concerns and depending on the nature of the challenges, they are grouped as either technical or non-technical. The challenges associated with the infrastructure itself or the operations formed the chunk of the technical challenges. Some of the factors include a wide demand-supply gap, installation safeties and bottlenecks; operational requirements and limits;

infrastructural safeties, operations, faults and maintenance; cyber-attacks, power thefts etc. The non-technical factors are majorly the external influencing criteria for a sustainable system, and these include formulation and implementation of regulatory policies, administrative issues, the political or leadership will to invest in the technology, employment of needed skill personnel, corruption, terrorism, prompt and efficient disaster management etc. Despite the challenges militating against the deployments, solutions abound on how they can be tackled. Some schemes presented in [4, 51-55] highlights how the grid can be secured. The next sessions give the highpoints of selected technical and non-technical challenges.

4. WIDE DEMAND-SUPPLY GAP

Most developing nations operate a power system which ultimately suffers higher demand compared with the supply as in the situation of Ghana, South Africa, Pakistan, India, Nigeria [10, 15, 56] etc. however, developing nations including Malaysia, China, Thailand and a few others have achieved 100% access to electricity. Figure 2 [57] depicts the electricity access of some selected developing nations. Several sub-Saharan African nations are worse off in this situation. The comparison trend of Figure 2 shows the difference among the shown regions and countries. The wide gap in the demand and supply pose dare difficulties in carrying out proper load shedding for optimal operations [58].

If supplies and access to electricity were adequate, demand response (DR) would be perfectly achieved as customers can conveniently take the full advantages in response to systems' overloads and pricing [38, 39]. Hence, allowing for customers to enjoy the associated incentives. The utility companies will be able to control peak power conditions on the grid effectively reducing the running cost while the customers' incentives usually come in form of controlled consumption which makes them active in the energy market and grants them an optimal mode of utilizing the running of the SGs [19, 30, 40, 41].

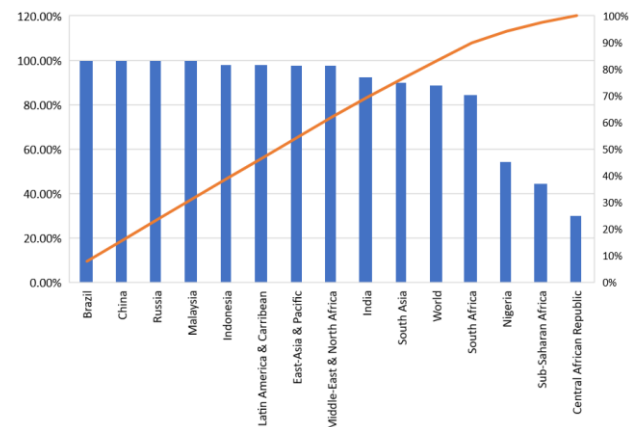


Figure 2. Access to Electricity (% of Population as at 2017) of selected Regions and Countries

DR program and pilot projects are most active in the US, China, Japan, Korea and UK with their markets having established regulatory policies and program [30].

DR also allows for off-grid source usually serving as backup for critical loads and hence, reduces dependence on the main grid [59]. By implication, DR program are achieved optimally if the demand-supply gap is not too wide. Unfortunately, most developing nations including those of middle East, sub-Saharan Africa and many parts of Asia still operate a power system supplying far below the demand. Worse still, most of those nations are not able to supply power for more than 12 hours per day.

Therefore, massive efforts are needed to critically provide for more generations as well as expansion of transmission capacities. Coincidentally, most of the developing nations in this category have abundant solar potential which are yet to be maximally tapped this potential. This is in spite the global trend of realizing distributed generations (DG) by harnessing renewable energy systems to derive its huge benefits especially to the environments [60-62].

5. ELECTRICITY THEFT AND SMART METERING

Worldwide, electricity theft menace is causing huge setback as billions of dollars are reportedly lost thereby causing utilities and governments enormous losses in revenue. Electricity theft inflicts the energy sector with shortage of fund for increased investments. Also, the governments are forced to consider subsidy payments else honest customers may be burdened in making up for the losses [43, 63, 64]. This also contributes to the ever-increasing demand-supply gap since accurate records for proper planning are tampered and consequently discourages the utilities from further commitments.

Some of the modes by which this unfortunate act is committed include physical manipulations of the meters, partial bypass involving connections of only a few loads, complete bypass of the meter where the meter is merely mounted to deceive officials but never connected, receipts of tips from customers to perpetuate billing irregularities, unpaid bills by unfaithful customers which usually lead to what is termed as 'bad debt', issuance of threats by thugs (which may prevent utility staff from either issuing bills or sanctioning some customers for unpaid bills) [43, 64] etc. The authors in [56] blamed high level of corruption as being responsible for power theft in most developing countries citing India and Pakistan scenarios.

According to World bank data, India, Brazil, China and US lose about 25%, 16%, 6% and 5% of their generated power, respectively [56, 65]. Pakistan reportedly loses about 20.4% of its dispatched energy [66] while this figure is put above 40% for the whole of southeast Asia [67]. Nigeria reportedly loses about 34%. In terms of yearly revenue, US, UK, India, Malaysia and Brazil reportedly lose over \$6 billion, GBP 173 million, \$16.2 billion, RM500 million and \$5 billion, respectively [43, 68], to the same menace. Northeast group LLC reported that worldwide, \$89.3 billion are lost due to electricity theft on yearly basis [69] With several other nations incurring the distress imposed by this menace in their various degrees. Developing nations reportedly loose between 20 to 50% of their expected revenue and this percentage is not even good news for the developed

nations as their records show between 3.5 to 30% loss [35, 68, 70].

A study conducted in Ghana on selected populace found that high electricity prices, corruption, poor law enforcement, and regulatory system, poor power supply quality, mass unemployment and high level of illiteracy could be blamed for electricity theft [71]. Meanwhile, a study by [56], had earlier identified suggested factors for reducing electricity thefts to include higher income earnings, poverty rate reduction, increased tax to GDP index, enhancement in electricity billings and collections, reduced corrupt practices by all players, increased involvements of the private sector in the grids' operations, improved literacy and awareness etc. a number of schemes have been presented for curbing electricity thefts in SGs environments [72-76].

Inspection of customers to determine abnormal load profile suspected theft cases is a common practice irrespective of whatever scheme used to detect electricity thieves [73] but comes with huge setbacks such as requisite large manpower, high cost of execution, connivance of utility staff with some customers, long period of time for little inspection, possibility of harassment of utility staff etc. Fortunately, Smart Electricity Meters (SEMs) deployment as a fundamental component of the advanced metering infrastructure (AMI) in SGs has brought about efficient metering, monitoring, and control between the essential parts and players of the grid [6, 68, 77], hence, aiding consumers and utility to better monitor consumptions with enhanced security [36, 48, 78, 79].

For maximum derivation of the systems' advantages for the end users, dynamic demand response, time-of-use (TOU), real-time pricing (RTP) and critical peak rebates (CPR) are some time-based rates offered to customers [80, 81]. They help achieve energy savings, cost reductions, adequate flexibility, security, offer magnificent data for further processing and are the key aspect of smart city design utilizing internet of things (IoT) [29, 30]. SEMs specifically help to monitor customers' consumption, and this can be improved usually by the application of machine learning-based algorithms capitalizing on its advantage of providing high frequent sampling data compared to the traditional meters [67]. Installations SEMs worldwide, are estimated at 313 million, 852 million and 1.1 billion by the years 2013, 2018 and 2023, respectively [26, 82].

Despite the advantages, the AMI's dependence on communication networks renders it vulnerable to so many threats and attacks. Hence, adversaries have found new dimensions to electricity thefts [43]. Customers' data safety is another major worry given the issues of breach of trusts and order most common in developing economies. This data, if disclosed inappropriately, could lead to serious privacy and security breach. Internet-based smart meters and especially google meters have been proposed in some works, but fears have grown about its possibilities of being hijacked for attacks [64, 83-86]. Hence, SEMs remain susceptible to cyber and other related physical manipulations and has become a source of worry in SGs deployments [87].

Although, SEMs have proffered proven supports for electricity theft detection, issues abound which have grown to be of major concerns in developing economies. Unstable political atmosphere, high corruption tendencies, high costs of the meters, insincerity of distribution companies since they make more money by estimated billings, growing cyber-attacks, failure of power regulators to implement rules and regulations guiding the utility companies etc. are just but a few of the factors militating against the deployments. Therefore, more studies must be carried out before full deployment to ensure safe and successful operations. Several works on the security of SEMs have been presented [26, 74, 88, 89] and more.

6. INFRASTRUCTURAL ATTACKS AND CYBERSECURITY

SGs deployments are envisioned to revolutionize the power schemes but the associated threats of its deployments pose major worries given the uniqueness of developing economies' various security issues involving thefts of infrastructures or attacks on them at the slightest provocation and the growing cyber-attacks [44, 90]. These could manifest as a result of thefts, state attacks, war, natural disasters, terrorism or any act of sabotage [91] hence, requiring concerted efforts to curb. The dependence of SGs on information technology utilizing communications and networking systems has unavoidably exposed it to myriads of vulnerabilities [92-95]. Transmission systems are reportedly the most targeted as over 60% of attacks on the grid targeted the subsystem. Transformers, Power relays, junction boxes, and the metering systems are also key areas suffering various attacks [44].

Generally, the critical energy infrastructure (CEI) including gas pipelines, gas plants etc. are often at the mercy of insurgent activities and terrorism [25] e.g. attacks by the Niger Delta Avengers on oil infrastructure in Nigeria (NGPowerHub, 2016), reported vandalism by hoodlums causing Kano Distribution Company of Nigeria a loss of about N108m (Daily Trust Newspaper, 9th Sept, 2016), state attacks such as the extensive energy 'denial' operations during the Iran-Iraq war of the 1999 Kosovo campaign, the huge destructions carried out by terrorists around the world [96, 97] etc.

With cyber-attacks set to cost global economy a huge sum of around US\$445 billion, it is certainly a grave threat to SG deployment [98, 99]. Detected in 2010 and with its capability to inflict physical damage to infrastructure, Stuxnet has grown to become the most famous cyber-attack [100]. Unlike physical attacks such as armed assaults, cyber-attacks pose dare threats involving critical process of detection [25]. An alarming rate of cybercrimes is equally experienced in Africa, Figure 3 [101] shows the cost the selected countries incur to fight cybercrimes despite being considered low in IT deployment and Figure 4 [54] shows how the African continent is spending on cybercrimes by industries.

Given the susceptibility of the CEI, it requires sophisticated solutions backed by critical vulnerability analysis to deliver reliable and secure energy supplies

[36, 38]. The wireless area network (WAN) must provide and support a secure end to end transmission to ensure the three main objective of a cyber-free system viz confidentiality, Integrity, and Privacy of data [102]. Although, some works have been presented on curbing cyber-attacks [4, 38, 44, 58, 94, 99, 103, 104], its ever-dynamic nature remains a worrying threat to SG deployments as no guarantee of a perfect system can be ascertained. And this is compounded by the rise in cybercrimes and poor response to fighting this crime in most developing worlds.

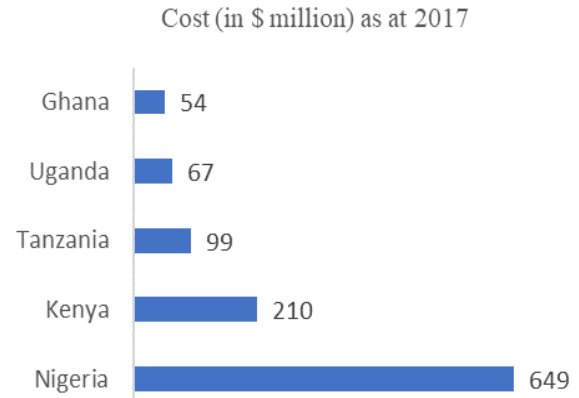


Figure 3. Cost of cybercrimes in selected African economies

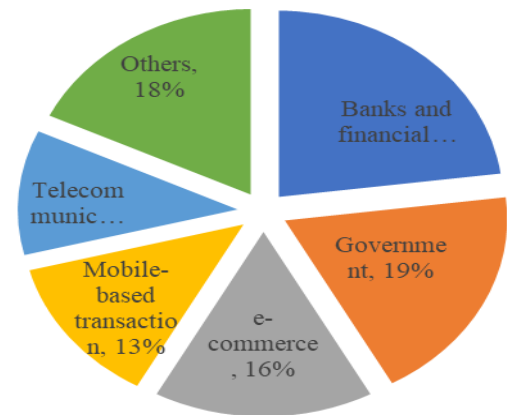


Figure 4. Cybercrimes cost in Africa (% of total) by Industries

7. TERRORISM

A damning threat which has greatly hit many parts of the worlds is terrorism. Although, a worldwide threat, its worse in developing nations especially those of the Middle East and Africa and it has led to huge destruction of lives and properties. Terrorism is being a responsible factor fueling violence and instability recently and causes long-term socio-economic damages in addition to immediate injuries, death and infrastructure damages. The high number of human lives often take precedence in reportage and in most cases, infrastructural damages are never captured even though they are hugely affected. This can occur in form of insurgency, war between states,

attacks by terrorist groups etc. Due to enormous effects, cost of doing business is often caused to surge up usually based on higher insurance premiums, sophisticated and expensive security measures, higher levels of uncertainties, reduced human, capital and physical resources, reduced gross domestic product (GDP), relatively higher salaries to at-risk employees [105-108] etc.

Therefore, it poses indefinable challenges to electricity infrastructure and given the high cost involvements as well as the complexities in SGs deployment, adequate measure must be taken to ensure requisite securities of the infrastructure. Where developed worlds have gone far in deploying secure measures, most of the developing world's struggle, even for the most basic security. Hence, the deployment of SGs automatically suffers some setback and requires that improved efforts be made before any massive deployment is made.

8. CLIMATE CHANGE, ENVIRONMENTAL THREATS AND DISASTER MANAGEMENT

Smart grid deployment poses high vulnerability to extreme weather situations and it is therefore crucial to assess all the power grid subsystem as growing investment requires improved system planning for sustainable deployment in the faces of climate change [109]. Extreme weather condition is listed amongst the top ranked global risks [99] and poses highly significant threats to future grid systems. To address this, human activities must be reassessed to ascertain ways of optimal control [110] especially by formulating and adopting policies aimed at addressing climate change [45, 111]. The 2015 Paris agreement signed under the UN framework convention is expected to be a key driver in addressing extreme weather condition with the commitment of 195 countries although the pulling out of the United States dealt a major blow. Luckily, SG technologies aid high level of renewable integration and hence, directly facilitate reductions in greenhouse gas emissions (GHG) thereby increasing the resiliency of CEI to climate change effects. However, the environmental impact of electricity systems must be a key priority by ensuing pollution prevention and a significant reduction in GHG emissions [108, 109].

Despite the efforts in the adoption of renewable energy systems, fossil fuel remains the dominant primary source of energy but its reported depletion, persistent fuel price hike, global warming and other environmental issues [112] dictate that pursuance and achievement of environmental safety is non-negotiable. Hence, all aspects of environmental safety especially the management of natural environmental hazards such as landslide, flood, earthquake, hurricanes etc. which could inflict severe havoc on power infrastructure need holistic assessment for successful SGs deployment.

In a more diversified and developed economy, such losses may have a temporary influence as resources are reallocated to other sectors or better security measures are promptly deployed to cushion the fears and save the situations while developing economies due to their limited resources and lack of commitments, manage

disasters in a rather abysmal manner thereby posing a major concern in SG deployment. Hence, the need for electricity sector to protect itself against natural disasters for increased resiliency of the system.

9. CORRUPTION AND POOR GOVERNMENT POLICIES & IMPLEMENTATION

Corruption can be identified in form of bribery, extortion, nepotism, exchange of favors, cronyism, judicial fraud, accounting fraud, electoral fraud, public service fraud, embezzlement, kleptocracy, influence peddling and conflict of interest [113]. Unfortunately, most developing nations suffer a severe unacceptable level of corruption. While efforts are ongoing by some of these nations to curb the menace which is fast crippling their economy, some appear very soft on this battle although, basically due to lack of political will. In most cases, cash released for projects are diverted and embezzled with little or no consequence. Governance issues have presented corruption related concerns mostly in Africa, South America, Asia, and Middle East countries. This is worsened by the persistent affinity of their leaders to cling to power even after some unproductive years in office. In [56], political instability, bribery and corruption, and lack of stability are said to be responsible for poor governance.

In Latin America, Brazil is said to be the largest electricity market and is indeed, one of the global emerging markets. However, SGs deployments have slowed due to poor regulatory policies, technical hurdles and the recent economic downturn [108]. A survey shows that rural Africans tip improved electricity and good roads as key developmental stride across the region [110]. So many roadmaps and frameworks have been drawn and budget allocated all for increased power infrastructure but always hardly materializes due to corruption, political instabilities, and poor policies implementation. In a 2014 report, most Africans believed corruption has cost the citizens, provision of reliable electricity and good roads [110].

A well-articulated, and highly monitored investment via a well-established policy framework with sincere political will devoid of the recurrent corrupt practices will yield a giant stride in SGs deployments [114] in the developing nations. Necessary collaborations must be established among utilities, governments, industries, and academia for any meaningful progress in a fully secured SG deployment across developing nations as is the case in most developed nations

10. RESEARCH FUNDING AND PLANNING

Most developing nations operate based on a very low budgetary allocation with low percent dedicated to power sector improvement. Hence, hampering the deployment of power scheme infrastructure even when the leadership is fully committed. China reportedly experienced slower economic growth from 7.7% to 7% and 7.3% in 2013 and 2014, respectively, with a fall in investment in electricity infrastructure [108]. Budget cuts and uncertainties in ease of doing business has continued to stagger in developing

nations in the face of political and economic instabilities [108].

The International Energy Agency (IEA)'s estimation of Sub-Saharan's electrification from 30% to 70% in 2040 set to gulp about \$205 billion [110] presents a huge amount for less than one-fifth of the investment in power sector in the region requiring steady investment condition and effective coordination among the various actors involved [110]. Unfortunately, most developing nations have very low GDPs (Figure 5 [28]). Although, Africa's economic performance held firm in 2015 however, with Africa's economic performance holding firm in 2015 despite the worldwide economic downturn, with GDP growth to 3.6% compared with the 3.1% global economy and 1.5% for the eurozone. In 2015, sub-Saharan Africa (excluding South Africa) grew faster than the continental average of 4.2%, with East Africa leading the way at 6.3%. Growth in Central, North and West Africa was estimated at above 3%, while Southern Africa grew by an average of 2.2%. Average growth in Africa is forecasted to remain moderate at 3.7% in 2016 but could likely accelerate to 4.5% in 2017. This forecast however, depends on the strength of the world economy and a gradual recovery in commodity prices [110]. Although, in emerging and developing Asia, the growth declined from 6.8% to 6.5% in 2015 and 2014, respectively [110]. India is expected to remain largely sheltered from the economic meltdown plaguing the region and the world at large. They will benefit from lower commodity prices due to low oil prices and with ambitious policy and regulatory policies, India's energy sector will receive a boost in the very near-term [108]. Steps identified in [45] as viable means of SG deployment in developing nations include understanding the need for SG, Governmental support and heavy investments.

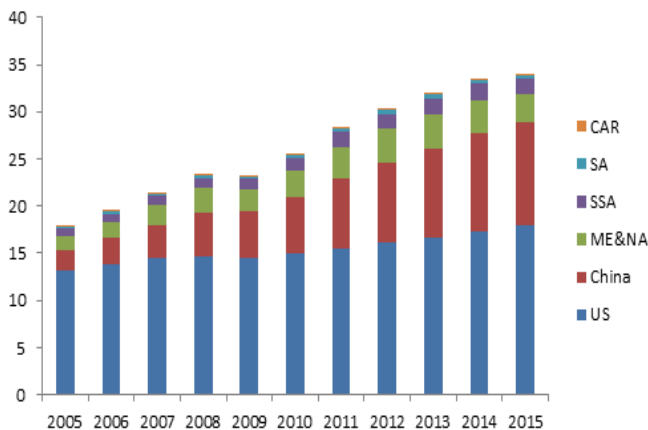


Figure 5. Gross Domestic Product in Trillion dollars

11. CONCLUSION

SGs deployments in developing nations face some factors militating against them. These factors identified as either technical or non-technical were discussed. Due to the high investment required compared to these nations' budgetary allocations, it is crucial that these deployment challenges be assessed, and priorities must be given to the improvement of critical infrastructure which all depend

on sustainable power supply system. Therefore, security issues must be well researched and tackled to allow for accelerated growth in power infrastructure and hence, in SG deployments. Drawing a reasonable time frame and making its policies implementable will be very critical in this regard. Also, developing nations must emulate countries like United States, United Kingdom, China, Russia, Malaysia, Japan, South Africa and a host of other countries spending in research sponsorship and implementations of the resulting output. Political instabilities and terrorism, as well as corruption, must be tackled with an utmost commitment by Government at all levels. Further works may consider the peculiarities of these factors to individual countries as some are practically more affected than the other.

ACKNOWLEDGMENT

The Authors wish to acknowledge the support of University of Ilorin, Ilorin, Nigeria, Universiti Teknologi Malaysia, Johor Bahru, Proudly Anebira and Alh. Hamza Usman (The Talba of Ebrialnd).

REFERENCES

- [1] Onyeji, I., M. Bazilian, and P. Nussbaumer, Contextualizing electricity access in sub-Saharan Africa. *Energy for Sustainable Development*, 2012. 16(4): p. 520-527.
- [2] Bhattacharyya, S.C., Energy access programmes and sustainable development: A critical review and analysis. *Energy for sustainable development*, 2012. 16(3): p. 260-271.
- [3] Salisu, S., et al., Techno-Economic Feasibility Analysis of an Off-Grid Hybrid Energy System for Rural Electrification in Nigeria. *International Journal of Renewable Energy Research (IJRER)*, 2019. 9(1): p. 261-270.
- [4] Wei, D., et al., Protecting smart grid automation systems against cyberattacks. *IEEE Transactions on Smart Grid*, 2011. 2(4): p. 782-795.
- [5] Li, Q. and G. Cao, Multicast authentication in the smart grid with one-time signature. *IEEE Transactions on Smart Grid*, 2011. 2(4): p. 686-696.
- [6] Siano, P., Demand response and smart grids—A survey. *Renewable and sustainable energy reviews*, 2014. 30: p. 461-478.
- [7] Delgado-Gomes, V., et al. Smart grid security issues. in 2015 9th International Conference on Compatibility and Power Electronics (CPE). 2015. IEEE.
- [8] Ofonyelu, C.C. and R. Eguabor, Metered and Unmetered Billing: How Asymmetric are the Phn Bills? *Journal of Social Economics Research*, 2014. 1(5): p. 97-107.
- [9] Arimoro, T., A. Oyetunji, and O. Odugboye, Analysis of Electricity Billing System in Corporate Buildings in Lagos, Nigeria. *Studies*, 2019. 1(6): p. 10-20.
- [10] Kessides, I.N., Chaos in power: Pakistan's electricity crisis. *Energy policy*, 2013. 55: p. 271-285.
- [11] Rahman, M., et al., A multi-agent approach for enhancing transient stability of smart grids.

- International Journal of Electrical Power & Energy Systems, 2015. 67: p. 488-500.
- [12] Otuoze, A.O. Transforming Nigeria's Electricity System To Meeting Future Demand Aimed At Reducing Greenhouse Gas Emissions Through An Effective Smart Grid Interoperability. in Proceedings of the OAU Faculty of Technology Conference, Ile-Ife, Nigeria (OAUtekConf 2012). 2012. Faculty of Technology, OAU, Ile-Ife, Nigeria.
- [13] Eissa, M., Protection techniques with renewable resources and smart grids—A survey. *Renewable and Sustainable Energy Reviews*, 2015. 52: p. 1645-1667.
- [14] Sen, R. and S.C. Bhattacharyya, Off-grid electricity generation with renewable energy technologies in India: An application of HOMER. *Renewable Energy*, 2014. 62: p. 388-398.
- [15] Kemausuor, F., et al., A review of trends, policies and plans for increasing energy access in Ghana. *Renewable and sustainable energy reviews*, 2011. 15(9): p. 5143-5154.
- [16] Yadoo, A. and H. Cruickshank, The role for low carbon electrification technologies in poverty reduction and climate change strategies: A focus on renewable energy mini-grids with case studies in Nepal, Peru and Kenya. *Energy Policy*, 2012. 42: p. 591-602.
- [17] Doll, C.N. and S. Pachauri, Estimating rural populations without access to electricity in developing countries through night-time light satellite imagery. *Energy Policy*, 2010. 38(10): p. 5661-5670.
- [18] Dagnachew, A.G., et al., Trade-offs and synergies between universal electricity access and climate change mitigation in Sub-Saharan Africa. *Energy Policy*, 2018. 114: p. 355-366.
- [19] Roy, A. and S. Bandyopadhyay, Introduction to Isolated Energy Systems, in *Wind Power Based Isolated Energy Systems*. 2019, Springer. p. 1-15.
- [20] Amin, S.B. and S. Rahman, *Energy, Employment and Poverty: The Bangladesh Experience*, in *Energy Resources in Bangladesh*. 2019, Springer. p. 107-111.
- [21] Pérez-Arriaga, I.J., et al., A utility approach to accelerate universal electricity access in less developed countries: A regulatory proposal. *ECONOMICS OF ENERGY & ENVIRONMENTAL POLICY*, 2019. 8(1): p. 33-50.
- [22] Oseni, M.O., Improving households' access to electricity and energy consumption pattern in Nigeria: Renewable energy alternative. *Renewable and Sustainable Energy Reviews*, 2012. 16(6): p. 3967-3974.
- [23] Gungor, V.C., et al., Smart grid technologies: Communication technologies and standards. *IEEE transactions on Industrial informatics*, 2011. 7(4): p. 529-539.
- [24] Cherp, A. and J. Jewell, The concept of energy security: Beyond the four As. *Energy Policy*, 2014. 75: p. 415-421.
- [25] Colak, I., et al., Smart grid projects in Europe: Current status, maturity and future scenarios. *Applied Energy*, 2015. 152: p. 58-70.
- [26] Shuaib, K., et al., Resiliency of Smart Power Meters to Common Security Attacks. *Procedia Computer Science*, 2015. 52: p. 145-152.
- [27] Kezunovic, M., Smart fault location for smart grids. *IEEE transactions on smart grid*, 2011. 2(1): p. 11-22.
- [28] Bigerna, S., C.A. Bollino, and S. Micheli, Socio-economic acceptability for smart grid development—a comprehensive review. *Journal of Cleaner Production*, 2016.
- [29] Fadaeenejad, M., et al., The present and future of smart power grid in developing countries. *Renewable and Sustainable Energy Reviews*, 2014. 29: p. 828-834.
- [30] 2016 Top Markets Report Smart Grid: A Market Assessment Tool for U.S. Exporters. April 2016: p. Accessed September 17th, 2016 via http://trade.gov/topmarkets/pdf/Smart_Grid_Top_Markets_Report.pdf.
- [31] Fan, X. and G. Gong, Security challenges in smart-grid metering and control systems. *Technology Innovation Management Review*, 2013. 3(7): p. 42.
- [32] Luthra, S., et al., Adoption of smart grid technologies: An analysis of interactions among barriers. *Renewable and Sustainable Energy Reviews*, 2014. 33: p. 554-565.
- [33] Amin, M., *Smart Grid*. PUBLIC UTILITIES FORTNIGHTLY, 2015.
- [34] Khurana, H., et al., Smart-grid security issues. *IEEE Security & Privacy*, 2010. 8(1).
- [35] Otuoze, A., et al., A Review of Smart Grids Deployment Issues in Developing Countries. *Arid Zone Journal of Engineering, Technology and Environment*, 2017. 13(6): p. 858-867.
- [36] Hawk, C. and A. Kaushiva, Cybersecurity and the smarter grid. *The Electricity Journal*, 2014. 27(8): p. 84-95.
- [37] Sultana, B., et al., Review on reliability improvement and power loss reduction in distribution system via network reconfiguration. *Renewable and sustainable energy reviews*, 2016. 66: p. 297-310.
- [38] Sridhar, S., A. Hahn, and M. Govindarasu, Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, 2012. 100(1): p. 210-224.
- [39] Verbong, G.P., S. Beemsterboer, and F. Sengers, Smart grids or smart users? Involving users in developing a low carbon electricity economy. *Energy Policy*, 2013. 52: p. 117-125.
- [40] Chakraborty, A.K. and N. Shaniia, Advanced metering infrastructure: Technology and challenges. in 2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). 2016. IEEE.
- [41] Sanjab, A., et al., Smart grid security: Threats, challenges, and solutions. *arXiv preprint arXiv:1606.06992*, 2016.
- [42] Khanna, N.Z., J. Guo, and X. Zheng, Effects of demand side management on Chinese household electricity consumption: Empirical findings from Chinese household survey. *Energy Policy*, 2016. 95: p. 113-125.

- [43] Sharma, T., et al., Of pilferers and poachers: Combating electricity theft in India. *Energy Research & Social Science*, 2016. 11: p. 40-52.
- [44] Kumar, V.A., K.K. Pandey, and D.K. Punia, Cyber security threats in the power sector: Need for a domain specific regulatory framework in India. *Energy Policy*, 2014. 65: p. 126-133.
- [45] Fadaeenejad, M., et al., The present and future of smart power grid in developing countries. *Renewable and Sustainable Energy Reviews*, 2014. 29: p. 828-834.
- [46] Kate, P.G. and J.R. Rana. ZIGBEE based monitoring theft detection and automatic electricity meter reading. in 2015 International Conference on Energy Systems and Applications. 2015. IEEE.
- [47] Otuoze, A.O., M.W. Mustafa, and R.M. Larik, Smart grids security challenges: classification by sources of threats. *Journal of Electrical Systems and Information Technology*, 2018.
- [48] Saputro, N., K. Akkaya, and S. Uludag, A survey of routing protocols for smart grid communications. *Computer Networks*, 2012. 56(11): p. 2742-2771.
- [49] Tuballa, M.L. and M.L. Abundo, A review of the development of Smart Grid technologies. *Renewable and Sustainable Energy Reviews*, 2016. 59: p. 710-725.
- [50] Salisu, S., M. Mustafa, and M. Mustapha. Predicting Global Solar Radiation in Nigeria Using Adaptive Neuro-Fuzzy Approach. in International Conference of Reliable Information and Communication Technology. 2017. Springer.
- [51] Giani, A., et al. Metrics for assessment of smart grid data integrity attacks. in 2012 IEEE Power and Energy Society General Meeting. 2012. IEEE.
- [52] Amin, S.M. Smart grid security, privacy, and resilient architectures: Opportunities and challenges. in 2012 IEEE Power and Energy Society General Meeting. 2012. IEEE.
- [53] Gharavi, H. and B. Hu. Dynamic key refreshment for smart grid mesh network security. in Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES. 2013. IEEE.
- [54] Giani, A., et al., Smart grid data integrity attacks. *IEEE Transactions on Smart Grid*, 2013. 4(3): p. 1244-1253.
- [55] Li, H., et al., An efficient merkle-tree-based authentication scheme for smart grid. *IEEE Systems Journal*, 2014. 8(2): p. 655-663.
- [56] Gaur, V. and E. Gupta, The determinants of electricity theft: An empirical analysis of Indian states. *Energy Policy*, 2016. 93: p. 127-136.
- [57] World Bank Open Data. p. Accessed via <http://data.worldbank.org> on 27th August 2019.
- [58] Mo, Y., et al., Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 2012. 100(1): p. 195-209.
- [59] Nakada, T., K. Shin, and S. Managi, The effect of demand response on purchase intention of distributed generation: Evidence from Japan. *Energy Policy*, 2016. 94: p. 307-316.
- [60] Mohammed, O., et al., Virtual synchronous generator: an overview. *Nigerian Journal of Technology*, 2019. 38(1): p. 153-164.
- [61] Boyle, G., Renewable energy. *Renewable Energy*, by Edited by Godfrey Boyle, pp. 456. Oxford University Press, May 2004. ISBN-10: 0199261784. ISBN-13: 9780199261789, 2004: p. 456.
- [62] Akorede, M.F., H. Hizam, and E. Pouresmaeil, Distributed energy resources and benefits to the environment. *Renewable and sustainable energy reviews*, 2010. 14(2): p. 724-734.
- [63] Mohammad, N., A. Barua, and M.A. Arafat. A smart prepaid energy metering system to control electricity theft. in International Conference on Power, Energy and Control (ICPEC), 2013. 562-565. 2013. IEEE.
- [64] Mohammad, N., A. Barua, and M.A. Arafat. A smart prepaid energy metering system to control electricity theft. in Power, Energy and Control (ICPEC), 2013 International Conference on. 2013. IEEE.
- [65] Krishna, V.B., et al. F-DETA: A framework for detecting electricity theft attacks in smart grids. in Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference on. 2016. IEEE.
- [66] Jamil, F. and E. Ahmad, An empirical study of electricity theft from electricity distribution companies in Pakistan. *Pakistan Development Review*, 2014. 53(3): p. 239.
- [67] Nikovski, D.N., et al. Smart meter data analysis for power theft detection. in International Workshop on Machine Learning and Data Mining in Pattern Recognition. 2013. Springer.
- [68] Jiang, R., et al., Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology*, 2014. 19(2): p. 105-120.
- [69] Jindal, A., et al., Decision tree and SVM-based data analytics for theft detection in smart grid. *IEEE Transactions on Industrial Informatics*, 2016. 12(3): p. 1005-1016.
- [70] Musungwini, S., A framework for monitoring electricity theft in Zimbabwe using mobile technologies. *Journal of Systems Integration*, 2016. 7(3): p. 54.
- [71] Yakubu, O., N. Babu, and O. Adjei, Electricity theft: Analysis of the underlying contributory factors in Ghana. *Energy Policy*, 2018. 123: p. 611-618.
- [72] Razavi, R., et al., A practical feature-engineering framework for electricity theft detection in smart grids. *Applied Energy*, 2019. 238: p. 481-494.
- [73] Ahmad, T., et al., Review of various modeling techniques for the detection of electricity theft in smart grid environment. *Renewable and Sustainable Energy Reviews*, 2018. 82: p. 2916-2933.
- [74] Yip, S.-C., et al. Detection of Energy Theft and Metering Defects in Advanced Metering Infrastructure Using Analytics. in 2018 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE). 2018. IEEE.
- [75] Govinda, K., R. Shav, and S. Prakash, Energy Theft Identification in Smart Grid, in *Silicon Photonics & High Performance Computing*. 2018, Springer. p. 9-15.

- [76] Ahmad, T., Non-technical loss analysis and prevention using smart meters. *Renewable and Sustainable Energy Reviews*, 2017. 72: p. 573-589.
- [77] Geelen, D., A. Reinders, and D. Keyson, Empowering the end-user in smart grids: Recommendations for the design of products and services. *Energy Policy*, 2013. 61: p. 151-161.
- [78] Derakhshan, G., H.A. Shayanfar, and A. Kazemi, The optimization of demand response programs in smart grids. *Energy Policy*, 2016. 94: p. 295-306.
- [79] Otuoze, A.O., et al., Electricity theft detection framework based on universal prediction algorithm. *Indonesian Journal of Electrical Engineering and Computer Science*, 2019. 15(2): p. 758-768.
- [80] Pina, A., C. Silva, and P. Ferrão, The impact of demand side management strategies in the penetration of renewable electricity. *Energy*, 2012. 41(1): p. 128-137.
- [81] Aghaei, J. and M.-I. Alizadeh, Demand response in smart electricity grids equipped with renewable energy sources: A review. *Renewable and Sustainable Energy Reviews*, 2013. 18: p. 64-72.
- [82] O'Malley, L., The Evolving Digital Utility: The convergence of energy and IT. p. Accessed September 16 via <https://www.marsdd.com/news-and-insights/the-evolving-digital-utility/>.
- [83] Depuru, S.S.S.R., L. Wang, and V. Devabhaktuni. A conceptual design using harmonics to reduce pilfering of electricity. in *IEEE PES General Meeting*. 2010. IEEE.
- [84] Nizar, A. and Z. Dong. Identification and detection of electricity customer behaviour irregularities. in *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES. 2009. IEEE*.
- [85] Moslehi, K. and R. Kumar, A Reliability Perspective of the Smart Grid. *IEEE Trans. Smart Grid*, 2010. 1(1): p. 57-64.
- [86] Surajudeen-Bakinde, N.T., et al. Development of an Internet based prepaid energy meter. in *AFRICON, 2017 IEEE. 2017. IEEE*.
- [87] Khan, A.R., et al., Load forecasting, dynamic pricing and DSM in smart grid: a review. *Renewable and Sustainable Energy Reviews*, 2016. 54: p. 1311-1322.
- [88] Patel, C. and N. Doshi, Security Challenges in IoT Cyber World, in *Security in Smart Cities: Models, Applications, and Challenges*. 2019, Springer. p. 171-191.
- [89] Zhang, S., T. Zheng, and B. Wang, A privacy protection scheme for smart meter that can verify terminal's trustworthiness. *International Journal of Electrical Power & Energy Systems*, 2019. 108: p. 117-124.
- [90] Oseni, M.O. and M.G. Pollitt, The promotion of regional integration of electricity markets: Lessons for developing countries. *Energy Policy*, 2016. 88: p. 628-638.
- [91] Yuan, Y., Z. Li, and K. Ren, Modeling load redistribution attacks in power systems. *IEEE Transactions on Smart Grid*, 2011. 2(2): p. 382-390.
- [92] Kisel, E., et al., Concept for Energy Security Matrix. *Energy Policy*, 2016. 95: p. 1-9.
- [93] Wang, W. and Z. Lu, Cyber security in the smart grid: Survey and challenges. *Computer networks*, 2013. 57(5): p. 1344-1371.
- [94] Stefanov, A. and C.-C. Liu, Cyber-physical system security and impact analysis. *IFAC Proceedings Volumes*, 2014. 47(3): p. 11238-11243.
- [95] Wang, X. and P. Yi, Security framework for wireless communications in smart distribution grid. *IEEE Transactions on Smart Grid*, 2011. 2(4): p. 809-818.
- [96] Onyeji, I., M. Bazilian, and C. Bronk, Cyber security and critical energy infrastructure. *The Electricity Journal*, 2014. 27(2): p. 52-60.
- [97] Klare, M., *Resource wars: The new landscape of global conflict*. 2001: Metropolitan Books.
- [98] Russell, B.D. and C.L. Benner, Intelligent systems for improved reliability and failure diagnosis in distribution systems. *IEEE Transactions on Smart Grid*, 2010. 1(1): p. 48-56.
- [99] Lala, C. and B. Panda, Evaluating damage from cyber attacks: a model and analysis. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 2001. 31(4): p. 300-310.
- [100] Yampolskiy, M., et al., A language for describing attacks on cyber-physical systems. *International Journal of Critical Infrastructure Protection*, 2015. 8: p. 40-52.
- [101] Africa, Q., Cybercrime is costing Africa's businesses billions. 2018: p. Accessed via <https://qz.com/africa/1303532/cybercrime-costs-businesses-in-kenya-south-africa-nigeria-billions/> on 5th February 2019.
- [102] Gobena, Y., et al. Practical architecture considerations for Smart Grid WAN network. in *Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES. 2011. IEEE*.
- [103] Kreutz, D., et al., A cyber-resilient architecture for critical security services. *Journal of Network and Computer Applications*, 2016. 63: p. 173-189.
- [104] Genge, B., I. Kiss, and P. Haller, A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, 2015. 10: p. 3-17.
- [105] Abadie, A. and J. Gardeazabal, Terrorism and the world economy. *European Economic Review*, 2008. 52(1): p. 1-27.
- [106] Sandler, T. and W. Enders, Economic consequences of terrorism in developed and developing countries. *Terrorism, economic development, and political openness*, 2008. 17.
- [107] Chibuike, U.C. and O.I. Eme, Terrorism & its Socio-Economic Effects in Nigeria. *Journal of Contemporary Research in Social Sciences*, 2019. 1(1): p. 97-113.
- [108] 2016 Top Markets Report Smart Grid: A Market Assessment Tool for U.S. Exporters. , 2016: p. Accessed via http://trade.gov/topmarkets/pdf/Smart_Grid_Top_Markets_Report.pdf, September 17th 2016.
- [109] Feldpausch-Parker, A.M., et al., Smart grid electricity system planning and climate disruptions: A review of climate and energy discourse post-

- Superstorm Sandy. *Renewable and Sustainable Energy Reviews*, 2018. 82: p. 1961-1968.
- [110] Nierop, S.C., *Envisioning resilient electrical infrastructure: A policy framework for incorporating future climate change into electricity sector planning*. *Environmental Science & Policy*, 2014. 40: p. 78-84.
- [111] Keho, Y., *What drives energy consumption in developing countries? The experience of selected African countries*. *Energy Policy*, 2016. 91: p. 233-246.
- [112] Asif, M. and T. Muneer, *Energy supply, its demand and security issues for developed and emerging economies*. *Renewable and Sustainable Energy Reviews*, 2007. 11(7): p. 1388-1413.
- [113] Rose-Ackerman, S. and B.J. Palifka, *Corruption and government: Causes, consequences, and reform*. 2016: Cambridge university press.
- [114] Gonzalez, M., *Smart Grid Investment Grows with Widespread Smart Meter Installations*. p. Accessed via http://vitalsigns.worldwatch.org/sites/default/files/vital_signs_smart_grid_final_pdf.pdf on September 16 2016.