RESEARCH ARTICLE

A Comparative Analysis of Cyber Security Laws and Policies in Nigeria and South Africa

Ngboawaji Daniel Nte[1]✉, Brebina Kelvin Enoke[2], Vigo Augustine Teru[3]

[1] Department of Intelligence and Security Studies Novena University Ogume, Delta State, NIGERIA

[2] Faculty of Law, Niger Delta University, Wilberforce Island, Amasoma, Bayelsa State, NIGERIA

[3] School of Postgraduate Studies, Department of Intelligence and Security Studies, Novena University Ogume, Delta State, NIGERIA

✉ profdnte@novenauniversity.edu.ng

Citation:
Nte, N. D., Enoke, B. K., & Teru, V. A. (2022). A Comparative Analysis of Cyber Security Laws and Policies in Nigeria and South Africa. *Law Research Review Quarterly, 8*(2), 233-258. https://doi.org/10.15294/lrrq.v8i2.56486

Submitted : January 20, 2022
Revised : March 11, 2022
Accepted : April 8, 2022
Online since: May 31, 2022

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract

There is free flow of information in the cyberspace and as a result, nations are obviously wary of the integrity of its data as part of both public safety and national security concerns. There are ways that the associated risk could be mitigated and mostly has to do with a proper development and implementation of Cyber security policies and strategies. This research focuses on the cyber security policies, strategies and laws of both Nigeria and South Africa and also making a comparative analysis of the current National Cyber Security Policy and Strategy of both countries and the necessary recommendations going forward. In the case of Nigeria, analytical evidence shows that the national documents were found to have satisfied most of the requirements in terms of content but failed to address other aspects of cyber security concerns in the country. On the other hand, South Africa as a country is lagging especially in governmental coordination, cybersecurity legislation, engagement with business and citizens, and skilled labour. The paper tends to explore these loopholes evident in the cyber security laws and policies of the aforesaid countries and made the necessary recommendations on how to adopt best and sustainable practices in dealing with issues related

to cyber security breaches including cybercrime in both countries.

Keywords: *Cybersecurity, Laws, Policy, Nigeria, South Africa*

1. INTRODUCTION

Infractions on the web including cybercrime can be viewed as part and parcel of the information security threat over the internet or cyberspace. Throughout the 21st Century, the world as it were, has transformed into what is now known as a digital world because of the advancements in research and development in the area of information communication technology, which globally has been accepted. Globally, different countries have designed coordinated national cyber security and cybercrime policies to ensure some level of national security confidence and elimination of cyber threats. It is generally agreed that countries recognise and organise cyber threats according to national prioritisation and range in ways that each country perceives the threats. The only exception to this analysis is Russia that has remained highly nebulous in the organisation of its national cyber security policy.

The challenges of security issues in the global cyber space is believed to emanate from technical primer and graduates into strategic dimension. It is also pertinent to create a national consciousness about the obvious need for the collective relevance of cyber security. This is because, while there are some tangible and evidential aspects of information communication technology (ICT) exists for all to see, others are not easily seen. In the midst of these the fact still remains that that postmodern world is built on ICT and the associated fall outs of the technological world. Today, about 58% of the world's population are online and the mobile –cellular subscription is about 8 billion which is almost the entire world population, and these figures are annually increasing. Unfortunately, most of these users, especially new users are not well aware of the risks involved

and the crimes being perpetrated, not to mention of how to safely use the systems with the basic security precautions in mind. (Kenneth, 2011, ITU: 2020).

Certain key assumptions are taken for granted when postulating on the general aims of cybersecurity functions in nations states. These assumptions are prevalent in all countries both developed and developing in a greatly networked world. Scholars have identified that the first aim is to provide a list of pre-determined, non-mandatory cybersecurity functions from which developed and developing countries may make a selection, for implementation. This means that countries that have not yet developed their own authoritative and normative sources, or experience skills and fiscal constraints, do not need to apply level 1 of the NCMF, but can select one or two of the predetermined, non-mandatory functions. Level 1 is applied, when following this approach, by a third party, to identify non-mandatory cybersecurity functions on behalf of the nation-state. Level 1 is thus still used, but applied by a third party, and not by the nation-state using the National Cybersecurity Mandatory Functions- NCMF (Jacobs, 2018).

In the same vein, the second aim is for nation states identifying their own national cybersecurity functions, to use this predetermined list of non-mandatory cybersecurity functions against which to measure the strategic relevance and completeness of their own identified national cybersecurity functions. The non-mandatory cybersecurity functions are all strategic in nature, (as opposed to tactical or operational), and, as such, provide a predetermined list of functions that are general in nature, against which to measure the strategic relevance and completeness of their mandatory national cybersecurity functions (Jacobs, 2018). It is further advantageous to have the general cybersecurity functions to use as a baseline, or foundation, against which to measure the completeness and relevance of a nation's identified national cybersecurity functions. Being able to measure the national cybersecurity functions against an

existing baseline is useful in that it ensures alignment with the international community and its cybersecurity efforts. The general quest for a grand strategy for a sustainable cybersecurity laws and strategy has pushed countries to draw defined laws and policies to guide them in national security template to protect the cyber space and public safety of the entire citizenry. Consequently, the table below shows a summary of cyber security policies of some selected counties in tandem with their national security policies as shown on Table 1.

TABLE 1. A Summary of National Cyber Security Policies of Some Countries

Country	Threat topology	Main measures	Vision	Principles/ policies
Australia	Terrorist, criminals, espionage.	Response, detection, awareness, partnership and regulation.	Secure, resilience and trusted electronic environment	National leadership, Shared responsibility, partnership, risk management, protection of Australian values.
Canada	States (military and espionage) Cybercriminals Terrorist groups.	Partnership, empowerment.	Making Cyberspace more secure for all Canadians.	Not Explicit.
Estonia	Focus on effects of threat actors.	Cooperation, education, regulations and change of character.	Reduce inherent vulnerability of cyberspace in Estonia.	Cyber security integrated in NSS, effort of all stakeholders, protection of human right; personal data and identity.
Finland	No typology available.	Collaboration, awareness, detection and legislation.	Secure vital functions, safe cyber domain, Global Forerunner in cyber security	Responsibility, collaboration, R&D, legislation.
Germany	Terrorism, crime and war; natural hazards and technical failure or human error.	Cooperation, coordination.	Substantial contribution to secure cyberspace.	All stakeholders act as partners, enforcing; rule of conduct standards and norms.
Netherland	States Private organizations	Partnership, threat and risk mitigation.	Security and confidence in an	Existing initiative linking and

Country	Threat topology	Main measures	Vision	Principles/ policies
	Professional criminals Terrorists Hacktivists Script kiddies Cyber- researchers Internal actors Non-actor.		open and free digital society.	reinforcement, clear responsibilities and partnership, legislation, national and human right.
S/ Africa	Implicit.	Legislation, partnership.	Ensuring confidence and trust in secure use of ICT.	Implicit.
UK	Criminals Nation-states Patriotic hackers Terrorist groups Hacktivists.	Risk base respond, Cooperative approach.	Vibrant, resilience and secure cyberspace.	Risk based approach, balancing security privacy and freedom, partnership.
US	Criminal hackers Organized criminal Groups Terrorist networks Advanced nation.	Diplomacy, defence and development.	Engage and empower American to secure their portion of cyberspace.	Protecting privacy and civil liberty.
EU	None publicly Available.	Partnership.	Resilience, reduce cybercrime, develop industrial and tech. resource, common defence policy.	Protecting fundamental rights, freedom of expression, personal data and privacy, shared responsibility, access for all.

The massive and apparent irreversible digitalization has left the world heavily reliant on information communication technology via a define networks. This is obvious from the several aspects of human civilization ranging from banking and commerce, education, businesses and so on. Everything is now online which has spread like a wildfire even to the most remote part of the earth of which Nigeria and South Africa are not left out. Both countries have a considerable number of information technology firms, and it keeps growing by the day. However, with these establishments comes several downsides. Criminals now

take advantage of this technology flame to perpetrate crime and steal information, and so therefore, this paper will focus on the strategies and policies adopted by both Nigeria and South Africa to curb against this type of crime.

Odumesi (2014) define Cybercrime as "*a crime that has to do with the abuse of digital resources in a cyberspace or via the internet or network networks, wither through wired or wireless communication.*" Crimes generally can be mitigated via physical measures which involves the use of *investigation*, *detection, apprehension,* and *prosecution*, by adopting means that involves the use of certain techniques that could help in addressing these crimes. However, when these crimes become digitalized, it becomes more difficult to address. Digitalized crimes have proved to be a challenge for law enforcement agencies because it is more difficult to detect, and traditional methods of solving crimes have proved to be useless because of the digitalization of these crimes.

Both Nigeria and South Africa have a massive cyber space presence and as a result have recorded a large share of cybercrime bridges. Nigeria for example is known for being a dwelling place computer related criminal activity which is also known as *419* or *yahoo-yahoo* and so many other cyber related crimes that has undermine its national security. No wonder anywhere you travel in this world, as long as you are a Nigeria, foreigners are always sceptical when it comes to dealing with you. Cyber security is now considered among the priority list for the federal government of Nigeria and that is why it is now directly handled by the Presidency via the Office of the National Security Adviser (ONSA). In 2015 the office of the National security Adviser (ONSA) drafted a National Cyber Security Policy and Strategy of which details of it will be discuss in this article.

The popular maxim that security is not a one man's business is validly true and that explains why the Nigerian Government has continued to look for the support and contributions of various stakeholders across different sectors to come together and work hand in glove towards

achieving a well secured National cyber security space. In South Africa, cyber security has been identified as an important component or aspect of its national security. This is so because we see more and geographical regions of South Africa being fully integrated into the global digital village, and this has necessitated the introduction of some governmental initiatives geared towards bridging the digital gap between sectors and addressing issues of cyber security.

This paper therefore performs a comparative analysis of the Nigerian and South African Cyber Security Policies and Strategies, it also seeks to explore better options in terms of functionality and applicability of the National Cyber Security Policies of both countries in relation to their environments.

The Problem Statement

Africa has for some time now been battling with cyber threats such as *ransomware*, *child pornography, phishing*, *malware*, *and abuse*, *denial of service*, and so on. According to BitSight (2016) report, Africa was worst hit by ransomware with two out of twenty institutions battling with ransomware on their network.

Grajek (2018) EDUCAUSE also shows that we have not really made much progress in the area of cyber security as it has been one of the top problem organizations are trying to contain in recent times. Statistics shows that so many institutions in both Nigeria and South African today, have embraced information technology without sitting down to ensure they have what it takes to maintain and sustain it thus ensuring the integrity of data within the system.

According to the National Data Protection Regulation in both countries, it mandates that any organization charged with personal information of individuals must secure such from security breaches such as *cyberattacks*, etc. Unfortunately, both Nigeria and South Africa do not have a coordinated approach to dealing with cybersecurity. Agreed

different structures have been established to handle issues related to cybersecurity, however, these structures are not enough to deal with cyber security issues. Black hat Hackers and are thriving on their systems and demanding for a ransom. Nigeria and South Africa must come to reality of the cyber threats they face considering the volume of data with both systems. This Paper will review and compare the policies and strategies adopted in Both Countries and Make recommendation on how to approach things going forward.

Review of Related Literature

The Office of the Nigerian National Security Adviser define Cyber security Strategy as the Preparedness of Nigeria to provide a united measures and national strategies towards assuring to an extent the security and protection of the nation's presence in the cyber spectrum.

It is important to note that the issue of cyber security should be given topmost priority because of how the world has transformed, and as such, intelligent consumers, policy makers and both government and non-governmental agencies and other stakeholders should craft out guiding principles in the form of policies and strategies so that anything related to cyber security should be well governed. Recently, so many data breaches have been recorded as revealed in the 2017, 2018 and 2019 Verizon data breach report and Privacy Rights Clearinghouse. The report focuses on isolating and analysing global Cybersecurity incidents and breaches in eight different sector which provides an excellent understanding to data and security bridges.

In Africa for example, record has it that we have recorded quiet a number of bridges. In fact according to the Verizon report, between 2017 and 2019, about one thousand one hundred and twenty-nine incidents across three hundred and eighty-two institutions and so many other instances which has led to the leakage of personal information all over the cyber space. The top among the incidents according to the report includes of unknown

category, attack from external sources, and few other of undisclosed cases. The loophole exploited by the hackers, could be as a result of either human or technological weaknesses or the combination of both.

In Nigeria for example, cybercrime has been flourishing for quiet sometime now and this is obvious from the fact that we have so many internet fraudsters popularly known as yahoo boys and also from students (Okeshola and Adeta 2013). Academic fraud, denial of service, phishing attacks, identity theft and financial crimes are some among the type of cybercrime activities experience from within the Country (Sawahel 2017). In South Africa, majority of cybercrime attacks happens in two areas. The first one is targeted towards the institutions' information assets both from within and other external forces, while the second aspect comes from the community members attacking other businesses and individuals.

Regarding African cyber security, Serianu (2016) pointed out that threats from within are the greatest threats to organizations in Africa when compared to external threats. In fact, The Nation (2019) reported an instance of an IT staff of a private university who defrauded the institution of about One Hundred and Eighty Million Naira (₦180, 000,000) using cyber means to channel the amount into his pocket. Sometimes in November 2016, the website of the Federal University of Technology Akure, Ondo State (FUTA) was hijacked by a foreign group from Indonesia (Ajah 2016). Although the University was able to recover from the attack, the motive behind that attack still remains a mystery. The University of Nigeria Nsukka, Enugu State (UNN) also experience an attack on their website recently as reported by Ikeji in 2019. The Joint Admission and Matriculation Board (JAMB) database was also attacked in 2017. Hackers were able to access the database and did some modifications in their records (Icirnigeria 2017, Olokor 2017).

The same agency was also hit in 2019 which forced the agency to re-conduct fresh exams (News Agency 2019). As mentioned by Borja (2006) there are records of students' intruding institutions networks to alter grades, steal or delete files.

According to Sawahel 2017, Africa lacks a proactive measure in the responding to cyber threats which is one of the reason for our failure. Muhammed Rudman for example in an interview with Serianu (2016), pointed out that he is aware of any technique or infrastructure in place by the Government of Nigeria to help especially private organizations to fight cybercrime. He also emphasized the fact that there is no legal framework and required skill to combat this type of crime in the country even though he acknowledged the existence of a National Cybersecurity Strategy and Policy documents.

Both Nigeria and South Africa agree to the fact that based on the reality of things, whatever Cyber policy or strategy they choose to adopt should have these components; Cybercrime, Cyber Terrorism, Cyber Espionage, Online Child Abuse and Exploitation, Hacktivism, National Cyber Security Strategy Lifecycle, Linear approach Strategies, Lifecycle approach and Hybrid Approach.

2. METHOD

The methodology employed for the primary research data is the qualitative research methodology. Quantitative research methodology utilizes a model where statistics are based on numerical data, while the qualitative research methodology uses non-numerical data. The analysis method involved a review of some similar works in the research field, which include but not limited to the review of the national cyber security policies and strategies for Nigeria and South Africa. A proper analysis and review of some selected national policy and strategy frameworks was done, after-which it was harmonized. The Nigerian national cyber

security strategy was reconciled in the light of the harmonized frameworks, and also extracting some similarities as a basis to appraise its competence. A comparative analysis of the Nigerian national cyber security policy and that of South Africa was performed thereafter.

3. RESULT AND DISCUSSION

A. Nigerian Cybersecurity Policies and Strategies

Internationally, within the framework of multilateral agreements, a lot of collaborative conventions and partnerships geared towards collective deterrence to cyber security threats exist and many more are ongoing at the moment. Accordingly, Nigeria has consistently been part of this global move to secure her cyber space. Consequently, the country has secured membership to the following organisations; the International Multilateral Partnership Against Cyber Threats (IMPACT), the Organization of Islamic Cooperation (OIC), the International Criminal Police Organization (INTERPOL) etc. In the same vein, concerted efforts have been made to join such cyber security related organisations like the Forum for Incident Response and Security Teams (FIRST), Global Prosecutors E-Crime Network (GPEN) amongst others. At the level of multilateral conventions and treaties, Nigeria has signed the Budapest convention on cybercrime to complement the numerous bilateral agreements between Nigeria and other countries to fashion out robust bilateral cyber security agreements and partnerships.

The Nigerian cybersecurity policies and strategies from the policy document focuses on eight (8) pillars as listed below:

1) Strengthening Cybersecurity Governance and Coordination
2) Fostering Protection of Critical National Information Infrastructure
3) Enhancing Cybersecurity incidence management
4) Strengthening legal and Regulatory framework

5) Enhancing Cyber defence capability
6) Promoting a thriving digital economy
7) Assuring monitoring and evaluation
8) Enhancing international cooperation

1. ***Strengthning Cybersecurity Governance and Coordination***

The office of the National Security Advisor (NSA) is mandated to establish a National Cybersecurity Coordination Centre (NCCC). This serving as the central body that will interact with major stakeholders to ensure a well secured cyber ecosystem in Nigeria. The NCCC is responsible for mapping out the responsibility of each stakeholder as highlighted above. The stakeholders include both local and international partners as well as government agencies and the private business owners.

2. ***Fostering Protection of Critical National Information Infrastructure***

The critical infrastructures include certain information and communication systems which is obviously good for economic development, financial transactions, social interactions and so on. In fact, they underpin our national life and existence as a nation so any destruction to these systems will definitely affect government operations, economic prosperity and even undermine national security. Consequently, the government deemed it necessary to formulate policies and strategies to guide and protect these critical infrastructures. The following are among the policies and strategies adopted.

1) Critical Information Infrastructure Protection and Resilience (CIIPR): Here It mentioned that Nigeria will ensure a comprehensive approach through stakeholders' interactions in both public and private sectors. Adequate information will be must be shared to the community to create awareness and coordinate risk based decision making and also will continue to update the list of CIIPR that requires protection

priorities and make sure all stakeholders have these at their disposal.

2) Identity and evaluate Potential Critical National Information Infrastructure: Government will liaise with owners and operators of these critical infrastructure to take inventory of these assets and do a risk analysis in other to ascertain the level of protection required.
3) Redundancy Mechanism for essential services: Compulsory backup for each of the critical infrastructures must be in place in the event of any disaster and to avoid a single point of failure.
4) National Vulnerability Assessment (NVA): They shall periodically carry out a vulnerability assessment under the guidance of NCCC with a view to find out if there is any weakness in the system.

3. Enhancing Cybersecurity Incidence Management

Cybersecurity incidence management will be realized by strengthening the national cyber security incidence response team, mechanism and incident response plan.

4. Strengthening Legal and Regulatory Framework

For Example, when it comes to internet security and child online protection, any omission that is against a child that is not acceptable in the physical environment is also prohibited online. This is necessary as it will protect children from exposure to bad contents. Mechanism will also be developed to assist women with the capacity and at the same time creating opportunities within the cyber spectrum.

5. Enhancing Cyber Defence Capability

The Defence Space Administration that is responsible for providing an enabling cyber environment for the Nigerian military will work hand in glove with NCCC and other agencies alongside think thanks to implement the National Cyber Defence strategy. It shall continually liaise with these agencies to ensure periodic trainings and technical skill acquisitions for personnel.

6. ***Promoting a thriving Digital Economy***

Nigeria really wants to use cybersecurity to move the use of internet for commercial and other government related activities that will enhance a flourishing digital economy. In view of this, the following was adopted by the government;

1) Take the Lead in having a cybersecurity culture and behaviour, which can be achieved through training programs.
2) Best practises must be adhered to by all stakeholders especially when handling government functions.
3) Security is a collective business, and as such it becomes the duty of every community member to report any online crime through a dedicated platform that will be provided by the government.
4) Government will adopt a mechanism for virtual currency to ensure its progressive use, and at the same time highlight its use.

7. ***Assuring Monitoring and Evaluation (M&E)***

Substandard or counterfeit soft wares and hardwires will not be tolerated from either private or government agencies. Furthermore, Government shall also develop the needful for annual licensing and registration.

8. ***Enhancing International Cooperation***

Nigeria will work closely with other stakeholders in cyber policies, strategy formulation, cyber law enforcement, threat intelligence sharing and capacity development.

B. Nigerian Cybersecurity Laws

The Nigerian Cybercrime Act 2015 gives the President the power to designate critical information system assets which includes some computer systems, networks and other IT infrastructure and also to come up with certain guidelines and procedures for auditing to ensure that those define assets still remains critical.

1) The Nigerian Cybercrime Act 2015 prescribes a death penalty for any offense perpetrated against a system that has been designated as a critical asset.

2) Anybody found guilty of hacking unlawfully into a computer system or network are liable to a fine of up to ₦10 Million or 5 years imprisonment.
3) The cybercrime law prohibits identity theft with a penalty of 3 years imprisonment or a fine of not less than ₦7 Million or to both.
4) Cyber-Stalking and Cyber-Bullying will attract a fine of not less than ₦2 million or imprisonment for a term of not less than 1 year or to.
5) Cybersquatting which is registering and using an internet domain name with intention will attract a fine or N5 million or nothing less than 2 years or both.
6) Racist or xenophobic, violent threats and abusive statements that could incite racial or religious violence are prohibited. Perpetrators will be fined of not less that N10 million or a minimum or 5 years imprisonment or both.
7) Service providers must keep and maintain all traffic and subscriber information, respecting individual's rights to privacy.
8) For the purpose of criminal investigation, individual or suspects electronic communication can be intercepted after receiving a court order duly signed by a judge.

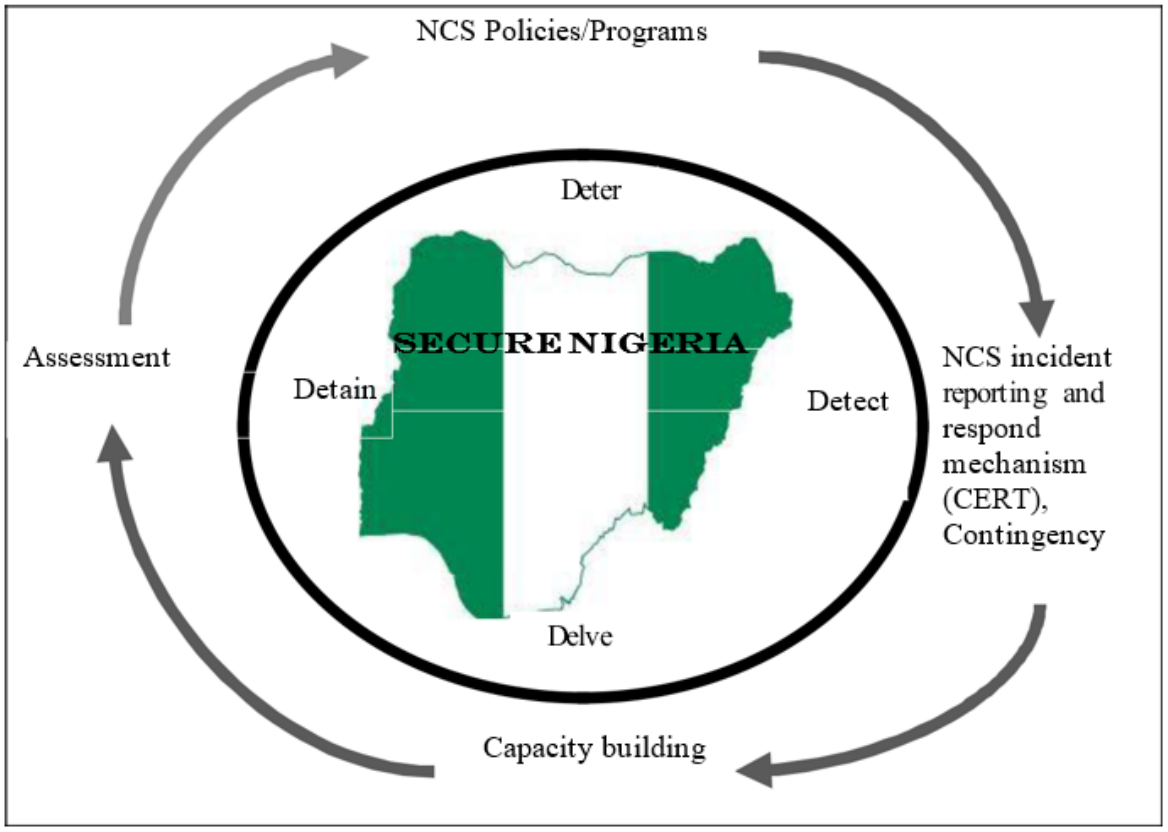

FIGURE 1 Nigeria's National Cybersecurity Policy

C. South African Cybersecurity Policies

The Cyber Security policy and strategy in South Africa is grouped into the following

1) Political will
2) Adapted organization Structures
3) Identifying accurate proactive and reactive measures
4) Reducing criminal opportunities
5) Education and awareness

1. Political will

This ensures national leadership both at individual and organizational level. The draft cyber security policy aims to ensure cooperation between the state organs in other to achieve the stated objective for achieving security of South Africa's information networks.

2. Adapted Organizational Structures

This proposes the presence of adequate national organizational structures that supports the implementation

of an effective cyber security solution for organizations, individuals, and governmental agencies. Having a national computer security incident response team (CSIRT) should be the desired organizational structure for harmonizing computer communication networks with economic and social development. Therefore, the development and establishment of a South African CSIRT is ongoing by the South African Department of Cybersecurity and other joint partners. The technicalities are clearly spelled out in the South African cyber security policy document.

3. Identifying Accurate Measures

It is imperative that cyber security should be machine driven in other to make the most of outputs and reduce human intervention which could lead to errors. Almost everyone in South Africa depends on data especially as it relates to digital infrastructures. Therefore, it is important that the decision taken regarding cyber security should be the right one. The full implementation of the South African cyber security policy should clearly identify functions and roles.

4. Reducing Criminal Opportunities

Cyber security cross with the execution of international legislation to reduce criminal opportunities. It is expected to raise the awareness of threat and vulnerabilities envisaged which could go a long way in reducing criminality in South Africa.

5. Education and Awareness

Continuous education on cyber security should be encouraged among experts in the fields of political, economic and legislations. Having a cyber security culture and awareness will enlighten people and ultimately achieve the stated objective in the policy and strategic document. The government of South Africa has tried in this regards as there are several awareness programmes developed for this purpose. In fact it is estimated that about 51% of South African population based on the sample dram in 2007/2008 are aware of some of the dangers on online activities, all of

this owing to the government initiatives to have many awareness programmes.

D. National Cybersecurity Advisory Council

This policy document mandates the formation and coordination of all cybersecurity programs. Under this policy, council members are appointed and their tenure duration are clearly spelled out by the Minister of Communications.

1. Computer Security Incident Response Team (CSIRT)

This is the formation of a team, cutting across different functional areas within the system are charged with the responsibility of preparing for and also responding to cybersecurity related incidents. Thus, acts as a contact point for threats and breaches related to cyber security. Usually, the response plan is in five phases; *identification of threats*, *analysis*, *containing such threat*, *mitigation* and *reporting the outcome*.

2. Cyber Inspectorate

The cyber inspectorate is charge with the responsibility of liaising with law enforcement agencies, to provide both private and public services. It is also responsible for inspecting and monitoring websites or related activities in the public domain and report in the event any bridge or compromise.

3. Law Enforcement

The policy provides for the exploitation of various initiatives to strengthen capacity among the law enforcement agencies charge with the responsibility of handling cybercrime. South Africa must comply with best practices in this line.

4. Minimize Cybersecurity Threats and Vulnerabilities

To reduce cyber threats and vulnerabilities, the policy mandates that the Minister of Communications come up with guidelines for the protection and identification of cybersecurity threats and vulnerabilities. Also there has to be a periodic review of best practices in intelligence

gathering, crime detection, investigation and prosecution of offenders.

5. Local and International Partnership

Regarding local and international partnerships, this policy mandates the formation of initiatives to ensure cooperation and coordination between local and international partnerships which could be either private or government sector. This ensures adequate information sharing amongst stakeholders, which could go a long way on securing South Africa's Cyberspace.

6. Innovation, Skills Development and Compliance

The popularity of Cybercrime and its continuous threats cannot be over emphasized. As such there is a continuous need to develop strategies to deal with related issues as they arise. These issues could be developing a well packaged cybersecurity programmes developing a Security culture to create awareness e.tc. The policy developed here will focus on the aforementioned issues in other to address them.

E. South African Cybersecurity Laws and Policies

In the Republic of South Africa, there are some reliable and operational sources of information relating to national cyber security laws and security found during this research and they include; The South African Cybercrimes and Cybersecurity Bill, The Protection of Critical Infrastructure Bill, The Protection of Personal Information Act 4 of 2013, The Electronic Communications and Transactions Act of 2002, as well as other governmental requirements expressed in the Department of Public Service and Administration (DPSA) Public Service Corporate Governance of Information and Communication Technology Policy framework which requires that COBIT be adopted by public sector organisations.

The Republic of South Africa identified six level of implementation of the country's national cyber security laws and policy. Consequently, according to Jacobs (2018)

NCMF applied to South Africa NCMF Level South Africa National cybersecurity identification function NCMF Level 1 (L1) Domain: Defensive domain. Mandate: Critical information infrastructure protection (CIIP) and National crisis management. Dimension: Government (SSA, DOD, DTPS, SITA) National (SABRIC) international (FIRST). National authoritative sources: NCPF, South African Cybercrimes and Cybersecurity Bill, Protection of Critical Infrastructure Bill, The Protection of Personal Information Act 4 of 2013, Electronic Communications and Transactions Act of 2002. National normative: COBIT 5. Mandatory national cybersecurity functions: Incident handling and monitoring and evaluation of national ICT as prescribed by NCPF and applicable to the selected domain and mandates. National cybersecurity selection and prioritisation function NCMF level 2 (L2) overall controlling body: National Cybersecurity Advisory Council. National strategic risk and threat assessment process: Using ISO/IEC 27005:2011. National cybersecurity function implementation NCMF level 3 (L3) After application of the national strategic risk and threat assessment process, a selection and prioritisation of the identified national cybersecurity functions takes place. In our example, the national incident handling and monitoring and evaluation of national ICT functions are selected and prioritised for implementation. NCMF level 4 (L4) Structures identified from where the selected and prioritised national cybersecurity functions are offered from as determined by considering the Defensive Domains lifecycle phases. The structure at national level is a CSIRT, and at organisational level, a SOC. For illustration, a CSIRT is selected.

Generally, a summary of the following actions constitutes a crime in the Republic of South Africa:

1) Any unauthorized intrusion or hijacking of data is a crime.
2) Any unauthorized hijacking that compromises the integrity of data is a crime, and that includes the creation

and distribution of viruses, worms or Trojan horses. However, the act must be perpetrated intentionally.

3) Any unlawful use of system or devices that are meant to serve as security measures for data protection is a crime and that includes the use of cracking software.
4) Denial of Service to any device or server in other to crash it is a crime.
5) Computer related fraud or forgery are classified as extortion and a crime that is punishable.
6) An accomplice to any of the crimes mentioned above is also guilty person.

F. Comparative Analysis of Cybersecurity Policies in Nigeria and South Africa

After thorough examination of the cybersecurity policies in both Nigeria and South Africa, it was discovered that both countries are far behind developed countries in areas like government coordination, legislation, stakeholder engagement and interaction and in skilled labour supply. There is no coordinated approach in both Nigeria and South Africa in handling cybersecurity. Even though there are structures in place to handle cyber related issues, these structures however are inadequate to holistically handle cyber security issues. In South Africa for Example, various legal establishments are in place to address cybersecurity, but then they have proved to be ineffective in handling the challenges the country faces in cybercrime.

Intensely securing the cyberspace of any country no doubt cannot be done alone. It requires Stakeholder collaboration given how digital and connected the world has become, hence it is referred to as a global village. Both Nigeria and South Africa have also failed in this regard especially in the area of development, monitoring and implementation of cyber related protocols and both software's and hardware's components. The South African government has slowly embraced a National Cybersecurity Policy Framework, but the problem is the slow

implementation reporting and there seems to be no light at the end of the tunnel for now since as there is no adequate coordination amongst the agencies and stakeholders. Indeed, there seems to be little, or no priority placed on cybersecurity in South Africa which is obvious from the fact that even the policy and strategic documents took two years to be adopted.

Another challenge faced individually by both Nigeria and South Africa is the fact that convincing citizens to accept and embrace best practices for cybersecurity has become very difficult even though it is part of the policy. Another challenged faced by both countries is that it has become difficult to convince business owners to take responsibility at times to defend themselves by adopting appropriate measures to curb cyber threats and at the same time escalate all successful attacks. The governments has a serious job on their hands to address this and needs to do whatever it takes to encourage this businesses to adopt this strategy. The problems are further compounded in both Nigeria and South Africa with the fact that there is a shortage of ICT skills, which has affected the deployment and development of ICT and ultimately the economy.

Nigeria's Cybersecurity Policy and strategy documents contains a well spelled out cybersecurity therapy for the country. However, the recent EndSars protests of last year October 2020, saw different attacks which compromised so many government and private assets and that shows that a lot needs to be done to actualize what is contained in the policy document. So, both Nigeria and South Africa have adopted a similar strategy to deal with Cybercrime, but the main issue is implementation which till date has remained a challenge.

4. CONCLUSION

In conclusion, well-structured cyber-security program requires a very robust commitment from the federal government to stimulate the required implementation of

recommended strategic actions. All stakeholders must display the required commitment by working hand in glove with government within the define scope to balance the social and economic cyber space.

In the course of the analysis of both Nigerian and South African Cyber Security Policies and Strategies, the outcome of the analysis reflects on the fact that the documents are to an extent comprehensive in terms of content because most of the expected contents are largely present as per the research work carried out. However, other aspects like the detail explanation of the current state of cyber security in the two countries, business relationship with internet service providers, the development of a military cyber defence capabilities and the establishment of a digital identity frameworks were absent or only barely involved.

There are also areas of concern from the research work carried out and as a result the following recommendation are proposed.

1) There should be details of the status or state of cyber security in both the strategic and policy documents of both Nigeria and South African.
2) The Policy document should be adapted to each country's local need to tackle local issues patterning cyber security.
3) There should be a digital identity framework so citizens can be identified within the cyberspace.
4) There should be a good partnership and relationship between the government and Internet Service Providers for better and more proactive monitoring.
5) Lastly, the policy and strategic documents should contain a national cyber defence military capability.

5. DECLARATION OF CONFLICTING INTERESTS

The Authors declare that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING
None

7. ACKNOWLEDGEMENT
None

8. REFERENCES
Ajah, M., (2016). FUTA Website Hacked By Indonesian Hacking Group. *NaijaTechGuy* [online]. available from: https://www.naijatechguy.com/2016/11/futa-website-hacked-by- indonesian.html [Accessed 11 May 2021].

Bit Sight, (2016). *The rising face of cyber crime: ransomware* [online]. BitSight Technologies. Available from: https://info.bitsight.com/bitsight-insights-ransomware-pr?utm_campaign=Q316%20BitSight%20Insights&utm_medium=Press%20Release&utm_source=Press [Accessed 29 Feb 2021].

Grajek, S., (2018). Top 10 IT Issues, 2018: The Remaking of Higher Education. *EDUCAUSE Review* [online], (2017–2018 EDUCAUSE), 36. Available from: https://er.educause.edu/-/media/files/articles/2018/1/er181100.pdf [Accessed 28 Feb 2021].

Icirnigeria, (2017). How Thieves Hacked Into Our Database - JAMB. *The ICIR* [online]. Available from: https://www.icirnigeria.org/how-thieves-hacked-into-our-database-jamb/ [Accessed 11 May 2021].

Ikeji, L., (2019). *University of Nigeria, Nsukka (UNN) official website hacked by suspected French hacker* [online]. Linda Ikeji's Blog. Available from: https://www.lindaikejisblog.com/2019/10/university-of-nigeria-nsukka-unn-official-website-hacked-by-suspected-french-hacker.html [Accessed 11 May 2021].

Jacobs, P.C. (2018). A National Cybersecurity Management Framework for Developing Countries. Johannesburg: University of Johannesburg. Available from: http://hdl.handle.net/102000/0002 (Accessed: 22 August 2021).

Loader, B. D. and Thomas, D. (2000). Introduction. In B. D. Loader and D. Thomas (Eds.), *Cyber crime: Law enforcement, surveillance and security in the information age* (pp. 1 –14)

Matthews, B. and Ross, L., (2010). *Research methods: a practical guide for the social sciences*. 1st ed. New York, NY: Pearson Longman.

News Agency, N., (2019). "Our Website has been Hacked and Some Results Upgraded" JAMB Cries-out ....Orders for Fresh Exam May 26ths. *Naija Live Tv* [online]. Available from: https://www.naijalivetv.com/our-website-has-been-hacked-and-some-results-upgraded-jamb-cries-out-orders-for-fresh-exam-may-26ths/ [Accessed 11 May 2021].

Nseyen, N., 2020. *2020 UTME: JAMB shuts down portal, announces new means of checking result* [online]. Daily Post Nigeria. Available from: https://dailypost.ng/2020/03/18/2020-utme-jamb-shuts-down-portal-announces-new-means-of-checking-result/ [Accessed 11 May 2021].

Odumesi, J. O. (2014). Combating the Menace of Cybercrime. *International Journal of Computer Science and Mobile Computing*, *3*(6), 980 – 991

Office of the National Security Adviser (2014). *National Cybersecurity Policy.* http://www.cybersecuritynigeria.org.ng/ncsf/index.php/downloadable-docs

Okeshola, F. B. and Adeta, A. K., (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research* [online], 3 (9), 17. Available from: http://www.aijcrnet.com/journals/Vol_3_No_9_September_2013/12.pdf [Accessed 26 Apr 2021].

Sawahel, W., (2017). *Universities face an age of cyber crime* [online]. University World News. Available from: https://www.universityworldnews.com/post.php?story=20170922080320 52 [Accessed 30 Apr 2021].

Serianu, A. (2016). *Africa Cyber Security Report 2016* [online]. Lavington, Kenya: Serianu Limited. Available from:

https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf [Accessed 30 Apr 2021].

The Nation, (2019). N180m fraud rocks Covenant University. *Latest Nigeria News, Nigerian Newspapers, Politics* [online], 18 May 2019. Available from: https://thenationonlineng.net/n180m-fraud-rocks-covenant-university/ [Accessed 10 May 2021].