COMPARATIVE ANALYSIS OF CYBERSECURITY STRATEGIES, POLICIES AND MEASURES BETWEEN NIGERIA AND KENYA

Enofogha Gabriel Urhukpaghogho

Abstract. The failure to deal with threats emerging from the cyber space was compounded by the fact that, in several states there were no proper definitions of functions, institutions, resources and skills. Consequently, the cyber security resilience can be achieved through the national cyber security strategy. The study's objective is to investigate and compare the cyber security policy and strategy drafts put in place in both Nigeria and Kenya in response to the emerging cyber security threats with the aim of proposing a working and sustainable cyber security strategy and framework for Africa and the world at large. The methodologies adopted for this work were analytic, expository, and critical. To create a sustainable cyber security strategy, there is a need to be aware of what technologies are in place to support the infrastructure. It is also essential to establish who takes responsibility for these technologies in order to avoid future dilemmas when decisions with reference to the infrastructure have to be made. The result of the study found out that the important element of a cybersecurity strategy includes but not limited to: An Information and Communication Technology Master Plan, information security policy, and Recovery and Continuity Planning. These form the basis of an ideal cybersecurity strategy. The study recommended that the implementation of cybersecurity strategy does not guarantee improved mitigation of cyber-attacks, particularly in Africa. Therefore, shifting the current security ecosystem to one that has major repercussions for negligent acts is necessary to decrease cybercrime incidents. This shift in priorities will need to be accompanied by further sensitization, security training, and adequate investments in security systems and collaboration between stakeholders.

Keywords: Cybersecurity, strategy, cybercrime, policy, comparison, Information and communication technology, Nigeria, Kenya, Africa

1 Introduction

Cyber security came about as a result of advances in information and communication technology (ICT). The cyber security threats became pronounced in Africa from 2007 through reading the attacks from Eastern Europe. Furthermore, the failure to deal with threats emerging from the cyber space was compounded by the fact that, in several states there were no proper definitions of functions, institutions, resources and skills. Consequently, the cyber security resilience can be achieved through the "national cyber security strategy" as was later developed by Estonia [1]. Cyber security is a menace of serious concern to the nation, Nigeria. Due to its national priority, it is now handled by the President's office. The President of Nigeria through his National Security Adviser in 2016 consented to the country's bill on Cyber Crime. The drafts on Nigeria cyber security policy and strategy were officially. In June, 2017, the National Cyber Security Policy and Strategy drafts were officially unveiled in 2017 in Lagos at a seminar [2]. In like manner with other nations with an advanced ICT infrastructure, Kenya's carries out its social, economic and national security activities in this digital, interconnected environment. However, these same technologies come along with new risks that can lead to an extensive damage to national security, economic growth, and critical infrastructures. Therefore, the Government of Kenya considers protecting its national cyberspace a responsibility of utmost priority in order to continue to encourage economic growth for the country and its citizens [3].

Moreover, most of the literature available on the cyber security threats legal frameworks and institutions, responses and the relevant strategies in the African region adopted to combat cyber security threats revealed that, there is no, or minimal efforts put in place to fight these threats in both countries. The political will to address the cyber security threats as part of the national security is also lacking. The unassertiveness of the securitization models developed and adopted is not clear in most of the African states. In fact, the general integration of the cyber security into national security strategic plans in most cases is the missing link in the security of the state and security of the cyber space. It is in this vein that, the study seeks to establish the legal frameworks and institutions available defense mechanisms as well as the adopted strategies.

Consequently, this paper would be very useful in the evaluation of the cyber security strategy and afterwards proffer contributions and make recommendations, preceding the implementation of the cybersecurity strategy eventually in any other part of the world. Also, following the insufficiency in the studies, it is incumbent that, information gaps in regard to the cyber security threats and national security in the African region, is an area that requires further studies. The study intends to generate and contribute more knowledge by assessing these threats, national security policies and strategies in place.

2 Literature Review

Recently, cyber security has continuously gained international and global attention. This is due to its essential benefits if harnessed properly, and conversely negative effect if not payed attention on national level. Consequently, there is the uprising of problems considering cyber security as a serious national consideration, with utmost priorities in numerous countries across the globe. This has resulted to the growth of the strategies on national cyber security all over the world, which is observed in so many countries in the world.

The existence of threats causing risks on the national security on India and France were respectively acknowledged by [4] and [5]. The Indian cyber security strategy was examined from a market-driven against a regulatory method, which was widely rejected for reasons such as deficit in private sector’s voluntary support by the private sector in assuring the requirement for national cyber security, nevertheless seen to be in agreement and supported by the United States amongst other countries.

Furthermore, [5] studied France’s strategy on cyber security, looking at it from a national defence and military angle, showing its proficiencies, obligations and also as projections geared at supporting and improving the nation’s cyber security. He noted that the national cyber security of France white paper works as an acceptable way to current innovations in an environment that is planned. From this explanation, the roles and capabilities of the military in improving cyber security as stated by the white paper were recognized, but criticized for the absence of standard equipment and budgetary restraints in attaining these objectives. Furthermore, it was explained that the white paper points out the key position of France in defence and security but this faulted as the European Union’s Common Security and Defence Policy’s (CSDP) operation recently, been noticed not to have a political will.

In connection with [5], [6] and [7] acknowledged the essential role played by the United States globally in improving cyber security. After analysing the Turkish cyber security strategy, [6] asserted that the national cyber security strategy of United States is considered amongst others as the most frequently accessed, signifying the country’s global importance on cyber security matters. While elucidating on the relevance of cyber space, they echoed an assertion made by the Cabinet Office of the United Kingdom in 2009 which identified the understanding of the country on her cyber security, in the 21st century, as crucial for the nations development safety. Nonetheless considered also from a military perspective, their investigation is different from that of [5]. It suggested methods to be applied on the cyber security strategy of a nation that is faced by a target country with a Deter-Disarm-Defend triangle, involving military procedures for defence. A review of the national cyber security strategy of Turkey was however recommended in order to allow for the addition of more aggressive strategies, in the face of the defensive ones presently available.

Analysing the strategy of cyber security in Japan, [7] made an attempt to highlight the lapses in some areas and suggested possible solutions for development. [7] recognized Japan’s attempt to make advances towards increasing her collaboration with other countries, but however, the nation’s cyber security independence was also acknowledged. Some of the recommendations suggested are hastening of the training of human resources in crucial areas in cyber security in order to improve partnership technically with other countries, awareness situated rightly, despite the currently available structure of high quality cyber security.

Despite the different enormous possibilities in which a nation's cyber security strategies may appear, generally, they reach agreement by a common objective which is to increase efforts towards achieving sustainable cyber security. Nonetheless, there are differences in the crucial points by which this aim is envisioned to be achieved.

2.1 Cyber Security Policy and Strategies

Strategies and policies are frameworks for development that are created my policy makers and executives at the highest level of an organization which is to be strictly followed, irrespective of imminent situations. A nation's cyber security strategy is her preparedness strategy make available organised strategic actions and measures geared ensuring security of a the country when using cyber space, protecting vital infrastructure of information, creating and fostering a community of cyber space that can be trusted. [2].

2.1.1 Importance of Strategies and Policies of Cyber Security

Amongst the concerns of many existing government, it is important to note that the issue of cyber security is an issue whose importance must be given great attention. Presently, the considerations of cyber security are unstoppably attracting the attention of the globe. With such great importance, the policy makers concerned, stakeholders and governments cannot do without carefully creating principles such as strategies and policies that are meant to guide and govern the issues of cyber security [2]. Together, a goal-driven and workable poly and strategy of cyber security would enable the achievement of a possibility of reduced successful incidence of cybercrime at the national level. Also, the cyber security strategy would empower a nation with the ability to take precaution over attacks of any kind and also quickly curtail them when they occur. It would also foster collaboration between countries in areas of development and security as it represents global equality [2]. Cyber security strategy and policy in its totality makes an attempt to make available a framework made up a collection of action plans guiding principles that are geared towards curbing cyber security and other incidents that are related.

2.2 Cases of Cybercrimes in Nigeria

Cybercrime activities are prevalent in Nigeria. It was reported recently by the Internet Crime Complaint Centre in the Daily Trust, a collaboration between the America's National White Collar Crime Centre and the Federal Bureau of Investigation (FBI) that Nigeria is ranked number three among the top ten countries where cybercrime is prevalent in the world, with 8% behind the United States [8]. According to [9], in Africa, Nigeria is number country in terms of the prevalence of internet and computer-related crimes, which is gaining ground across the sub-region of West Africa. Similarly, the American national Fraud Information Centre ranked Nigeria cybercrime impact per capita as being exceptionally high while reporting money offers in Nigeria as an online scam that is very fast, which in 2001 has risen to 90 % [10].

2.3 The Kenya Cyberspace

ICT remained significant in Kenya's economy and more pronounced from 2000 [11]. However, from 2004, Kenya's ICT economy had not developed into a single entity. It was still characterised by fragmented institutions which were complimented by fragmented legislative acts that promulgated them. Kenya is placed amongst the leading ICT giants in Africa and thus having an economy of US$5.6bn. In fact, this was a significant growth in both technologies and infrastructure. It should be noted that 31% of Kenya's economy is on the electronic platforms with Mpesa leading the pack [12]. Kenya's national critical infrastructure starts from the satellite links, undersea cables joining at Mombasa, the great fibre linkage from Mombasa to Nairobi. The internal has public safety and termini security at the road, air and seaports. It includes the main highway surveillance and key installations, buildings and business hubs through the closed circuit television systems (CCTV). This is illustrated in the figure 1 below.

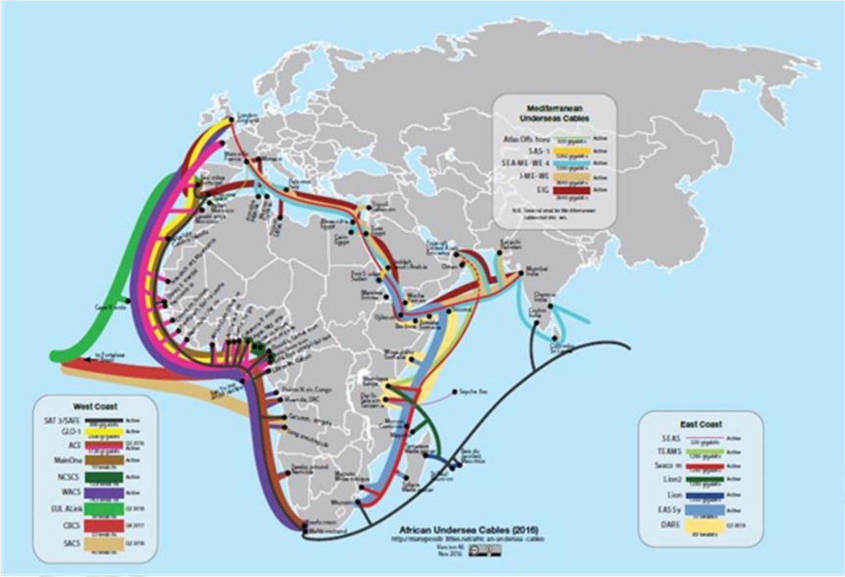


Figure 1: Undersea cables provisions.
Source: African Undersea Cables

2.3.1 Cases of Cybercrime in Kenya

An international group on cybercrime working from Kenya is aiming at organizations within and outside the country through Business Email Compromise (BEC) a type of phishing. Hacking and impersonation of corporate email accounts by criminals to deceive companies into releasing sensitive data or money to the criminal's account [13]. Fairfax County government in Washington DC was robbed of a huge amount of money by cyber criminals in Kenya by accepting instructions it thought was coming from Dell, its computer suppliers based in Texas, to redirect payment to a new account in Ohio. The money was channelled to Nairobi from Ohio. This attack was just a part of an organised and well-planned international criminal BEC phishing arrangement was discovered and interrupted by the Federal Bureau of Investigation (FBI) of the United States.

2.3.2 Legal Frameworks in Kenya

Some of the legal frameworks include "the Penal Code, Kenya Communication and information (Amendment Act Cap 411)". Other notable cyber security legislations in Kenya include "the Data protection Act (2019) and computer misuse and cybercrimes Act (2018)". The principal document for structuring all the legal frameworks of a state is the constitution. Thus, all other subsequent legislature efforts will be in the spirit of the constitution [14]. The Constitution of Kenya, Chapter 14, acknowledges protection of the nation from all threats. Hence, it is certainly that, the constitution is observant of the dynamics in national security. Since security has evolved to include the societal, economics, military, political and environment to be essential parts of national security. The Computer Misuse and Cyber Crime Act of 2018, pronounces the crime in the republic of Kenya [14]. The act is administered under the main criminal offences in the state by the NPS to enable its reinforcement. The Kenya Information and Communication Act, 2019 has provisions for the formulation of institutions such as the Communication Authority of Kenya (CAK) mandated to come up with a cyber-security management framework [15].

2.4 Cyber security Legal Frameworks in Nigeria and Kenya

The purpose of the legal framework of cyber security is to recognise the strategy needed to ensure the implementation, management, sustainability of areas needed in the strategy of cyber security which are effective in fighting cybercrime in Kenya and Nigeria. In these two countries, the existence of the cyber-specific laws that govern states is not adequately pronounced [16]. Although this gap in the legal frameworks and provisions of the laws is glaring, this does not mean that there are no rules that govern cyberspace activities [17]. States in regional or sub-regional groupings, agree upon parameters which are the rules that govern the behaviour of the states.

The general applicable rules of international law govern behaviour conduct at the cyber space [18]. The international law is applicable to the cyberspace, as a flexible and adequate body of laws, with power to regulate the regions and states once they are institutionalized. The structure of the international law itself makes it adaptive and accommodative to the advent of new phenomenon, such as the cyberspace security and the inherent operations, hence there is need for efforts to regulate these operations [19]. The operations in the cyber space and methodologies, tools and instruments applied in the processes, qualify to be governed by international law, as it was used to govern the nuclear weapons [20].

2.4.1 African Union (AU) Cyber Security Strategies

At the extra-ordinary conference held in Johannesburg of the African Union Ministers who are in control of ICT in 2009, the minister looked at different issues related to the development and growth of ICT in Africa. It was agreed that the African Union Commission, in collaboration with the Economic Commission for Africa of the United Nations should create a legal framework for Africa that would deal with issues like electronic transactions, data protection, and cyber security [21].

The African Union in 2011 presented the draft African union convention on the establishment of a credible legal framework for cyber security in Africa. the purpose of the drafters was to make existing legislation strong in Member States with respect to ICTs. With respect to the mandate which was not restricted to cybercrime only, but also involved other ICT society related issues such as electronic transactions and data protection. The convention which was seen to be more sustainable than other approaches in other regions contains four parts. Part one has to do with electronic commerce. It solves various areas such as predetermined obligation of an electronic provider of goods and services make responsibility in electronic form and electronic transactions security. Part two addresses issues related to the protection of data. While part three deals with how to fight cybercrime. Section 1 is made up of five chapters. This involves a collection of six definitions which include electronic communication, computerized data, racism and xenophobia in ICTs, minor, child pornography and computer system. The fourth chapter involves the monitoring structures of the nation's cyber security. The chapter 5 was dedicated to collaboration amongst nations [22].

2.4.2 Cyber Security Response Strategies Frameworks in Africa as a Region

The cyber security threats in the Africa region are a concern compared to developed regions such as the Europe and America. The cyber security threats have manifested as a force to reckon within in the regional and nation security. It is further expounded by the fact that, the concepts of safeguarding the cyberspace from possible threats have become an important agenda in most of the African states [23]. The increased awareness is not on an exponential scale, as some other states have remained unassuming in implementation of cyber defense mechanisms, as part of national security agenda. These threats in the continent have fascinated the African region to revise the regional strategic security plans at hand. Africa Union Group of the Experts Report (2019), states that, the region finalized the response strategies and hence needed implementation [24].

An assessment of the cyber security strategy in Africa indicates that creation of awareness is very important either separately or as part of the responsibility of the suggested national strategy [25]. Though there are no cybersecurity strategy and policy in some African countries, some organisations have already discovered the importance of international coordination and increase in awareness on cybersecurity some of which include the African Information Society Initiative (UNECA/AISI) (United Nations, 2018), the Internet Numbers Registry for Africa [26], ITU/GCA, 2018, The Southern African Development Community (SADC), 2018 and Information Security Group of Africa (ISG)-Africa, 2018.

Efforts are available in Africa such as the Information Security Group of Africa, 2018. This is an organized community and industry-wide movement to enlighten Africans on how to safely and responsibly use computers and the internet in order to reduce the risks that come along with its use and also build the trust of consumers. Of recent, a partnership with more than twenty non-governmental organizations and official agencies from various African countries has been made known as Facebook in order to the safer internet day usually celebrated on the 6th of February [27]. The safer internet day emphasises on making the internet safe, particularly for youths.

3 Requirements for Sustainable Strategy of Cyber Security

To create a sustainable strategy of cyber security, there is a need to be aware of what technologies are in place to support the infrastructure. It is also essential to establish who takes responsibility for these technologies in order to avoid future dilemmas when decisions with reference to the infrastructure have to be made [28].

3.1 Human Capital

As much as we currently have many operations automated, there is still the human component of the information systems still involved. Too often the cause of data breach, cyber-attack or even systems sabotage is an employee, or a hacktivist. The employees as people who constantly interact with the system are of great concern and thus to ensure that the cyber security strategy is well supported it is important to look at the way an employee (especially IT professionals) is hired, and terminated and this has to be explicitly stated in the ICT master plan.

3.2 Budgeting

Attaining an optimum level of information security is not a cheap endeavour, when budgeting; it is important to take a clear consideration on the cost of cybercrime, inherent risk and creating a fund dedicated to mitigating and transferring the information security risks. It is therefore paramount to make it clear in the master plan on how information security is going to be financed and further outlining the emergency funds for unforeseen events and funds that aim at catering for the training programs and human capital development related programs.

3.3 Guiding Principles

There is need to ensure that a cyber security strategy includes guiding principles that will propel and constantly put the organization in check towards the attainment of the desired information technology goals in a manner that promotes the security of the entire communication infrastructure.

3.4 Creating a Cybersecurity Strategy

A cyber security strategy is the time bound plan that informs in the prudent ways of addressing identified cybersecurity challenges in a specified manner. It constitutes of the following sections:

3.4.1 Introduction Page

It is important to understand from what angle the decision to institute a cyber security strategy and the rationale behind the establishment of its authority are supposed to be in an overview section that provides for the scope of the strategy, objectives, who or what authority is responsible for the implantation maintenance and enforcement of the strategy, and the validity of the strategy. In my view, the introduction is the best place to establish the reasoning behind the strategy and the notwithstanding the efforts that have been done to mitigate the risks associated with the cyber security of the said country.

3.4.2 Strategy Context

On comparison between various strategies, the context of the strategy seeks to outline the identified threats, vulnerabilities and hazards/disasters that may endanger the cyber security for that given time. However, this section is the non-rigid section in that the content can be adjusted in quarterly manner as threats and vulnerabilities are on the rise constantly and so are the ways of addressing them.

3.4.3 Response to Strategy Context

In order to better address the challenges, the mandate and the guiding principles to the charged authority to implement the strategy through following the best practice standards in order to conform to the global standards are clearly outlined in this part. Generally, this section assigns roles and responsibilities, key expected outcomes and guiding principles.

3.4.4 Defence

To have a cyber secure environment is constantly becoming the number one priority to most organizations and institutions, this section therefore addresses what is to be defended and how it ought to be defended notwithstanding what is to be developed to promote the identified defence metrics.

3.4.5 Deterrence

This section explicitly states the areas that are to be well addressed in order to guard the institution from identified set of the unfavourable set of events, incidents, and crimes. It further prescribes strategies of dealing with such incidents in a manner that ensures the cyber secure environment is constantly at the optimum level.

3.5 Plan to Check Quality of the Proposed Strategy

The region of Africa is one with the highest rate of cybercrime that affects its economic, strategic and social growth and development.

It has been reported that the inter alai approximate cost have risen up to $175 million for Kenya, $85 for Tanzania and $550 million for Nigeria [29]. Nigeria and Kenya have comparable cyber security infrastructure which requires certain knowledge, infrastructure, skills, tools, as well as necessary equipment pertinent to the field. Therefore, this study compares the emerging cyber security strategies of Nigeria and Kenya with the aim of proposing a working and sustainable framework of cyber security strategy for Africa and the world at large. However, after the development and execution of the strategy, there would be a need to assess the quality of the proposed cyber security strategy. Through the evaluation of the results achieved by the activities of the strategy, precautionary and corrective measures that will bring about the upgrading of the subsequently strategy can be taken. Assessment is also required to find out whether the purpose and the programmed results have been achieved effectively.

3.1 Evaluation Approach

The following should be considered in stating the evaluation report for the strategy.

a. Definition of the evaluation limit, the main purposes, the envisaged result and its periodicity.
b. Implementation of the principle of separation of duties, i.e., specifying the responsibility of assessing the efficacy of the national strategy of cyber security and its activities to self-governing body, an overseer or a third part that can be trusted.
c. Following of both a qualitative and quantitative method with emphases on both the outcome and impact.
d. An assessment that is self-impact for the strategy's individual activity taking note of the view of the key participants
e. There will be an impact assessment from the outside for each of the strategy's activity with consideration of the view of the affected and/or external users.
f. There will be evaluation of every activity against the key performance indicators and action plan agreed upon on when the activity starts.
g. Preparation of a report on systematic evaluation explaining the results achieved and what should be expected in the subsequent evaluation.
h. Conduction of a benchmarking study for comparing the strategies amongst the Member States involved.

Furthermore, the Global Cybersecurity Index (GCI) will be used as a guide to measure security index before and after the implementation of the proposed strategy. The GCI is a reliable tool that can be used to assess countries' commitment to cyber security at an international level. The level of development or involvement of every country's cyber security strategy will be examined along the following five pillars:

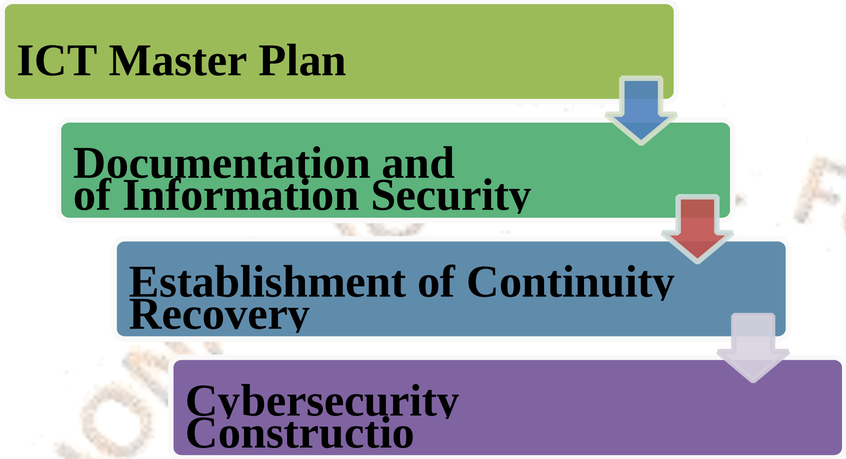
The GCI is a trusted reference that measures the commitment of countries to cybersecurity at a global level. Each country's level of development or engagement of her cyber security strategy will be assessed along five pillars:

(i) Legal Processes
(ii) Technical Processes
(iii) Organizational Processes
(iv) Capacity Development
(v) Cooperation.

4 Flowchart and Description of Developed Cyber Security Framework

4.1 Proposed Framework

The important element of a cybersecurity strategy includes but not limited to: An ICT Master Plan, information security policy, and Recovery and Continuity Planning. These form the basis of an ideal cybersecurity strategy.


ICT Master Plan
Documentation and of Information Security
Establishment of Continuity Recovery
Cybersecurity Constructio

4.1.1 Anatomy of Framework

The anatomy of framework offers the organizations of the necessary tools needed to securely keep information related to cybersecurity. In the framework, cybersecurity goals can be thought out and well-articulated and cybersecurity protocols and processes can be easily updated.

First Element: ICT Master Plan

The strategic area of focus under the ICT master Plan should involve but not restricted to the following:

i. Definition of National Assets and its identification
ii. Infrastructure Plan and Critical Components Identification
iii. Budgeting for ICT and sources of the budget
v. Conception of Human capital and development of human skill
vi. Definition of the stakeholders.
vii. Strategy on Management of Projects
viii. ICT future Plans
viii. National Vision for ICT

Among every cyber security strategy that could be developed, it has been one of the findings of this thesis work that the creation of an ICT master plan appears to be the most important and a key element. As identified from the study of Nigeria and Kenya, a major step in the creation of efficient cybersecurity strategy is to commence the construction of ICT master plan.

Second Element: Government Policy on Information Security

Here, emphasis is on Government’s policy plan on information security. The following checklist was founded to be critical in ensuring Government’s policy on information security in the cyberspace.

i. A detailed ICT Master Plan.
ii. Well stated and thought-out Security Objectives
iii. Release of specific security outlines.
iv. Security outlines related to specific assets of both private and public stakeholders.

v. Security outlines related to specific assets of the people
vi. ICT-Related Laws
vii. Security Viewpoint
viii. Standards and industry best practices.

When it comes to the definition of essential parameters towards ensuring proper security measures for generated information, the storage of such information and the dissemination of the information within the infrastructures available in a government or organization, the above checklist forms the second layer of strategy for cybersecurity.

Third Element: Continuity and Recovery Plan

Since the purpose of every attack on infrastructure is to bring it down or abuse it, when such situations occurs, there should be a plan to restore the infrastructure back to normal working conditions. In order to ensure continuity and recovery plan, the following should be part of the plan to ensure continuity and recovery plan.

i. Master Plan for ICT.
ii. Policy on Information Security.
iii. Incidents management and Events identification and analysis.
iv. Authority and measures.
v. Security Standards and Procedures.

This security and recovery plan ensures that organizations have control of the cybersecurity strategy in place.

The Goal: Cybersecurity Strategy

The essential elements that should be present in cybersecurity strategy are itemized next.

i. Master Plan for ICT.
ii. Policy on Information Security.
iii. Plans for Continuity and recovery of infrastructure.
iv. Definition of Cyberspace security landscape.
v. Preparedness of stakeholders.
vi. Strategic goals and objectives.

The completion of cybersecurity strategy is of great importance to a nation because it ensures a foundation upon which strategic formulation of legislation for response towards cybercrimes and cybercriminals.

4.2 Relevance of the Framework

(a) **Assists Stakeholders in Making Informed Decisions**: There are several decisions to be made from time to time. The presence of a framework is a guide to prevent stakeholders from derailing from the strategy in place. Such decisions include financial decisions where there is need to plan the budget to finance cybersecurity operations and programs as highlighted in the strategy. This will ensure that no part of the program towards the realization of the strategy suffers. This also leads to improved use of cybersecurity budget.

(b) **Provision of Common Way to Address Cybersecurity Concerns:** One of the impressive benefits provided by having a framework is that it ensures that every stakeholder has a common way to address cyber threat in order to ensure cybersecurity. The steps are well articulated and stated in the framework for every stakeholder to implement.

(c) **Ensuring Collaboration between Stakeholders:** One of the things that strengthen the implementation of strategy towards ensuring cybersecurity is collaboration. Through collaboration, ideas and strategies can be shared as well as critical information about emerging trends in cyberattacks and new dimensions in cybersecurity.

(d) **Time Saving through clear structure for taking action**: With the presence of a framework in place, it becomes easier for stakeholders to map the present stage they are in their journey to cybersecurity by identifying gaps. With this, stakeholders can have a clear and practicable discussion with organizational stakeholders. The journey to cybersecurity is made easier when stakeholders know their present stage and where they are supposed to be next.

4.3 Improving the Framework

For the period proposed for using the framework, the possible improvement of the framework can be achieved by following the steps discussed next.

4.3.1 Framework Documentation

A very useful process in object-oriented application framework development is documentation of the framework because it is a precondition to utilize the framework. The final goal of framework documentation is to have a simple, easy-to-use, effective, accurate, and comprehensive documentation.

4.3.2 Training, Involvement and Communication

In order to ensure the success of cybersecurity strategy implementation, every user has to be involved in the security process. Furthermore, the objectives and goals of the strategy have to be communicated as well as other indices of the desired result. In light of this, organizations need to be prepared for cyberattacks. When an emergency situation arises, effective communication is very important. In the case of failure of systems, a quick communication with all the employees is very necessary and to coordinate an effective response to the emergency.

4.3.3 Administrative Actions

The purpose of Administrative actions is to show that institutions will not tolerate some actions that are detrimental to the implementation of their strategy towards ensuring cybersecurity. These actions send a very clear message that the institution will not accept any excuse for actions that may lead to some undesired outcomes. This can be achieved by making the employees complete the policy compliance form. Whenever an employee is found culpable for their action, legal prosecution immediately ensues either in a criminal or civil court in order to recover organizational loss incurred as a result of the employees' actions.

4.3.4 Global Cyber Alliance

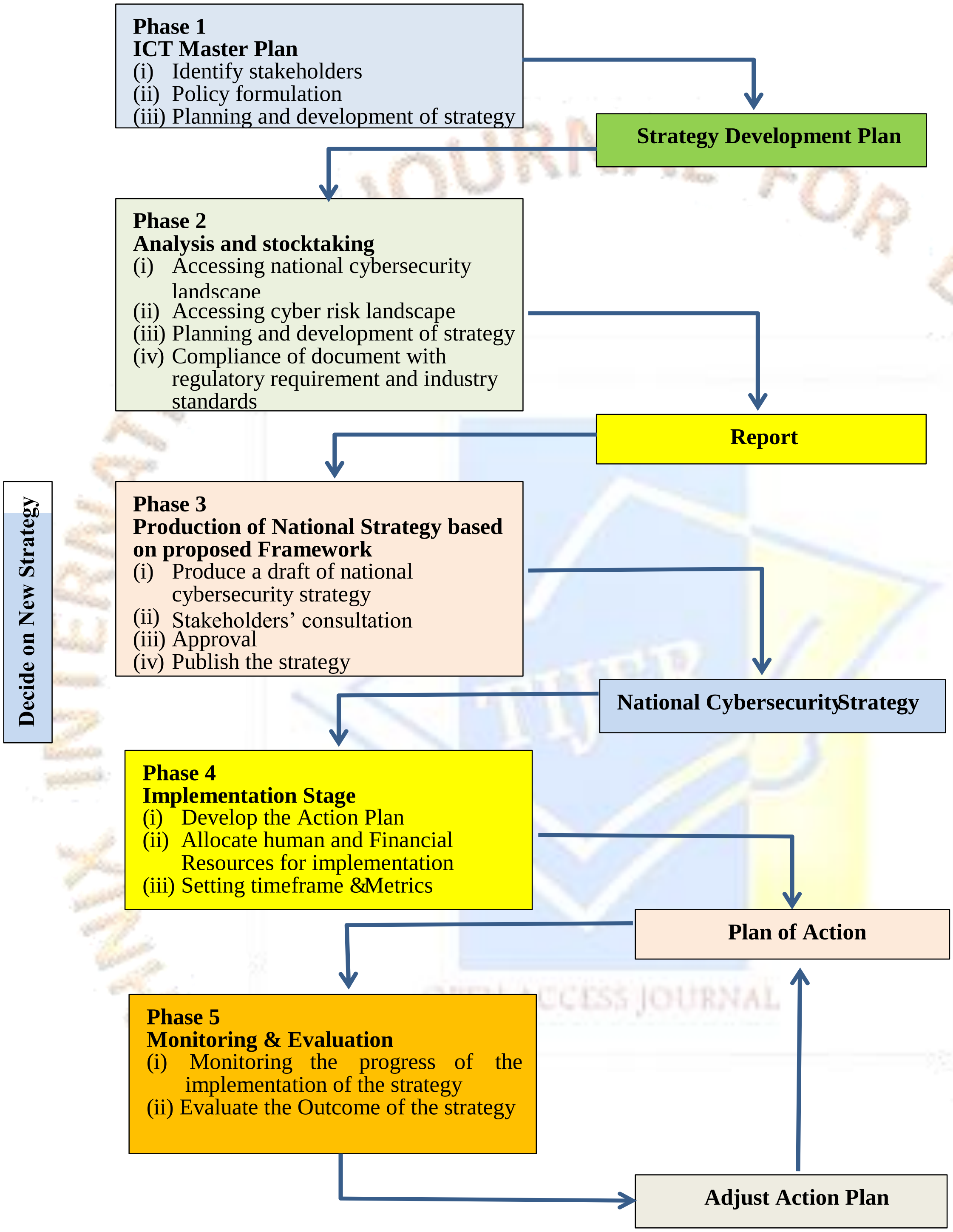
The security of the internet is a challenging task that are presently confronting policy makers and the clear lack of trust between institutions or policy makers has led some institutions to join cyber alliances like the global cyber alliance. Some of these alliances are mainly created for technical information sharing and intelligence. On the other hand, some are mainly created to address some vulnerability in the cyber world. Therefore, in order to thwart threats in the cyberspace, a centralized approach becomes necessary.

4.3.5 Internal Audit Department

Audit Department play a major role in the management of cyber threats by organizations or institutions through the provision of independent assessment of needed and existing controls, and by assisting the audit committee comprehend and address various risks that organization run in the digital space. The evolution of threats from cyberattacks has necessitated that internal audit should understand and carry out the assessment of institution's capacity in managing risks from cyberattacks. Therefore, an effective step by the internal audit is to embark on cyber risk assessment and summarizes their findings for audit committee and the board. The board then drives a risk-based and multilayer cybersecurity plan for internal audit.

4.4 Proposed Phases for Implementation of Centralized National Cybersecurity Strategy

The life cycle of a national cybersecurity strategy could be summarized in five major phases:


Phase 1
ICT Master Plan
(i) Identify stakeholders
(ii) Policy formulation
(iii) Planning and development of strategy
Strategy Development Plan
Phase 2
Analysis and stocktaking
(i) Accessing national cybersecurity landscape
(ii) Accessing cyber risk landscape
(iii) Planning and development of strategy
(iv) Compliance of document with regulatory requirement and industry standards
Report
Decide on New Strategy
Phase 3
Production of National Strategy based on proposed Framework
(i) Produce a draft of national cybersecurity strategy
(ii) Stakeholders' consultation
(iii) Approval
(iv) Publish the strategy
National CybersecurityStrategy
Phase 4
Implementation Stage
(i) Develop the Action Plan
(ii) Allocate human and Financial Resources for implementation
(iii) Setting timeframe &Metrics
Plan of Action
Phase 5
Monitoring & Evaluation
(i) Monitoring the progress of the implementation of the strategy
(ii) Evaluate the Outcome of the strategy
Adjust Action Plan

5 Conclusion

The implementation of cybersecurity strategy does not guarantee improved mitigation of cyber-attacks, particularly in Africa. Shifting the current security ecosystem to one that has major repercussions for negligent acts is necessary to decrease cybercrime incidents. Enforcement of existing legislation and strategy and the assignment of liabilities must be emphasized. This shift in priorities will need to be accompanied by further sensitization, security training, adequate investments in security systems, and collaboration between stakeholders. Each stakeholder must ensure that they are doing their part to prevent cybercrime, or know that they could be held liable for negligence. This ensures adequate motivation to protect data and invest in advanced security measures.

Based on research, cybercrime cannot be defeated solely through the implementation of conventional legislative policies and acts. Policies must be accompanied by sufficient funding and enforcement efforts. The coming together of all key members in the in the operational and governance level guard the privacy and security of users of internet. A safe and secure ICT environment warrants a shared and collective responsibility amongst all nations. It is also a necessity if African nations wish to digitally transform the continent and reap the benefits of technology to support human and economic development.

References

1. Kelly, J.: Strategic perspectives on cyber-security management and public policies. *European Cyber-security Journal, 2016, 1(1): 26-72.*

2. Osho, O. and Onoja, A. D.: National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. *International Journal of Cyber Criminology, 2017, 9 (1): 120 – 143.*

3. Government of Kenya, Ministry of Information Communications and Technology, Cybersecurity Strategy, 2016, pp. 1 – 13.

4. Data Security Council of India. Analysis of National Cyber Security Policy (NCSP –2013). http://dsci.in/search/node/1474.

5. Watanabe, L. France’s New Strategy: The 2013 White Paper [White paper], 2013. http://www.css.ethz.ch/publications/pdfs/CSSAnalysis-139-EN.pdf.

6. Şentürk, H., Çil, Z.C., Şeref, S. Cyber Security Analysis of Turkey. *International Journal of Information Security Science, 2012, 1(4), 112-125.*

7. Nitta, Y. Japan’s Approach towards International Strategy on Cyber Security Cooperation, 2013. http://lsgs.georgetown.edu/sites/lsgs/files/Japan_edited%20v2.pdf_for_printout.pdf

8. Folashade, B. O. and Abimbola, K. A.: The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research. 2016, 3(9).*

9. Ribadu, E. Cyber Crime and Commercial Fraud; A Nigerian Perspective. A paper presented at the Modern Law for Global Commerce, Vienna 9th – 12th July, 2017.

10. Saulawa, M. A. and Abubakar, M. K. Cybercrime in Nigeria: An Overview of Cybercrime Act 2013. *Journal of Law, Policy and Globalization. 2017, Vol. 34.*

11. Brencil, K. Kenya Cyber Security Report 2018. Nairobi: SERIANU Publication, 2018, pp. 35-37.

12. Douwe, K. The definition of cyber security. Oxford: University of Oxford, 2019.

13. Daghar, M. Cybercrime /Is Kenya the new playground for cyber criminals? ENACT observer, 2020.

14. Barry, B. and Little, R. International Systems in World History: Remaking the Study of International Relations, 1st Ed. Oxford: Oxford University Press, 2017.

15. CAK. A Collaborative Approach to National Cyber security Resilience. A Collaborative Approach to National Cyber security Resilience. Nairobi, Kenya, 2019.

16. Stefan, F.: Cyberspace Security: A definition and a description of remaining problems. Vienna: University Vienna - Institute of Government & European Studies, 2017.

17. James, L. and Katrina, T.: Cyber-security and Cyber-warfare, Preliminary Assessment of National Doctrine and Organization. Washington, D.C.: Centre for Strategic and International Studies, 2016.

18. Dighton, F.: Defining a Framework for Decision Making in Cyberspace: Strengthening Cyber- security Series. Pennsylvania: Indiana University Press, 2018.

19. Lars, B., Steffen, J. and Finn, S.: The Security-Development Nexus Expressions of Sovereignty and Securitization in Southern Africa. Cape Town, South Africa, 2017. p. 33.

20. CyberCity, E.: Media Statement SADC Capacity Building Workshop on Cyber Security and SADC Regional Cyber Drill. Mauritius, 2018. Pp. 34-35.

21. Hassan, A. B., Lass, F. D. and Makinde, J.: Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology. 2015, 2(7).*

22. Maitanmi, O., Ogunlere, S., Ayinde, S. and Adekunle, Y.: Impact of Cybercrimes on Nigerian Economy. *The International Journal of Engineering and Science (IJES), 2016, 2 (4): 45-51.*

23. Nyirenda-Jere, T. and Biru, T. Internet development and Internet governance in Africa. Geneva: Internet Society, 2019, p. 5.

24. Cavelty, M. D.: Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (1st ed). Boulder: Lynne Rienner, 2017, pp. 1-25.

25. Dlamini, I., Taute, B. and Radebe, J. Framework for an African policy towards creating cyber security awareness, The Southern African Cyber Security Awareness Workshop (SACSAW) 2019, pp. 15-31.

26. AfriNIC: “The internet numbers registry for Africa”. https://www.afrinic.net/, 2018.

27. Maslennikov, D. Kaspersky Security Bulletin 2018.The overall statistics for 2018. Available at https://securelist.com/kaspersky-security-bulletin-2018-theoverall-statistics-for-2018/36703/

28. Hansen,.L. and Nissenbaum, H. Digital Disaster, Cyber Security, and the Copenhagen School. New York: New York University, 2019. P. 246.

29. Serianu: “Africa cyber security report”. http://www.serianu.com/downloads/AfricaCyberSecurity Report2016.