NIGERIA'S CYBERSECURITY STRATEGY AND NATIONAL SECURITY POLICY

Adebukola Olubunmi, Ayoola (Ph.D)
bukkyayoola2014@gmail.com
+2348034754318
&
Iyanu-Oluwa Ayobami, Ayodele
History and International Studies Programme
Bowen University, Iwo Osun, Nigeria
ayodeleiyanuoluwa74@gmail.com
iyanu-oluwa.ayodele@bowen.edu.ng
https://orcid.org/0000-0001-5169-5891
+2348162235943

Abstract
Cybersecurity in the last two decades has grown exponentially as it relates to national security for countries around the world. The cybersecurity strategy of Nigeria is an important sectorial part of Nigeria's national security policy. The Office of the National Security Adviser considers the protection of cyber assets important and strategic. In the last ten years, Nigeria has been able to develop and implement a cybersecurity strategy which has dictated the direction of the protection of cyber assets and addressed challenges in the cyberspace. This paper examines the strategic position of a strong and effective cyber security policy in Nigeria's national security. The paper examines how a robust cyber security policy can help protect Nigeria's cyber assets from attacks from state and non-state actors in the era of cyber wars. The study relies mainly on both primary and secondary sources. Primary sources include official documents from the National Security Adviser office while secondary sources involve analysing existing papers and works on the subject matter. Using content analysis, the study argues that Nigeria's cyber security policy cannot be excluded from her national security policy and strategy as the cyber security strategy is a sectorial strategy needed by the security policy and strategy to handle national security issues arising from cyber-attacks, cyber espionage, and other related cyber offenses.

Keywords: Insecurity, cyberspace, cyber-security, strategy, and national policy

Introduction
Cybersecurity in the last two decades has grown exponentially as it relates to national security for countries around the world. The cybersecurity strategy of Nigeria has become an important part of its national security policy. Protecting critical national infrastructures and the safety of private sector assets has become a major concern.

In the last ten years, Nigeria has developed and implemented a cybersecurity strategy to provide a direction for the protection of cyber assets and address challenges in cyberspace. Still, despite its efforts, the country has failed to achieve a desirable result. Issues of cybercrimes like cyber terrorism, cyber espionage, cyber conflicts, money laundering and con-artistes (*yahoo yahoo trade*) and online child abuse[i] have in recent times assumed an alarming rate both in the private and official spaces with government security agents falling culprits of aiding and abetting cyber con-artistes in their heinous crime. All these have also given Nigeria and Nigerians a negative image within the international community.

The cybersecurity strategy of Nigeria is embedded in the national security policy as one of the four sectorial strategies of Nigeria's national security. The grand strategy for national security developed in the year 2000 by President Olusegun Obasanjo was the foundation for the development of the national security strategy in 2014 by the office of the National Security Adviser headed by Colonel Dasuki Sambo (Rtd.).[ii]

The national security strategy identified national security interests and threats to national security. The sectorial strategies were developed in response to the threats identified, which include information technology and cybercrimes[iii].

The sectorial strategies contain four key strategies, which include the national cybersecurity policy. This shows the relationship between national security policy and national cyber security policy. The national cybersecurity policy is the guiding policy for Nigeria towards combating cyber threats from internal and external aggressions from state or non-state actors to protect both public and private assets and infrastructures.

The Nigerian National Security Strategy of 2014[iv] was developed to combat security threats facing the country under the administration of President Goodluck Jonathan. This document was developed under Colonel Sambo Dasuki's (rtd) leadership, the then National Security Adviser. The policy document identified the various security challenges faced by the country, particularly terrorism, which is one of the major security threats to Nigeria. In the document, all other threats to national security were identified, including cybercrimes and related offenses. The document identified a robust cybersecurity strategy as one of its sectorial strategies required by the national security strategy to function properly to combat threats to the nation. The strategy provides a common framework on which the nation should focus its efforts. To properly articulate the government's strategy for tackling these security challenges, there is a need for a strategic plan in the form of a document to guide security agencies in the conception of ideas, formulation of policies and conduct of operations so that every single agency will be guided appropriately and be seen to be working

towards the same goal: the awareness that individual agencies are part of a larger whole, which when properly coordinated would present a neat, coherent, orderly and complete system.

The 2019 national security strategy[v] is an update of the 2014 Nigerian national security strategy. The changes can be seen in the name of the document. This document reflects new perspectives and frameworks to ensure the protection of the Nigerian state in terms of her national security. The document was developed by the office of the National Security Adviser under the leadership of Major General Babagana Moguno (Rtd) during the first term of President Muhammadu Buhari. The policy document aims to ensure a secure, safe, just, peaceful, prosperous, and strong nation. The mission is the application of national power to ensure security (human and physical) while ensuring peace and stability with the promotion of Nigeria's interests. The document identified key objectives such as national interests, the geo-strategic environment of Nigeria, national security threats such as terrorism and violent extremism, armed banditry, porous borders and cybercrimes and technology.

The document pays attention to protecting Nigeria and the Nigerian people from any form of internal and external security threat, promoting Nigeria's prosperity and sustainable development, promoting regional and international interests and, lastly, peaceful co-existence. The 2019 national security policy document provides a framework and guidelines for protecting Nigerian territory. It is a holistic document as it considers all areas, such as cybersecurity policy.

Nigeria's first cybersecurity policy document was developed in the year 2014. It was called National Cybersecurity Policy[vi], and it was developed during the administration of Goodluck Jonathan. The policy was implemented under the leadership of Colonel Sambo Dasuki (Rtd.), then the National Security Adviser. The policy was developed upon the realisation of the country to the importance of the protection of cyberspace and its implication on national security. The policy document identified national cybersecurity threats, such as online child porn, cyber terrorism, cyberbullying, and cyber espionage. The collaboration between national security strategy and cybersecurity with the national doctrines will be adopted to combat cyber threats. The document did provide the groundwork for cybersecurity for national security. However, it had its pitfalls, such as no proper implementation framework, which led to the update of the present policy document in 2021.

The update to the 2014 document is the National Cybersecurity Policy and Strategy, 2021[vii]. The document was developed with new realities, including Nigeria being one of Africa's leading digitally connected nations. The new policy identified several cyber threats that already existed in the 2014 document with

modifications such as pandemic-induced cyber threats and election interference. The new document considers the policy's direction, governance and coordination of the policy, management of the legal framework to ensure the law is on the same page with the policy, and, lastly, the protection of national assets.

Bayo Sule et al.[viii] examine the implication of cybercrime and weak cybersecurity defense for Nigeria's national security and digital economy. They opine that cybersecurity is a major challenge to national security. With the rising case of insecurity in Nigeria, it is evident that national security is in bad shape. Their attention was also drawn to digital economy as the world has moved from traditional economy to effective use of the internet and its machinery. This, they claim, has therefore, made Nigeria susceptible to cyber threats. They observed that the various challenges of cybersecurity to national security include poor funding, inadequately trained personnel and working frameworks. According to them, the prospects are positioned toward funding, training, and structured framework.

On the other hand, Denise Baken[ix] identifies Nigeria's vulnerability to cyber warfare, particularly with the rising presence of violent state actors in Nigeria such as Boko Haram, ISWAP, and others. He elaborated on the exponential use of cyber warfare as the new form of warfare with reference to states like China, the US and others. He referenced the leaked identity of DSS operatives by Boko Haram, which compromised the covers of personnel and affected the infiltration of the sect. Denise considers a strategic cyber security strategy that will help in the new form of warfare: cyber warfare. Idowu Bobade[x] identified the relationship between national security and cyber security, stating that high-security awareness will reduce cyber threats. He appraised cyber threats and national security from the angle of increased accessibility to the Internet and Internet-enabled devices, which has made crimes and other related offenses to be on the increase in the country. The impact of cyber threats on Nigeria was assessed to include the possibility of indirect or direct attacks that can work against the state or private sectors. The challenges of combating cybercrimes were also highlighted. These include lack of funding, poor training, lack of infrastructure, and cyber strategy, among others.

Adewunmi Falode[xi] posits that Nigeria has an active and expanding presence in cyberspace, with critical sectors of the economy relying on access to cyber technology. He argues that the presence of cyber threats necessitated the development of the national cybersecurity strategy in 2014. A review of the national cybersecurity strategy was done with the prevailing dynamics of the Nigerian situation. The study examined international conventions on cybersecurity, international law and its effect on national security as it relates to cybersecurity to conclude that a strong cybersecurity policy is not just a tool for

national security but also economic prosperity and this is because cybersecurity protects every sector of the Nigerian economy.

Nigeria's National Security Strategy

Nigeria's national security strategy provides the direction for the protection of the Nigerian people and territory. To understand this strategy well, it is important to study the concept of national security and its interpretation in the Nigerian context. The definition of national security that will be adopted comes from the grand strategy document developed during the administration of President Olusegun Obasanjo in the year 2004. National security is defined "as the aggregation of the security interest of all individuals, communities, ethnic groups, political entities and institutions in the territory of Nigeria''[xii]. This can be interpreted to mean the protection of all Nigerians and institutions within the territory of Nigeria irrespective of their affiliations. The 2014 national security document identified two critical threat areas: the national security interests[xiii], paying close attention to the security and the welfare of the people in areas such as sovereignty and defense of territorial integrity and so on. In the areas of threats to national security, they included terrorism, organised crimes, kidnapping, cyber threats[xiv] and so on. The document further identifies sectorial strategies, which the national strategy relies on and is derived from the grand strategy. The sectorial strategies were developed as a response to the threats to national security. The sectorial strategies include national defense policy, national counter-terrorism strategy, national policy on public safety and security and national cybersecurity strategy. The national cybersecurity provided a framework of guiding principles and action plans to address cybersecurity threats[xv].

The national security strategy of 2019 was an update of the 2014 document. The vision and mission of the new policy document can be summarised as ensuring the security of Nigeria and the prosperity of its people, while the mission is to ensure physical and human security using all strategic means to ensure peaceful co-existence, national unity, prosperity and ensuring the promotion of Nigeria's interest across regional, continental, and global affairs.[xvi]

The 2019 national security strategy objectives are summarised as protecting the Nigerian people and territory, promoting economic prosperity and sustainable development, promoting national and peaceful co-existence, and enhancing regional and international interests. The document identified security threats in contemporary times which include terrorism and violent extremism, armed banditry and kidnapping, transnational organised crime, porous borders and cybercrimes, technology challenges and many more[xvii]. It is important to state that the sectorial strategies developed in the 2014 policy document are also used as a response mechanism for threats identified by the 2019 document.

Understanding Nigeria's Cyber Security Strategy

Cyber security became prominent in Nigeria in 2014 with the development of the first-ever national policy document. The national cybersecurity strategy, as it was called, was developed by the Office of the National Security Adviser upon the realisation that cyberspace has become an essential component of 21st-century activities.
The understanding that critical and non-critical activities are increasingly migrating to cyberspace and state actors' response to protect state and private sector assets and critical infrastructure from state and non-state actors from threats and attacks prompted cyber security in Nigeria.[xviii]

The 2014 policy document on cybersecurity recognises cyberspace as an indispensable global domain coming after land, air, sea and space, particularly with the increase in states' dependency on information and communications infrastructures in governing societies, conducting business, exercising individual rights on interactions and freedom of communication[xix]. Cyberspace allows for open interactions with no defined boundary as in the case of the other domains, and this allows both state and non-state actors, including violent ones, to use cyberspace for their selfish and destructive purposes. The document identified cyber threats in Nigerian cyberspace, including cybercrime, cyber-espionage, cyber-conflict, cyber-terrorism, child online abuse and exploitation, which the policy seeks to tackle. The national doctrine on cybersecurity was an integral part of the 2014 policy document and its goal was to provide needed framework to counter cyber threats of all kinds[xx]. As stated by the 2014 document, the vision and mission of cybersecurity are summarised as a safe, vibrant, and trusted community providing opportunities for its people to safeguard national assets and interests to ensure peaceful interactions and proactive engagement in cyberspace for national prosperity. The mission was to provide harmonious, sustainable, integrated national cybersecurity readiness and coordination to counter cyber threats[xxi].

The new policy document on cybersecurity developed in 2021 is an update to the 2014 document. The update was required to provide a better-structured policy to meet the new threats faced by Nigeria and provide context for cybersecurity to meet up with global standards regarding the framework to counter threats. The 2021 document was borne out of understanding the realities of Nigeria being a leading digitally connected nation, ranking 57th in the global cybersecurity index, and the outbreak of the COVID-19 pandemic and the presence of new threats, making the document timely and strategic.

The new threats identified by the new policy document include pandemic-induced cyber threats, election interference, and online gender exploitation, with

previous threats already identified in the 2014 policy document include online child abuse, cybercrime, cyber terrorism, and a host of others[xxii]. The new policy on cybersecurity provides the national doctrine which rotates around the protection of the citizens national and private key infrastructures. These will be done by providing safe and secure cyberspace without restrictions on the rights of citizens and private organizations[xxiii]. The new policy document provides a national cybersecurity direction, paying attention to national objectives, which include protecting national security, strengthening economic development, and fighting corruption. It also contains four fundamental national cybersecurity considerations: security and well-being, cybersecurity and economic development, technological development, and regional and international collaboration. There are also eight pillars of strategic focus.

These include governance and coordination, legal and regulatory framework, cyber-defense capability and monitoring and evaluation[xxiv]. The priorities of the 2021 policy are directed at the preservation of Nigeria's sovereignty, territorial integrity, and human security, and ensuring we uphold regional and international laws around cybersecurity.[xxv] A comparative study of the 2014 and 2021 policies on cybersecurity has been done to have an in-depth understanding of cybersecurity policy in Nigeria.

The Impact of National Cybersecurity Policy and Strategy on National Security

The grand strategy document of 2000, developed under the administration of President Olusegun Obasanjo, provides the foundation for a policy document on national security in Nigeria, while Nigeria's national security strategy of 2014 was able to identify sectorial strategies which are important to the actualisation of the national security strategy.[xxvi] One of the four sectorial strategies is the national cyber security strategy developed to provide frameworks and guidelines for combating cyber threats/attacks against Nigeria. The various cyber threats already identified have made it imperative for Nigeria to develop a robust cyber security policy and strategy particularly in the era of cyber warfare, cyber espionage, and even cyber terrorism which the country is susceptible to as it has fought terrorism in the last 12 years.

The strategy's development has helped protect key national critical infrastructures and private assets as Nigeria is fully embracing the digital economy, which translates to the reality of all our sectors moving away from a manual system to a digital system. Every area of the Nigerian economy has been digitalised to protect government and private assets from threats/attacks which will, in turn, hamper the ideology of national security, which is to protect the Nigerian people and territory, irrespective of affiliation.

Challenges of National Cybersecurity Policy and Strategy to National Security

We have established the importance of the national cybersecurity policy to national security and cannot ignore the obstacles that stand in the way of achieving the policy's purpose for national security. The implementation of the policy is one of the greatest challenges to national security, which is a common problem in Nigeria. The framework is available. Unfortunately, Nigeria finds it hard to put machineries in place to ensure the policy is fully activated. The reasons for this are not far-fetched and, in this case, the lack of proper funding structure to provide required facilities and manpower. The actualisation of the policy will require the purchase of state-of-the-art equipment and the employment of industry experts in participating government agencies. Funds must be set aside from the defense budget to provide the required needs to build a robust system to implement the policy.

Another major challenge is the lack of inter-agency collaboration to implement the policy. All hands must be on deck to achieve the common goal of protecting the Nigerian people and territory. The office of the National Security Adviser, which is the coordinating centre, must ensure everyone plays their role and share vital intelligence and data to ensure the policy is properly put into action and its objectives achieved. International collaboration should be encouraged without compromising national integrity and sovereignty.

Conclusion

This work examined the importance of the national cybersecurity policy and its proper implementation for national security. Nigeria considers cyberspace an important domain that can alter her national security interest with the abundance of threats identified in the national cybersecurity strategy, particularly cyber warfare, cyber espionage, and cyber terrorism, to mention a few. The work also studied the synergy between the national security policy and national cybersecurity policy[xxvii] to help give a better insight into the impact of the policy on national security. National security cannot be achieved effectively if national cybersecurity is ineffective in countering threats posed to the Nigerian state. Finally, the cybersecurity policy looks good theoretically but requires all available resources to see its implementation practically. It requires comprehensive funding and, most importantly, the availability of experts and collaborations among agencies.

ENDNOTES

[iv] Office of the National Security Adviser (ONSA), *National Cybersecurity Policy*, (Abuja: Government Printers,2014)
[iv]Brig. Gen (rtd.) Saleh Bala, Dr Emile Ouedrago, *National Security Strategy: Nigeria Case Study (Working Paper),* (Abuja: Africa Centre for Strategic Studies, 2018), 1-7
[iv] *Ibid.*
[iv]ONSA, " *Nigerian National Security Policy*",(Abuja: Government Printers, 2014)
[iv] ONSA, *National Security Strategy,(*Abuja: Government Printers, 2019)
[iv] ONSA*, National Cybersecurity Policy*, (Abuja: Government Printers, 2014)
[iv] ONSA, *National Cybersecurity Policy and Strategy*,(Abuja: Government Printers, 2021).
[iv]Babayo Sule, Bakri Mat, Usman Sambo, Mohammed Kwarah Tal and Muhammad Aminu, "Cybersecurity and Cybercrime in Nigeria: The Implication on National Security and Digital Economy", *Journal of Intelligence and Cyber Security*, Vol. 4, 1-35
[iv] Denis. N. Baken, *Cyber Warfare and Nigeria's Vulnerability*, Available at https://www.e-ir.info/2013/11/03/cyber-warfare-and-nigerias-vulnerability/on/february,22,2022,10.32p.m, Accessed on 22-02-2022, 1-7
[iv] Idowu Bobade Yusuf, "Cyberthreats and National Security in Nigeria", *NDC Journal, Vol. 13*, No.2 https://ndcjournal.ndc.gov.bd/ndcj/index.php/ndcj/article/view/133 accessed on February 22, 2022, 10.31pm. pp. 148-159
[iv] Adewunmi J. Falode, *Cybersecurity Policy in Nigeria : A Tool for National Security and Economic Prosperity*, Available at https://ebrary.net/173537/political_science/cybersecurity_policy_nigeria_tool_national_security_economic_prosperity on March 27, Accessed on 22-02- 2022, 9.30am
[iv]Brig. Gen (rtd.) Saleh Bala, Dr Emile Ouedrago, *National Security Strategy: Nigeria Case Study (Working Paper)*,(Abuja: Africa Centre for Strategic Studies, 2018), 2
[iv] *Ibid*. 3
[iv] *Ibid*.
[iv] *Ibid*. 4
[iv] ONSA, *National Security Strategy*, (Abuja: Government Printers, 2019), xvii
[iv] *Ibid.* 8-12
[iv] ONSA, National *Cybersecurity Policy*, (Abuja: Government Printers, 2014), 7
[iv] *Ibid.* 7

[iv] *Ibid.* 8
[iv] *Ibid*. 13
[iv] ONSA, *National Cybersecurity Policy and Strategy*,(Abuja: Government Printers, 2021), 3
[iv]*Ibid.* 13
[iv] *Ibid.* 5
[iv] *Ibid*. 10
[iv]Brig. Gen (rtd.) Saleh Bala, Dr Emile Ouedrago, *National Security Strategy, Nigeria Case Study (Working Paper),* (Abuja: Africa Centre for Strategic Studies, 2018), 3