REVISITING NIGERIA'S NATIONAL DEFENSE POLICY FOR A SECURED CYBER DOMAIN IN THE 21ST CENTURY

Mubarak Ahmed Mashi[1]
Aliyu Mukhtar Katsina[2]

ABSTRACT

This paper interrogates Nigeria's cyber domain regarding the Nigerian National Defense Policy. The paper argues that the change in global politics, the rise of non-state actors, as well as the proliferation of small and light weapons (SALWs), which have been largely facilitated by advancements in technology and globalization, have combined to alter the nature of security threats. Hence, there is a strong need for alteration in the Defense Policy of Nation states to accommodate the variation in threat perception and analysis, to deal with the challenges of the 21st Century security environment. The paper reveals that Nigeria's security environment has undergone a lot of transformations, following the end of the Cold War, with its attendant implications for the Nigerian National Defense Policy (2006), as presently framed, failed to make adequate provision for addressing 21st-century security challenges facing the country, particularly, in the area of cyber warfare. The paper recommends among others an encompassing approach, which views national defense from both military and non-military perspectives; that the Nigerian government should embark on an endogenously inspired technological advancement program that will enable her to develop a robust technological base, which is a vital imperative in the 21st Century security environment, and that the Nigerian Armed Forces, which is the most critical instrument in the discharge of her defense policy and

[1] Mubarak Ahmed Mashi is a Lecturer in the Department of Political Science, Umaru Musa Yar'adua University (UMYU), Katsina, Nigeria. ahmed.mubarak@umyu.edu.ng

[2] Dr Aliyu Mukhtar Katsina is of the Department of Political Science, Umaru Musa Yaradua University (UMYU), Katsina, Nigeria. Aliyu.mukhtar@umyu.edu.ng

objectives, be retrained and reoriented, to pave way for the requisite cyber competences needed to equitably discharge their responsibilities.

Key Words: Cybercrime, Defense, Policy, Security, Warfare.

INTRODUCTION

In recent times, the change in global politics, the rise of non-state actors, who now challenge the State which hitherto had sole control over the instrument of force, and the proliferation of Small Arms and Light Weapons (SALWs), as a result of their availability at cheap prices in the black market, which has been largely facilitated by advancement in technology and global interconnectedness. These have combined to alter the object and subject of security, as the individual became the object of threat much more than the State. This has brought a shift in the national defense paradigm. Therefore, there is a strong need for alteration in the Defense Policy of Nation states to accommodate this alteration in pattern to deal with the challenges of the 21st Century security environment (Ayegba and Yerima, 2017).

In light of the foregoing, this paper interrogates Nigeria's cyber domain, concerning the Nigerian National Defence Policy and cyber warfare in the 21st Century. To achieve this objective, an analysis of the concept of national security and defense transformation will follow the introduction and merge into an analysis of the concept of cybercrime/cyber warfare. A synopsis of Nigeria's 21st Century cyber domain will precede an examination of the issues and challenges of cybercrime in Nigeria. Lastly, we shall proffer some strategies on how to overcome the challenges of cyber warfare in the context of defense policy transformation in the 21st Century. The conclusion will be a summary of the chapter.

CONCEPTUAL ISSUES

National Security

There exists significant confusion in the security literature regarding the connotation of security. The realist belief perceives security initially in military terms, and thus gives states priority. They suggest that,

protecting their territorial integrity must be number one in the minds of national leaders and that, security is essentially the freedom from fear of attack by another country or non-state actors/terrorists. Therefore, armed aggression should be a foremost security priority/concern for states. Furthermore, for states to be secured, they must prepare for war to prevent war; states must prepare for war to keep the peace. This should be every state's supreme obligation above any other security concern. Thus, safeguarding the state by military force matters most (Kegley and Blanton, 2010). To the realist, security must be well-defined primarily in terms of each country's capacity to resist armed threats to its survival and national values by either external enemies or insurgents at home. This perspective elevates the protection of entire States' interests above those of individuals.

According to Carey (2000), security is a strange phenomenon, a subjective "feeling" and therefore relational and relative, rather than an objective "thing" that can be handled. You cannot touch security; you can only feel secure. Therefore, if security is something that can only be felt, it must be secured from something – a threat. For the state, the most obvious threat is that of invasion from another state, while for the individual, it could be a threat of hunger, disease, physical violence, torture, and terrorism among others. For Lippmann (1944), national security is the capability of a country to protect its core values, both in terms that a state need not sacrifice core values in avoiding war and can maintain them by winning the war. In the discipline of International Relations (IR), the term means "national security" or the protection of a state from external threats. This meaning emerged from the practice of international politics after the First World War. The term may convey more general meanings including the safety of individuals from violence or crimes, religious peace of mind, and financial measures to sustain a certain standard of living.

Defense Policy

Baylis (1977) views defense policy as a concept that is freely used by laymen and analysts alike, but its true meaning is hardly defined with accuracy. Be that as it may, however, he argued, the term incorporates

a wide range of activities, some of which are stressed in some uses of the term and some others in diverse ways. Katsina (in Alabi, 2011), posits that national defense policy is the policy directed at coordinating all required human and material resources to resist an attack from a hostile neighbor or enemy. Also, it involves the procedure of developing the weapons system, training, and deployment of personnel to actualize defense objectives, which are the preservation of territorial integrity, sovereignty, and strategic interests. Bassey stated that defense policy is both a dynamic and complex process and offered a definition of defense policy thus:

> The defense policy of a country implies the overall tendencies principles that underlie the provision, deployment, and use of military capabilities to facilitate the "protection, and the pursuit of the perceived national interests of the state". Such "national interest" may concern armed forces, economic, political, or ideological values of one kind or another. They may also concern intangible objects, such as the territorial integrity of the State. Thus, to the extent that foreign policy objectives are outward-directed (that is, concerned with "acquiring something of core value desired by international actor", then there are fundamentally no [principles of concern to states that do not directly or indirectly impinge on considerations of military power calculus (Bassey, 2011:3).

Furthermore, Fwa (2011) opined that defense in strategic terms is the sum of the deployment of a nation's resources to authenticate its territorial and sovereign independence; while as a concept of war, it means the application of military means to fend off direct attacks on a nation by an invading force. At the heart of the defense objective, therefore, is the projection of the core values of Nation states. Thus, to avoid chaos on the international scene, Nation states need a defense policy to secure their core values.

The Nigerian National Defense Policy (NNDP), comprises the philosophy and objectives of the country's defense policy. The NNDP's philosophy is as follows;

i. The Nigerian state is paramount and is the guarantor of the security and well-being of the people;
ii. The Nigerian state is an important player in international politics, particularly in Africa; hence certain responsibilities are expected from her;
iii. The armed forces are the most critical instrument of Nigeria in the discharge of her responsibilities, at both domestic and international levels;
iv. The security of the state is the primary focus of the defense policy (National Defense Policy document, 2006: 4,9, and 12).

No doubt, the above thinking serves as the driving force behind Nigeria's defense policy, intending to protect her national interests, as provided in the constitution; and therefore, shapes her defense policy objectives which include among others, the following:

i. Protection of Nigeria's sovereignty, citizens, values, cultures, interests, resources, and territory against external threats;
ii. Provision of defense as well as strategic advice and information to the government;
iii. Promotion of security consciousness among Nigerians;
iv. Participation in disaster management and humanitarian relief operations at home and abroad;
v. Ensuring security and stability in the West African sub-region through collective security;
vi. Participation in bi-lateral and multi-lateral operations; and
vii. Contributing to international peace and security (National Defense Policy document, 2006: 22-23).

From the foregoing, it is obvious that the major objective of any nation's defense policy is to equip the nation with the capability to guarantee the protection of her territorial integrity, national interest,

political values, economic resources as well as social values within her domestic environment and in the international system.

Defense Transformation

In military terms, a transformation has a broader and more encompassing meaning, hence, it is subjected to different interpretations amongst the different military services within a country; and from one national armed force to the other. The concept has its protagonists and usefulness in the United States, but its objectives are being practiced globally in distinct ways, propelled by diverse motivations. The meaning and scope of transformation, and particularly defense transformation, have been viewed variously by different scholars. Defense Transformation was defined by the 2001 Quadrennial Defense Review Report (QDR) thus:

> Transformation results from the exploitation of new approaches to operational concepts and capabilities, the use of old and new technologies, and new forms of organization that more effectively anticipate new or still emerging strategic and operational challenges and opportunities and that render previous methods of conducting war obsolete or subordinate. Transformation can involve a fundamental change in the form of military operations, as well as a potential change in their scale. It can encompass the displacement of one form of war with another, such as fundamental in the ways war is waged in the air, on land, and at sea. It can also involve the emergence of new kinds of war, such as the armed conflict in new dimensions of the battlespace (in Dombrowski and Ross, 2008:15-16).

Markov (2009:526) defined defense transformation as "a process of shaping the future warfare, development, and use of armed forces. It is not an attempt to predict what will happen. It is a well-planned development and combination of circumstances leading to the desired

change". Markov went further and outlined a few very vital points on defense transformation which are enumerated below:

i. Defense transformation is a profound, revolutionary change that is not an option but a requirement for an organization to be successful and to be one step ahead of other rivals;
ii. It is a process, not an end state. And this process is future-oriented and affects the entire organization, its policies, and structures at all levels. Hence, it requires a broad approach, which goes beyond the armed forces and includes other non-military components of society and the international community;
iii. Being future-oriented, defense transformation is not an attempt to adapt the organization to the possible changes in the environment, but to shape future warfare, and to make changes happen in the way we want them to happen;
iv. Shaping the future and the acquired advantage is due to the development of new concepts or a combination of new concepts; and
v. To conduct and win a war, we need military capabilities including technology, appropriately educated leaders, trained units, adequate equipment, organization, and operating procedures.

In this paper, defense transformation is defined as a revamp in the defense policy, military strategy, and military doctrines of a Nation-state; to alter the conduct and operation of its armed forces through training, to cope with the contemporary challenges of the 21st-century security environment. It is an approach meant to marry both military and non-military components of security together, thereby, enhancing robust and encompassing national security.

Cybercrime

According to Parker (1998), cybercrime is any intentional and malicious activity associated with computers as objects, subjects, instruments, or symbols in which a victim suffers a loss and a perpetrator make, or may have made, a gain. This view focuses largely on the consideration of gains and losses associated with cybercrime incidences and limits the type of actions that are criminalized under cybercrime. Sofaer (2013) views cybercrime as a criminal activity perpetrated by individuals or syndicates involving Information Communication Technology (ICT) infrastructure and the internet networks such as phishing theft, manipulation of data, hacking, and Electronic Commerce (e-commerce) fraud. This includes unauthorized damage, deletion, deterioration, alteration, or suppression of computer data. This view is comprehensive as it identifies key attributes like hacking, electronic commerce (e-commerce) fraud, and other interferences in cyberspace which undermines the smooth operation of national defense and security, in the 21st-century security domain.

Cyber warfare

Cyber warfare is a form of cybercrime that is defined as the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military. However, the problem with cyber warfare is that it's very hard to work out who launched the attack in the first place. In most cases, nobody will want to claim responsibility for attacks (IT Pro, 2019).

AN OVERVIEW OF NIGERIA'S 21ST-CENTURY NATIONAL SECURITY DOMAIN

Nigeria, like most nation-states, is not immune from the contemporary challenges that have emerged in the post-Cold security international environment. Zabadi (2011), stated that Nigeria's security environment is distinguished by five symbiotic overlapping layers of manifestations of security weaknesses and threats. He analyzed these levels with the aid of a concentric circle and contented that, security threats and vulnerabilities that exist or originate from the innermost layer (people),

when ignored or insufficiently addressed, can move as far as undermining the security environment of the outermost layer (international security). Equally, security threats and vulnerabilities that exist or emanate from the international level, when ignored or insufficiently addressed, can move as far as undermining the security environment of individuals (people) in a state such as Nigeria. Globalization and increasing interdependence of states now meant that security challenges that are localized can become transnationalism or internationalized overnight. This is the epistemic context that frames our understanding of Nigeria's security environment (Zabadi, 2011:89). The Nigerian state is facing several threats from non-state actors within and outside of its national boundaries. Oloru (2014) observed that Nigeria has the highest percentage (70%) of illicit arms in the West African sub-region. It is these Small and Light Weapons (SALWs) in civilian hands, that have continued to fuel and sustain the activities of violent non-state actors such as the Boko Haram, al Qaeda, and ISIS cells in the sub-region. The combined activities of these terrorist groups have continued to threaten Nigeria's territorial integrity. Also, the activists of transnational organized crime groups, have gained so much attention in recent times. Their activities range from money laundering, human trafficking, cybercrimes (yahoo-yahoo), advanced free fraud (otherwise known as 419), and drug trafficking, among others (United Nations Office on Drugs and Crime, 2010). The association of some Nigerians in these criminal activities has continued to damage the image of Nigeria and Nigerians in the comity of nations. There is no doubt that the forces of globalization have aided the perpetration of these transnational crimes, as it has fueled the global flow of arms, while at the same time, helping to erode the power and legitimacy of the state.

Another form of threat that has emerged in the contemporary security environment, is the phenomenon of climate change. According to the Intergovernmental Panel on Climate Change (IPCC), Africa is already experiencing the negative effect of climate change. Nigeria, like most African countries, has a low adaptive capacity. Consequently, climate change affected Nigeria's security by complicating the effects of other sensitive issues such as poverty, unemployment, and health

issues, etc. (Zabadi, 2011:94). The consequence of climate change in Nigeria includes among others, extreme poverty, frequent natural disasters, deforestation, desertification, resources scarcity, and depletion of the ozone layer. All these manifestations, which are mutually reinforcing, work to undermine Nigeria's security.

The Boko Haram violence in 2009, affected five northern states and witnessed the death of hundreds of people and the destruction of properties worth millions of naira. However, the sect has since transformed into a terrorist organization, which targets both Muslims and Christians, leaving in its wake, casualties too numerous to count. From the kidnapping of school girls, from their dormitory, in Chibok town and Dapchi, to the declaration of the so-called Islamic caliphate, which witnessed the sacking of several communities in Borno, Yobe, and Adamawa state, with the attendant displacement of approximately 1.8 million people (Umar, et al, 2014). The internal displacement of millions of people, the resultant hunger and humanitarian crises; and the ongoing counterinsurgency and counterterrorism operations in northeast, Nigeria by the Nigerian Armed forces, speaks volume of the immensity of the security challenges, facing the Nigerian state.

A major fallout of communal clashes and ethnoreligious crises is the rising number of Internally Displaced Persons (IDPs) in the country. According to the United Nations Higher Commissioner for Refugees (UNHCR) to Nigeria and the Economic Community of West African States (ECOWAS), the number of IDPs in Nigeria, as of November 2016, stood at 2,093,030. No doubt, IDPs constitute both security and development challenges, as scarce resources needed for developmental projects are committed to catering to them. Similarly, IDPs constitute a burden on their host communities, as they exert huge strain on infrastructure and resources, are susceptible to violent crimes such as rape, human trafficking, and robbery; and are equally exposed to health hazards due to the often-poor sanitary conditions in the IDP camps.

Furthermore, contemporary security threats emanating from the international system such as terrorism, transnational organized crimes, climate change, and global economic recession, among others; though far away from Nigeria, have a direct impact that is felt in the country,

especially in a globalized world. For instance, the economic recession has resulted in increasing restructuring and downsizing in our local banks and industries, and the outright closure of some of our industries. The resultant laying off of staff has further aggravated the problem of unemployment and poverty level, fueling frustration and privation, and has led several youths into criminal activities, thuggery, insurgency, and militancy in Nigeria (Umar et al., 2014).

Similarly, the changing nature of warfare as a result of globalization and the attendant technological advancement, vis-à-vis Nigeria's technological base, has further aided in the drastic transformation of Nigeria's security environment. Rapid technological advancement has brought about a change in the nature and character of warfare. War has now assumed an asymmetric dimension, where the battlefield has been largely transmogrified into a battle space, with a much wider landscape, which includes among others, cyber warfare/cybercrime, Net-Centric Operations, and Net-Centric Warfare. As a result of these changes, the enemy is not known, and surprise, though an old weapon of war, has assumed even more relevant tactics of warfare. This development largely accounts for why the Counter Terrorism and Counter Insurgency Operations in the northeast have become protracted (Dala, 2011).

From the foregoing, it is evident that Nigeria's security environment has undergone a lot of transformations, following the end of the Cold War, with its attendant implications for national security. Unfortunately, the Nigerian National Defense Policy (2006), as presently framed, failed to make adequate provisions for addressing 21st-century security challenges facing the country, particularly, in the area of cyber warfare. Hence, there is a need for defense transformation to adequately secure Nigeria's cyber domain.

CYBER WARFARE AND NATIONAL SECURITY IN NIGERIA: A LINKAGE ANALYSIS

Advancement in technology leading to increasing interconnectedness has made the world a global village. Thus, the security domain of most nations of the world is accessible through cyberspace, which is a global

infrastructure that facilitates information exchange among nations, firms, and persons. Unfortunately, the growth in application and reliance on digital networks has been accompanied by illicit activities such as cyber warfare (Bright, 2012). Hence, cyber warfare directly impacts national security, which is the sum of a nation's efforts to protect and preserve the state, its institutions, and the well-being of its citizenry. As governments, businesses, and financial institutions continue to adopt Internet-based systems, the spread of cyberwarfare has increasingly inhibited economic and social development and by extension, national security. Accordingly, cyberwarfare perpetrated by states and non-state actors through attacks on computer networks, especially within the security sector is of grave concern for national security in the 21st century (Ibikunle, 2013).

The evolution of cyber warfare in Nigeria dates to the early 1980s, with the advent of facsimile machines which facilitated digital communication. Facsimile machines connected to fixed telephone lines were used by fraudulent individuals to send scam letters to unsuspecting victims. These attacks gradually evolved into large-scale cybercrimes, using cyber channels. The liberalization of the telecommunication sector led to increased internet penetration in the security sector, and an increase in cybercrime ranging from 4 percent in 1985 to 28.3 percent in 2000. Accordingly, as the growth in internet penetration continued, government institutions, businesses, and financial institutions adopted Internet-based systems, which exposed them to cyber warfare (Ibikunle, 2013).

In Nigeria, the drive towards a cashless economy and electronic commerce led to an increase in reported cases of cybercrimes, from about 900 in 2000 to over 2,780 in 2015. Besides, Nigeria's Deposit Money Banks (DMBs) are estimated to have lost 203 billion to cybercrimes between 2001 and 2013. The situation is worrisome, as cybercriminals develop creative ways to undermine the existing national security measures. Thus, in a bid to address the threat of cyberwarfare in the country, the Federal Government of Nigeria (FGN), formulated the National Policy on cybercrime and enacted the Cyber Crime Act 2015 and the Nigerian Computer Emergency Response Team

(NG CERT), a response team to manage, secure and achieve safe cyberspace was also put in place.

Other policy instruments such as the National Security Strategy, and Nigeria Electronic Transaction Bill, were initiated to curtail cyber warfare and related crimes. In addition, other agencies include the Economic and Financial Crimes Commission (EFCC) and Office of the National Security Adviser (ONSA) – the lead agency saddled with the responsibility to deploy specialized skills and infrastructure for curtailing cyber warfare. Despite these efforts, illicit cyber activities in the country have not abated (Zabadi, 2013). There has continued to impact negatively on national security and the financial sector, as an acute gap in cyber infrastructure and facilities continues to exist, as evident from incessant cyber-attacks and network failures in many security institutions. In fact, some of Nigeria's national security institutions are not even connected to an internet network. So, how do they contribute to the fight against cyber warfare?

However, there are several issues arising from the prevalence of cyberwarfare in Nigeria's security domain. Some of these include the absence of a robust regulatory framework. For instance, the Nigeria Cyber Working Group (NCWG) was dissolved in 2007 and has not been replaced (Ojabo, 2014). This created an institutional lacuna in the area of checking and enforcement of guidelines/regulation on cyber transactions in Nigeria. Similarly, the Cybercrime Advisory Council established under the Cybercrime Act 2015, has not made a significant impact either. The body functions alongside the ng cert under the Office of the National Security Adviser (ONSA).

Furthermore, the processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access are essential to secure the cyber space. Enhancing cyber security and protecting critical national information infrastructure, are crucial to the economic wellbeing of the nation. This becomes more relevant today, as most cyber-attacks in Nigeria are perpetrated within the financial sector. These include hacking, cracking of security codes for electronic transactions, Automated Teller Machines (ATM) cards and Electronic Marketing (e-marketing) product

sites. This situation is so, as only 20 percent of online businesses in Nigeria can contain cybercrimes, while 80 percent are vulnerable. Thus, the deficit of standard ICT infrastructure has constituted a major setback in the protection of the cyber domain in Nigeria against cyber-attacks (Ojabo, 2014).

Inter-agency coordination efforts are essential to curbing cyber warfare. It is vital to translate policies into desired outcomes. It facilitates synergy among institutions, organs, and agencies that are involved in combating cyber warfare in Nigeria. However, the fight against cyber warfare is plagued by weak interagency coordination. For instance, Section 41(1) of the Cybercrime Act 2015 tasked the ONSA as the coordinating body for all security and enforcement agencies involved in fighting cybercrime in the country. Yet, the coordination and enforcement to combat cybercrimes are equally supervised by NG CERT, which is domiciled in the ONSA. Similarly, the EFCC was established to investigate financial crimes such as advance fee fraud also known as "419" and money laundering. This results in a clash of responsibility and the attendant weak coordination, which has become the lot of these institutions. Thus, creating an avenue for cyber criminals to strive by leveraging the weak coordination among security agencies (Muogillim, 2014; Rosenthal, 2016).

This paper argues that the current situation of Nigeria's cyber domain could be attributed to the failure of defence policy makers to recognize the nexus between national security and cyber warfare, which is reflected in the failure to make adequate provisions to cater to this menace in the National Defense Policy document. It is the apparent recognition of this gap that has necessitated the remedial measures taken by the FGN, as stated above. However, this gap has created a situation, where remedial measures being put in place by successive governments in Nigeria, have so far failed to secure the nation's cyber domain.

REVISITING NIGERIA'S NATIONAL DEFENSE POLICY FOR A SECURED CYBER DOMAIN

Current trends in defense policy analysis, suggest an encompassing approach, which views national defense from both conventional military and nonconventional non-military perspectives. Hence, defense transformation entails the handling of both dimensions with equal vigor and attention, as the changing pattern of the international security environment, has shown that, the strategy towards national defense in the 21st Century goes beyond conventional military doctrines in isolation. Without any fear of contradiction, one can say that, Nigeria's national defence questions, are largely, non-military in nature and emanate from both the internal and external environment. Consequently, the paper calls for a revisit of the current Nigerian National Defense Policy (2006) in line with the following recommendations:

The Nigerian government should embark on an endogenously inspired technological advancement program that will enable her develop a robust technological base, which is a vital imperative in the 21st Century security environment. A coherent strategy for the protection of ICT infrastructure is a necessary requirement to curtail cyber warfare. The objective of the suggested strategy is aimed at identifying and creating an endogenously inspired technological base that will be difficult for foreigners to hack into without internal collaborators. It will also involve giving differential treatment for information systems infrastructure such as computer systems and network daily in sectors that are vital to the nations' security.

The Nigerian Armed Forces, is the most critical instrument in the discharge of her defense policy and objectives, at both domestic and international levels. We recommend education for defense transformation of the Armed Forces; this way, military personnel will be retrained and reoriented, to enable them to acquire the requisite competencies needed to equitably discharge their responsibilities. Thus, a planned strategic response that provides preparedness, capability for cyber offensive capability, and retribution for the Armed Forces of Nigeria is required to improve the fight against cyber warfare. The

NNDP could provide the necessary incentives and legal premises for the ONSA, the AFN, and other security agencies to act quickly and intelligently, when the need arises to defend the nation's security.

Furthermore, a coordinating body to harness interagency collaboration to combat cyber warfare is crucial in the defense and security sector. The establishment of such a coordinating body would mitigate the challenge of interagency rivalry among the agencies involved in minimizing cyber warfare. The objective is to achieve the objectives of the Cyber Act 2015. This would involve developing effective frameworks and interfaces for interagency collaboration in curtailing cyber warfare for enhanced national security. Besides, the NNDP should provide for the creation of the requisite technical capacity for the prevention and detection of cyber-attacks (a sort of early warning system), among law enforcement, security, and intelligence agencies. This would improve decision making towards preventing cyber warfare in Nigeria's security domain.

Additionally, a standard reporting procedure is germane to resolving cyber warfare in Nigeria. The NNDP should harmonize standard reporting procedures for cyber warfare offences, to ensure uniformity at all reporting institutions. The FGN could leverage on the FBI C1 reporting platform to establish a convenient and easy-to-use reporting mechanism that alerts authorities to sustained criminal violations in the cyber space. This would build confidence and erode suspicion among agencies as well as encourage reporting for procedure for adoption by all stakeholders.

Conclusion

This paper has attempted to unveil the essential linkage between Nigeria's cyber domain and Nigeria National Defense Policy in the light of the changing international security environment, occasioned by the demise of the Cold War. We have outlined these changes and the threats there pose to Nigeria's cyber domain. We submit that, the Nigerian National Defense Policy has not adequately captured how cyber threats directly affect the Nigerian people. This loophole has therefore left a void that ought to be filled.

REFERENCES

Alabi, D.O. (2011). Defence policy, military professionalism, and the development question in Nigeria. In Mbachu, O. and Yesufu, M.L. (Eds.). *Contemporary strategic studies: Theoretical perspectives and policy options* (pp.169-202). Medusa Academic Publishers Ltd.

Ayegba, S.B. and Yerima, H. (2017). Defense and security with human face: Human security and defense transformation in Nigeria". In Tar, U.A. (Ed.). *Defence transformation and the consolidation of democracy in Nigeria* (pp. 351-366). Academy Publishers Ltd.

Bassey, C. (2011). Defence policy discourse. In Bassey, C.O. and Dokubo, C.Q.(Eds.). *Defence Policy of Nigeria: Capability and Context* (p.3). Author House.

Baylis, J. (Ed.). (1977). *Defence policy in a changing world*. Croom Helm.

Bright, M.S. (2012). Cyber world and the challenges of the developing world. *Journal of International Studies,* 4 (17), p.15.

Carey, R. (2000). The contemporary nature of security. In Trevor, C.S. (Ed.). *Issues in International Relations*. Rutledge.

Dala, M.B. (2011). Defense Transformation: Challenges for the Nigerian Military. In Mbachu, O. and Sokoto, A.A. (Eds.). *Nigerian Defense and Security: Policies and Strategies* (pp. 379-396). Medusa Academic Publishers Ltd.

Dikongue, A.A. (2016). Nigeria has 2,093,030 IDPs. https://allafrica.com/stories/201611210151.html

Dombrowski, P. and Ross, A. L. (2008). The revolution in military affairs, transformation, and the defense industry security challenges, 4. (4). https://www.regionalsecurity.org.au/Resources/Files/vol4no4DombrowskiandRoss.pdf.

Fwa, K.L. (2011). Towards evolving a defence and security policy for Nigeria: Challenges in the 21st century. In Mbachu, O. and Yesufu, M.L. (Eds.). *Contemporary strategic studies: Theoretical perspectives and policy options.* (pp.99-120). Medusa Academic Publishers Ltd.

Ibikunle, F. (2013). Estimating the global cost of cybercrime economic impact of cybercrime ii report summary. Vol. 3(1). http://www.mcafae.com/us/resources/reports/rp-economic-impact-cybercrime2-summary.pdf.

IT Pro (2019). What is cyber warfare. https://www.itpro.co.uk/security/28170/what-is-cyber-warfare.

Kegley, Jr., C.W. and Blanton, S.L. (2010). *World politics: Trends and transformation (Int'l Ed.)* Wadsworth.

Lippmann, W. (1944). U.S. foreign policy. Hamish Hamilton.

Markov, Z. (2009). Educational aspects of defense transformation. *AARMS,* 8 (3), 525-537. http: //www. zmne.hu/aarms/volume8/issue3/pdf/13mark.pdf.

Muogilim, N.A. (2014). Cybercrime and national security in Nigeria: An appraisal. Research Project submitted at the National Defence College, Abuja, Course 22, June 2014.

Nigerian National Defense Policy (NNDP). National defence policy document (2006). Pp. 4,9,12,22-23.

Ojabo, D. (2014). Cybercrime: A threat to e-banking adoption in Nigeria. *Business Day,* 21 September, 2014. P. 21.

Oluro, M.J. (2014). Arms proliferation and insurgency: The case of Boko Haram in Northern Nigeria. https://www.academia/.../Arms_Proliferation_and_Insurgency.

Parker, B.D. (1998). *Fighting computer crime: a new framework for protecting information.* John Wiley and Son.

Richards, O. (2016). CSEAN wants more education to tackle cybercrime menace. *The Guardian Newspaper,* 19 August, 2016. http://guardian.ng/ng/business-services/csean-wants-more-education-to-tackle-cybercrime-manace.

Safaer, A.D. (2013). Cybercrime and security: The transnational dimension. Hoover Press.

Umar, A., Nmodu, A., Oyoyo, I., Benjamin, I. and Kareem, H. (2014). Nigeria: Gwoza under siege-Boko Haram kills 300, wipes out three villages. https://allafrica.com//00037184.html.

Zabadi, I. (2013). The national security and decision-making process in a democracy. In Mbachu, I.O., and Bature, U. (Eds.). *Internal*

security management in Nigeria: A study in terrorism and counter-terrorism (p.546). Medusa Publishers.

Zabadi, I. (2011). Nigerian defence and security environment. In Mbachu, I.O. and Sokoto, A.A. (Eds.). *Nigerian defence and security: Policies and strategy* (pp. 84-112). Medusa Academic Publishers Ltd.