*Global Journal of Applied, Management and Social Sciences (GOJAMSS); Vol.20, September 2020; P.90 – 101 (ISSN: 2276 – 9013)*

# AN ASSESSMENT OF CYBER SECURITY THREATS AND THE NATIONAL SECURITY QUESTION IN NIGERIA

**NATHANIEL OLUWASEUN**
**Department of Political Science and Public Administration,**
**Babcock University Ilisan-Remo,**
**Ogun-State, Nigeria**

**&**

**OLAWOLE OJO**
**Department of Political Science and Public Administration,**
**Babcock University Ilisan-Remo,**
**Ogun-State, Nigeria**
**Corresponding e-mail: ojool@babcock.edu.ng**

## Abstract

*This paper is to assessed cyber security threats and the questions of national security in Nigeria. This was borne out of the growing cyber security threats such as kidnapping, calculated murder, theft, terrorism and other vices that has evolved in relation to the increasing use of internet solutions in the country. The paper argued that identifying the nature of cyber security threats and its effect on national security is crucial to identifying options for mitigating the cyber security threats facing the nation.*

*To this end, the methodology adopted for the collection, analysis and interpretation of relevant data was developed after review of the extant of literature. Specifically, the survey research design was adopted with an interview of 6 key informants from selected security organisation using the convenience sampling method. After review of the qualitative data, the findings of the research support the conclusion that cyber security threats significantly affected national security. The same formed the basis for the recommendations of the paper.*

**Key words: National Security, Cybersecurity**

## Introduction

With the rising wave of terrorism and global conflict, national security is a topical issue that cannot be relegated to the background. The concept of security remains ambiguous, creating room for conflicting discourse on the subject matter. Prior to the 21st century, McSweeney (1991) acknowledged the difficulty in defining the context of security which he stated was an elusive term that resists scholarly definition in spite of the recurrent use of security in multiple contexts and heterogeneous circumstances. What could, however, be taken as a contemporary insight into the nature of security was advanced by Bourne (2014) on the axiom that security relates to the protection of individuals or nations from threat, survival of an entity and being absolved from any form of harm caused by a second or third party. These remain a critical underpinning to national security, a concept which emerged after the Second World War and has changed with the pace of international relations development.

The state cannot be said to function effectively without a comprehensive security architecture which covers the military aspect of security at the national level. All these support the assertion of Burgess (2008) who claimed that the state is the primary provider of security. With the recent advancement in terrorist propaganda and the increasing volatility of internet users and facilities to attack, the need for assessing national security towards preserving and protecting the national interest of the people comes to the table (Baylis and Smith, 2001). Of course, Nuechterlein (1976) remains correct to note that national security is the only sustainable and efficient means of protecting the local and international interest of a nation.

The Nigerian Information Communication and Technological (ICT) landscape has rapidly evolved over time, giving individuals and the government the platform to interact, share information and coordinate all manner of the transaction which has now been supported by the electronic platforms. In a report by the Nigerian Communication Commission (NCC, 2018), over 98 million Nigerians are now active internet users. This from the current population estimate of 180 million strongly suggests that 44.44% of the citizens are now on the internet. To further match the data, a recent survey by Oliveserah Business and Academic Concept on the eGovernment Performance of 312 Ministries, Departments and Agencies of the Federal Government of Nigeria revealed that nearly 90% of government agencies now have functional electronic channels. Even though the report shows that electronic functionality, quality of service and issues of security are poor, the fact remains that government and the citizens are now functioning within the global cyberspace (Oliveserah BAC, 2018). The growth in the number of internet users, citizens and government inclusive could have influenced national security in undesirable ways.

The threat posed by the internet became a significant research issue from the late 1990s and have thus far emerged as an issue of national importance today (Boniface et al, 2014). Cyber threats which are set of criminal activities perpetrated through the proliferation of ICT windows have become increasingly difficult for governmental and non-governmental agencies to deal with. Suffice to note that this is not only a challenge peculiar to developing economies such as Nigeria. There is an ongoing debate on the role of Russia in hacking into the American Electoral system while issues relating to the hacking of Sonny system remain fresh in the cybersecurity discourse. With developed economies facing the same threat, one begins to wonder what changes developing economies have in mitigating the threat posed by the new cyber world.

Without a sustainable, far-reaching and proactive response to this threat, there are potentials for cybercriminals to go beyond hacking of government website to stealing and leaking security information that may be detrimental to the existence of the country. Worst still is the reality of Boko Haram and other elements which are avowed enemies of the state. The access of such criminal elements to intelligence due to the cyber breach could spell doom for the country. What appears to be a challenge in tacking the threat of cybersecurity in Nigeria appears to be a lack of strategic focus on addressing the threat. In Reyes (2007), the global approach has always been segmented along the lines of legislation and legal enforcement on one hand and enhancement of forensic capabilities of security agencies. Within this framework of intervention, Nigeria has not been able to find the most appropriate strategy, talk more of identifying the nature of the cyber threat that is most likely to affect the nation's security in the short, medium and long-term. Therefore, this paper seeks to critically assess the implication of cybersecurity threats and the national security question of Nigeria. Cyber security threat is a major threat to national security in Nigeria. The Nigerian security landscape is becoming more complex with the threat of terrorism on the geographical front and cyber threat which is fast emerging to complicate the already worsened threat of economic, social and political insecurity in the country. Globally, it is recommended that countries conduct a routine assessment of its security threats, especially cybersecurity threat (Akinsuyi, 2009) which constitute internal and external threats to the country's national security. Interesting as this sounds, there is a little-known effort towards reviewing the myriad of potential cyber threats which when not addressed may expose the country to serious national security crises which may throw the country into jeopardy. These possibility and other issues further noted herein formed the critical motivation for the research.

**Objectives of the Study**

The objective of the research is to assess cyber security threats and national security questions in Nigeria. In this research, the focus is to:

1. Identify the current threat of cyber security in Nigeria.
2. Examine how the current cyber security threat could affect national security.
3. Propose solution to the cyber security threats to national security in Nigeria.

## Research Question

1. What is the current threat of cyber security in Nigeria?
2. How does the current threat of cyber security affect national security in Nigeria?
3. What could be done to solve the cyber security threat to national security in Nigeria?

## Literature Review

### Concept of Cyber Security

The cyber space is made up of the internet, but also other information systems that support Government, businesses, infrastructure and services. Security refers to the degree of resistance to or protection from harm according to Wikipedia. It is a topical issue globally that is given priority among all other social issues because without security it is difficult to make any substantial social improvement The concept of security is applicable to any vulnerable and valuable asset such as people, homes, community, organizations or nations. Security refers to a measure that is employed to ensure peaceful coexistence and development at large (Adebayo, 2011). When adequate security is put in place according to Adebayo, there will be an absence of fear, threat, anxiety, tension and apprehension over the loss of life property, freedom, properties, values and ideals.

Building on the above, we can consider national security from David Baldwin (1997) perspective that national security concentrates on the preservation of acquired values and not on the absence of threats. To Arnold (1952), it refers to some degree of protection of values previously acquired in a nation-state. National security can be defined both in its objective and subjective sense; objectively, it is the measure of the absence of threats to acquired values while in its subjective sense national security means the absence of fear of such values being attacked.

The concept of cybersecurity is not very clear because there is no universally accepted definition of the concept. It has been relatively used in various sectors such as political, military, industrial and economic spheres. Scholars today consider all these aspects in their attempt to give a definition to the concept of cybersecurity. As expected, the definitions have become more holistic. Cybersecurity is related to many other aspects of security. The relationship between cybersecurity and other aspects of security can be understood through certain terms. According to Von Solms and Van Niekerk (2013), cybersecurity can be defined as the protection of cyberspace, the electronic information it contains, the Information Communication Technologies (ICT) which supports it and those who make use of cyberspace. The goal of cybersecurity is to ensure that the security properties of the organization and user's assets are maintained security-wise, the general security goals are made up of the availability, integrity, and confidentiality of information across cyberspace (ITU, 2008). For Brechbhl et al (2010), cybersecurity is essentially about managing future risk and responding to current and past incidents and attacks.

### Nature of Cyber Attack

Cyber-attack takes the form of a syntactic, semantic or blended attack which combines both (Choo, 2011). The syntactic attack takes advantage of technical vulnerabilities in both software's and hardware's to commit a crime which may be to install malware on systems to steal data. Semantic attacks focus on social vulnerabilities to have access to personal information such as scam solicitations and online fraud (auction). Social engineering is a form of online psychological manipulation that involves an attacker misleading an individual into revealing sensitive information in order to gain access to a system. There are two categories of cyber-attacks and they are; malicious software attacks and Denial of Service (DOS). Below is a discussion on the two categories of cyber-attacks:

**a. Malicious Software (malware) attacks**

Any software that brings harm to a computer system and its user refers to the malicious software. Hackers work earnestly to build new techniques that can be employed to take advantage of vulnerabilities. This includes exploitative systems such as Ransom ware which is used to extort sensitive information from individuals (Schreier, 2012; McAfee, 2011).

### b. Denial of Service (DOS) attacks

Denial of service in the report of Techopedia (2014) occurs when a hacker attempts to prevent a legitimate user from accessing the service. This form of attack does not change, modify or destroy system resources but they affect a system by diminishing the system's ability to function properly. They can bring down a system without destroying its resources (Kizza, 2014).

## Theoretical Framework

### The Securitization Theory

The broadening of the security debate brought about the securitization theory. This school of thought was developed by scholars from the Copenhagen school, following the fundamental ideas of security in relation to survival. An issue that involves security is one which constitutes an existential threat to the survival of the referent object (Peoples and Vaughan-Williams, 2010). As such, a referent object is an entity or a state that is under threat and that needs protection. An existential threat to a referent object can, therefore, be said to be a security issue. When an issue constitutes a security issue and is a threat, it is justified to adopt extreme political measures to handle it (Peoples and Vaughan-Williams, 2010). This means that the issue is securitized. The process of an issue being securitized starts from it first being politicized and when it escalates it is considered as securitized. This implies that political actors with legitimate authority by means of speech acts can initiate securitization. The speech act theory stands out here as a very important concept for the Copenhagen school. In clear views, Abrahamsen (2005) notes the possibility to analyze the social construction of security issues by evaluating the corresponding securitizing speech acts which are the legitimate way of representing and recognizing threats. Security, when mentioned by a representative of the state, moves a specific development into an area and by so don claims a unique right to use whatever means required to block such threats. When an individual or institution with a certain level of authority can perform an action or function by saying certain words or phrase. These speech acts are known as performatives and merely uttering the words accomplishes a social act (Peoples and Vaughan-Williams2010).

For performative-utterances to be effective, it must meet certain conditions which are; it must be said by someone in a position of authority, it must be said in the right context and it must follow the established rituals or formulas. If it follows these conditions, the speech is said to be fictitious and the speech act is considered as successful. In the same vein, securitization abides by a general mode of operation which requires acceptance between the state representatives (the agent of the securitization speech) and the relevant audience that the speech applies to which is often the citizens of the state. In this regard, Peoples and Vaughan-Williams (2010) stated that threats and vulnerabilities have to be existential threats to a referent object by a securitizing actor who through that generates approval of emerging measures beyond rules that would otherwise bind. This makes securitization a political choice to conceptualize an issue in a certain way (Abrahamsen, 2005). National security has an unimaginable power when invoked as an instrument of social and political mobilization. For securitization to be effective, an audience which is in most cases the citizens of the state has to accept the fact that a threat is credible. In addition, three factors are also considered as critical for the accomplishment of a speech act, they increase the tendency for the success of securitization. These conditions include:

1. An existential threat is presented as legitimate the use of extraordinary measures in curbing the threat.
2. That the securitizing actor is in a position of authority and has the socio-political capita to convince the audience of the existential threat.
3. That the objects related to the issue have historical connotations of threat, danger or a history of previous hostile sentiments (e.g. rival states in competition) (People and Vaughan-Williams, 2010).

It is noteworthy that even though the conditions outlined are necessary for a successful securitization, none of them is sufficient enough to actualize a successful securitization. In a bid to assess the impact of cyber security threat to the Nigerian National security between 2011 and 2017, the securitization theory created a baseline for the research. The existential threat of cyber insecurity and its impact on the Nigerian people which could be referred to as referent object invariably indicates the existence of security threat in which this theory makes room for its redress through the identification of the securitizing actor (the internal and external cybersecurity threat) and development of strategies to block such threats. This would therefore be essential to effectively addressing the research questions.

That notwithstanding, there has been criticism of the securitisation theories which are herein reflected. Clara (2018) criticised the notion of security in the securitization theory on the premise that security is a relative term which depends on the context in which it is applied. True to this, what could be security in the context of developing countries may not resonate with the security narrative of the developing economies, hence some loopholes in the theory. Rita (2006) had faulted the limitation of the scope of security to action and the activities of agents but noted that security is a holistic concept which also covers the rule of law, policies and processes regarding how security is to be achieved in a given context. Sarah et al (2015) was resolute that the securitization theory may have clearly itemised the evolution of security complexes in any system but were concerned that the theory did not show whether the evolution has an end or not and it does not provide a clear roadmap for resolving security threat issues. More so, it is difficult to tell if the theory is a best fit for cybersecurity threats or not. Stephane and Catarina (2017) countered Sarah et al (2015) criticism by arguing that the securitisation theory covers diverse issues including cybersecurity but in Stephane and Catarina (2007) assertion, the theory rather fail to provide an indicator as to what factors can be considered as security threat and which are not.

## Methodology

The research was based on the survey research design which is effective for generating primary data from relevant segment of the population for the purpose of achieving the research objectives (Creswell, 2009).

The population for the study included Information Technology Companies and Security Companies in Nigeria. The purposive sampling method was selected for identifying relevant IT companies and Security organizations were invited to take part in the research towards assessing cyber security threat and its implication on the national security question.

The data was collected from the Key Informant using the already defined instrument through an interview. Depending on the consent, availability and preference of the key informant to be engaged, the interview was conducted physically, through phone call, and chat. The response from the key informant was thereafter sorted out and analysed in line with the framework for data analysis.

Since qualitative data will be generated for the purpose of the research, a qualitative inclined method of data analysis was used to draw meaning from the data generated from the key informant. In this regard, the content analysis method was used to analyse the feedback from the interview. That is, the data from the various key informants was organised into themes and form the basis for review to determine where there were similarity and contrast in the views advanced to establish the general position from the response.

**Data Presentation and Analysis**
**Demographics of Key Informant**
**Table 1**
A total of 6 key informants took part in the research. Their profile is summarised below.

| **Key Informant Identification Code** | **Sector** | **Experience** |
|---|---|---|
| KI1 | Information Technology | He is the CEO of an information technology firm involved in networking, system engineering, and software development |
| KI2 | Information Technology (IT) | He is an IT expert working in a software engineering company with over 5 years of experience. |
| KI3 | Information Technology (IT) | He is an IT consultant and researcher with experience in system security. |
| KI4 | Security Company | He is a security personnel working in a leading security firm in Nigeria. |
| KI5 | Security Company | He is a Security Expert and a Lawyer with a specialty in strategic security management. |
| KI6 | Security Company | He is a security personnel with a paramilitary security agency in Nigeria. |

Source: Field Survey (2019).

**Concept of Cybersecurity and National Security**

KI1 states:

> *Cybersecurity has to do with the computer and computer-related items such as network, networking and servers, keeping them safe from unwanted access, keeping them from the reach of those people you don't want to have access to it. National security has to do with keeping things safe in Nigeria, lives, properties, etc, keeping them safe from unwanted access.*

It is rather expressed by KI2 thus:

> *Cybersecurity is straight forward, it stands for security issues or matters relating to the internet and its facilities, how people connect to the internet and also connect the system over the cyberspace. National security is anything within the space of protecting, handling, managing and securing the nation which also envelopes cybersecurity because there is part of government activities that are connected and linked via the cyberspace including to international companies. It relates to the nation in general and the institutions.*

KI3 rather shared the same view:

> *Cyber Security is like policies and checks to secure the cyberspace including the internet and cloud services. National security could be physical, including securing the lives of human and animals.*

KI4 expressed the following opinion:

> *Cybersecurity is the protection of all online activities from fraud or malfunction. While national security is maintaining a country's territorial integrity including sensitive security information*

In addition to the foregoing, KI5 opined as follows:

> *Cybersecurity deals basically with the protection of identities, data's, information about ourselves, others or a particular set of people on the world wide web and National Security implies doing everything possible to safeguard, protect, the life and properties of a citizens of a particular nation or country even if it is inconvenient for them at that moment.*

KI6 rather had the following view about the concept.

> *Cybersecurity has to do with not being threatened on the internet space while national security is not being threatened given a particular geographical location let say a country.*

**Identification of Cyber Security Threats in Nigeria,**

KI1 identified the threats as follows:

> *Of course, there are cybersecurity threats. The world is now a global village and the virtual space (internet) is now merging such that what is happening in virtual space is happening in real life; activities taking place in the net now have repercussions on the human being in real life. People are being chatted-up on Facebook to come to a particular location where they get robbed or lose their lives. People banking details online and on employment sites which expose their information. This is not only so for Nigeria but other countries that are using I.T.*

For KI2, the threat is noted thus:

> *Cybersecurity has become very keen and I don't think anybody or any organization is not affected, so I can say yes. Take a look at the case where Russians had access to information from the US and I think that is possible in Nigeria even in countries where security is not yet a priority so I believe some stakeholders would have been affected.*

KI3 shared this perspective about the threat:

> *I won't say there is cybersecurity threat in Nigeria, rather Nigeria is a cybersecurity threat to other countries. That is, in the case of Yahoo-Yahoo that is all over the place; people do that for a living.*

KI4 rather stated:

> *Yes, there are cybersecurity threats in Nigeria. The current threat includes: we are not aware that we are being threatened; lack of adequate laws to tackle cybercrime in the country; failure to adequately implement existing laws; high level of poverty.*

Lastly, KI6 was of the following viewpoint:

> *Yes, our cybersecurity is been threatened. Threat to personal life threat to government institutions threat to private organizations and a threat to our personal freedom.*

**Impact of cyber security on National Security in Nigeria,**

KI1 identified the impact as follows:

> *Of course, just like earlier noted, what happens on the net (site, computers and IT gadget) is happening in real life. For example, the banking sector is strongly engaging internet for their service which is making life easier for everybody and the banks. The boundary between cyber security and national security is so thin that you cannot separate them; it is the people in the nation that are operating on the virtual space so whatsoever happens on the cyberspace has significant impact on national security since there is no clear bother to say this is where cyberspace stops and national security stops.*

KI2 also shared the same view.

> *Yes, I think cybersecurity can affect national security. Some organization that might hold weight in terms of contributing to the country GDP may be exploited by hackers and that will affect the growth of the economy. For example, in China they ensure that their cyberspace is secured to the extent that connecting to website in China might be blocked off because they know how this will affect them at the national level. So I will say it depends; it is very easy that if you can penetrate a nation's cyberspace, you can manipulate whatever information you need and you can cause as much havoc as physical security.*

KI3 identified the impact and expressed it in the following ways:

> *Yes, it can in a way, as fraudsters see cybercrime as a means to survive not knowing that it is actually theft and when they can't go through with the yahoo-yahoo, they turn to carry guns and robbery which is a mind thing.*

KI4 was as resolute as others, expressing this view as follows:

> *Yes, it can affect national security because when people are defrauded online especially when huge sums of money is lost, businesses fail, unemployment increase and crime grow. A very high crime rate constitute a threat to national security, for example, banditry in the northwest of Nigeria.*

KI5 was also instrumental in this regard and noted as follows:

> *Yes, it can; most kidnapping issues is due to leakage of personal data of citizens on the internet; terrorism by Boko Haram in Nigeria is also a product of cybersecurity threat; not from a verifiable source, but the just concluded Nigeria Election, 2019 also have some element of cyber crimes in play.*

In addition to the above, KI6 was of the foregoing view:

> *Cybersecurity and national security are inseparable even though they are different; cybersecurity plays a great role in national building and as such, it affects national security. Cyberspace has help aid terrorism in many nations. In Nigeria, cyber threat ranges from online fraud popularly called yahoo-yahoo, infringement on people's private lives via social media, aided terrorism, for example, Boko haram, breaking into government database, and also fraudulent hacking into financial institution database giving way to easy money laundering. Also, I'll give another example. When a medical database is hacked into, it ends up producing hazardous population figure of a country's population. Also, investors lose interest in investing in an economy with lose financial database.*

**Interpretation**

The research generated insight into critical cybersecurity threats in Nigeria. These threats includes the killing and robbery induced by social media platforms, vulnerability of the country to external cyber security attacks which can be viewed in the context of manipulation of computer system by other countries to cause havoc in the internal economy thereby crippling institutions (Gercke, 2011; Kizza, 2014; Serianu, 2014). It was also observed that part of the impact of cybersecurity on national security in Nigeria includes the decline in the volume of GDP due to the constant attack on companies and sectors with significant contribution to the GDP thereby causing a huge loss in government revenue with implication on security spending.

**Conclusion**

From the findings of the research, it was noted that the current cybersecurity threats in Nigeria includes the incessant killing and robbery induced by social media platforms, the vulnerability of the country to external cyber security attacks, prevalence of cyber crimes such as scams and frauds (yahoo-yahoo), high vulnerability due to poor awareness about cybersecurity threats, the lack of relevant regulatory laws and poor implementation of existing laws. Also, the high level of poverty and continuous threat to human life, personal freedom and institutions were observed.

In line with research objective two, the impact of cyber security threat to national security was observed to include; declined in the volume of GDP due to attack on critical companies which results in low security spending, the manipulation of security information to cause physical havoc, spillover effect of cybercrimes on robbery and increase in crime rates. Other impact observed includes kidnapping and worsening pace of terrorism, the negative impact on election malpractices, money laundering and lack of confidence in the economy.

It is further concluded in relations to research objective three that the way out to preventing cybersecurity risk and its impact on national security includes the development of a culture of proactive screening of the cyberspace to detect threat and establishment of agency to ensure fulfillment, the use of technologies to improve cybersecurity and a significant improvement in the level of national awareness on the threat, education and training.Improvement and enactment of other cybersecurity laws and prosecution of offenders and rehabilitation of cybercriminals and utilizing them to clamp down on the cybercrime wave were also identified as strategic solutions.

From the foregoing, the research concludes that cybersecurity threats are prevalent in the Nigerian system and it has a significant negative impact on national security.

**Recommendations**

1. Based on the identified Cybersecurity threat in line with Research Objective 1, there is a need for greater awareness on the cyber-security threats in Nigeria.

2. Since some effects of cybersecurty threat on national security has been noted in line with Research Objective 2, there is a need for instituting a Proactive cyber-security mitigation agency.

3. From the observed mitigation measures as identified in line with research objective 3, the government of Nigeria needs to focus on the improvement and enactment of relevant laws.

4. Also in line with objective 3, there is a need for effective collaboration between the arms of government

5. In addition to the findings of research objective 3, more emphasis should be placed on Licensing and Regulation of IT companies

**References**

Abrahamsen, R. (2005). 'Blair's Africa: The Politics of Securitization and Fear'.*Alternatives: Global, Local, Political, 30*, 55-80.

Achumba, I., Ighomereho, O., &Akpor-Robaro, M. (2013). Security challenges in Nigeria and the implications for business activities and sustainable development. *Journal of Economics and Sustainable Development, 4*(1), 23-29.

Adebayo, A. (2011). *Democratic elections and Nigeria's national security*. Ibadan: John Archers.

Akhakpe, I. (2012). Election crisis, liberal democracy and national security in Nigeria's fourth republic. *European Scientific Journal*, *8*(2), 40-52.

Akinsuyi, (2009). *The drawing of Information Security Legislations, What Nigerian CorporationsCan Do to Prepare*. Retrieved from https://pdfs.semanticscholar.org/a060/99e8a545c94ac1e052b7b0e375b5822e40bf.pdf

Baldwin, D.A. (1997). The Concept of Security. *Review of International Studies*. 23(1): 5-26.

Baylis, J. and Smith, S. 2001. *The Globalization of World Politics: An Introduction to International Relations*. Oxford: Oxford University Press.

Baylis, J. and Smith, S. (2001). *The Globalization of World Politics: An Introduction to International Relations*. Oxford. Oxford University Press

Boniface et al (2014). Analyzing *Issues of Cyber Threats in Nigeria*. Retrieved from https://pdfs.semanticscholar.org/a060/99e8a545c94ac1e052b7b0e375b5822e40bf.pdf

Bourne, M. (2014). *Understanding Security*. London: Palgrave Macmillan.

Bourne, M. (2014). *Understanding Security*. London: Palgrave Macmillan

Brechbhl, H. Bruce, R. Dynes, S. & Johnson, E. M. (2010). Protecting Critical Information Infrastructure: Developing Cyber-security Policy. *Information Technology for Development, 16*(1), 83- 91.

Burgess, J. P. (2008). *Non-Military Security Challenges in contemporary security and strategy*. Houndmills: Palgrave Macmillan.

Buzan, B. (1991). *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. New York: L. Rienner Publishers.

Chinedu R. (2018). *SMEDAN Website Hacked*. Retrieved from https://itedgenews.ng/2018/09/13/smedan-website-hacked/

Choo, K. R. (2011). The Cyber Threat Landscape: Challenges and Future Research Directions. *Computers & Security*.30: 719- 731.

Eriksson, J. Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) relevant Theory? *International Political Science Review*. *27*(2), 221-244.

Geers, K. (2011). *Strategic Cyber Security*. NATO Cooperative Cyber Defense Centre of Excellence. Tallinn, Estonia.

Gercke, M. (2011). *Understanding Cybercrime: A Guide for Developing Countries*. Geneva: International Telecommunications Union (ITU). Retrieved from www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Gilbert, D. (2014). *Hacktivists Hit Back at Israel After Death of Anonymous Member in West Bank*. Retrieved from http://www.ibtimes.co.uk/hacktivists-hits-back-israel-after-death-anonymous-member-west-bank-1458623

Graham, J. Howard, R. and Olson, R. (2011). *Cyber Security Essentials*. Auerbach Publications: Taylor and Francis Group.

Guilmartin, J. F. (2013). *Reflections on the Revolution in Military Affairs.The RMA Debate*. Retrieved from http://www.comw.org/rma/fulltext/reflect.html#versus

Held, D., & McGrew, A. (1998). The end of the old order? *Review of International Studies, 24*(3), 219-242.

International Telecommunications Union (ITU). (2008). *Data Networks, Open System Communications and Security: Telecommunication Security: Overview of Cyber Security*. ITU-TX.1205: series X: Geneva: ITU.

Kesan, J. P. and Hayes, C. M. (2012). Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. *Harvard Journal of Law and Technology*, *25*(2), 417-527.

Kizza, J. M. (2014). Computer Network Security and Cyber Ethics. (4th ed). Jefferson NC: McFarland &Co Inc.

Klare, M. T. and Chandrani, Y. (1998). *World Security: Challenges for a new century*. (3rd ed). New York: St. Martin's Press.

Klimburg, A. (2012). *National Cyber Security Framework Manual*. NATO CCD COE.Talinn, Estonia.

Lewis, J. A. (2014). National Perceptions of Cyber Threats. *Strategic Analysis*. *38*(4), 566-576.

Lin, H. (2012). 'Some Modest Steps Towards Greater Cyber Security.' Bulletin of the Atomic Scientists. *68*(5), 2012.

McAfee.(2011). *McAfee Threat Report: Fourth Quarter 2010*. Retrieved from https://personalmacgeniuses.com/wp-content/uploads/rp-quarterly-threat-q4-2010.pdf

McSweeney, B. (1999). 'Security, Identity and Interests: *A Sociology of International Relations. Cambridge*: Cambridge University Press.

Neuneck, G. &Alwardt, C. (2008). The Revolution in Military Affairs, its Driving Forces, Elements and Complexity: Interdisciplinary Research Group on Disarmament, Arms Control and Risk Technologies. *Institute for Peace Research and Security Policy*. University of Hamburg.

Nuechterlein, D. E. (1976). 'National Interests and Foreign Policy: A Conceptual Framework for Analysis and Decision-Making.*' British Journal of International Studies*. *2*(3), 246-266.

Ogbonnaya, M, &Ehigiamusoe, K. (2013). Niger Delta militancy and Boko Haram insurgency: Nationalsecurity in Nigeria. *Global Security Studies*. *4*(3), 11- 25

Oliveserah BAC (2018). *2018 eGovernment Performance Index Survey*. Retrieved from https://drive.google.com/file/d/1X4_kMD8lY6BS-t87Q3sx6Gi7Am0pqzMo/view

Oriakhi, D., &Osemwengie, P. (2012). The impact of national security on foreign direct investment in Nigeria: an empirical analysis. *Journal of Economics and Sustainable Development. 3*(2), 18 – 44.

Peoples, C. and Vaughan-Williams, N. (2010). *Critical security studies: An introduction*. London: Routledge.

Reveron, D. S. (2012). *Cyber Challenges and National Security: Threats, Opportunities, and Power in a Virtual World*. Baltimore, MD: Georgetown University Press.

Reyes, A. (2007). *Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors*. Rockland: Syngress.

Rezk, D. (2010). *The Revolution in Military Affairs and the Changing Nature of Warfare in the Middle East*. Retrieved from http://blogs.lse.ac.uk/ideas/2010/04/the-revolution-in-military-affairs-and-the-changing-nature-of-warfare-in-the-middle-east/Accessed. 9 April 2013.

Romm, J. (1993). *Defining national security: The non-military aspect.* New York: Council of Foreign Relations Press.

Saleh, A. (2010). Broadening the Concept of Security: Identity and Societal Security. *Geopolitics Quarterly*. *6*(4), 228-241.

Schreier, F. (2012). On Cyber Warfare. *DCAF Horizon 2015 Working Paper*. *7*(2), 4-8

Serianu.(2014). '*Kenya Cyber Security Report. Rethinking Cyber Security – An Integrated Approach: Processes, Intelligence and Monitoring.'*Nairobi.

Sofaer, A. D. Clark, D. Diffie, W. (2010). *Cyber Security and International Agreements.* Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy.

Techopedia.(2014). *Definition of Denial of Service (DoS) Attack*. Retrieved from http://www.techopedia.com/definition/24841/denial-of-service-attack-dos.

United Nations Institute for Disarmament Research (UNIDR). (2013). *The Cyber Index: International Security Trends and Realities*. Geneva, Switzerland.

Von Solms, R. & van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*. *10*(1), 1- 6.

Weng Loo, B. F. (2005). Transforming the Strategic Landscape of Southeast Asia. Contemporary Southeast Asia. *A Journal of International and Strategic Affairs*. 27(3), 388-405.

Wolfers, A. (1952). National Security as an Ambiguous Symbol. *Political Science Quarterly*. *67*(4), 481-502.