CYBER THEATRE A FIFTH DOMAIN OF INTERNATIONAL POLITICS: AFRICA AND THE REST OF THE WORLD IN THE CYBERSPACE

RESEARCH ARTICLE

R. A. Lukman Adewale QUADRI
National Institute for Policy and Strategic Studies (NIPSS)
Kuru near Jos, Plateau State. Nigeria
mvdwallay.quadri@gmail.com
ORCID: 0000-0002-1352-030X
Monsuru Olaitan RASAQ
Pan African University for Governance, Humanities, and Social Sciences (PAUGHSS)
olaitanmonsuru19@gmail.com
ORCID: 0000-0002-3849-1234

Gönderim Tarihi: 24.09.2020 Kabul Tarihi: 02.12.2020
Alıntı: QUADRI, L.A. & RASAQ, M. O. (2020). Cyber Theatre a Fifth Domain of International Politics: Africa and the rest of the world in the Cyberspace. AHBV Akdeniz Havzası ve Afrika Medeniyetleri Dergisi, 2(2),98-111.

ABSTRACT: The cyberspace has now become a space theatre that enshrines activities such as cyber strategy, cybersecurity, cyber defence, and cyberwar. The cyberspace is a realm likened to the global arena where involved or interested actors are spurred by one interest or the other. The challenge in such a realm is the lack of a central authority to enforce order. This explains why the cyberspace will remain an arena of cyberwar since no state nor individual has a monopoly over the internet. Issue of anonymous identity in the cyberspace has proven to be a challenge without a solution in sight as trojans and cyber-actors infiltrate national Cyber Securities. However, national cybersecurity has made success in identifying the source or location of a cyber-threat or attack, but identifying the attacker or hacker remains something difficult. It is because cyber warrior has perfected the art of hiding their identity during cyber-attacks. However, there are success stories of some cyber warriors being identified and incarcerated by security operative; this remains scanty. The cyberspace is a double-edged sword at the individual unit, state and global levels. Cyberwar can only come to an abrupt opt when morality becomes a norm. Cyberwar is a means to an end in the hands of cyber-actors. China, Russia, North Korea, Iran, America, terrorist networks, individuals, investors, universities, companies, and other stakeholders have prioritised the use of cyberspace due to its efficiency and accuracy. The cyberspace has presented itself to humanity as a viable alternative to land, water, and space. Nevertheless, the African continent use of the cyberspace is defensive but not strategic; the strategic use of the cyberspace can serve as an ancillary to the fulfilment of core national interests. The Western, Asian and American axes are indulged in the strategic use of the cyberspace.

Keywords: Cyber; Cybersecurity; Cyberattack; Cyberwar; Cyber-strategy; Cybercrime; Cyber-army

Cyber-Théâtre Un Cinquième Domaıne De La Politıque Internatıonale: L'Afrique et Le Reste Du Monde Dans Le Cyberspace

RESUME: Le cyberespace est désormais devenu un théâtre spatial qui consacre des activités telles que la cyber-stratégie, la cybersécurité, la cyberdéfense et la cyberguerre. Le cyberespace est un domaine assimilé à l'arène mondiale où les acteurs impliqués ou intéressés sont animés par un intérêt ou un autre. Le défi dans un tel domaine est le manque d'autorité centrale pour faire respecter l'ordre. Cela explique pourquoi le cyberespace restera une arène de cyberguerre puisqu'aucun État ni individu n'a le monopole d'Internet. La question de l'identité anonyme dans le cyberespace s'est avérée être un défi sans solution en vue alors que les chevaux de Troie et les cyber-acteurs s'infiltrent dans les Cyber Securities nationaux. Cependant, la cybersécurité nationale a réussi à identifier la source ou l'emplacement d'une cyber-menace ou d'une attaque, mais l'identification de l'attaquant ou du hacker reste quelque chose de difficile. C'est parce que le cyber-guerrier a perfectionné l'art de cacher son identité lors de cyber-attaques. Cependant, il existe des exemples de réussite de certains cyber-guerriers identifiés et incarcérés par un agent de sécurité; cela reste maigre. Le cyberespace est une épée à double tranchant aux niveaux de l'unité individuelle, de l'État et du monde. La cyberguerre ne peut aboutir à un choix brutal que lorsque la moralité devient une norme. La cyberguerre est un moyen de parvenir à une fin entre les mains des cyber-acteurs. La Chine, la Russie, la Corée du Nord, l'Iran, l'Amérique, les réseaux terroristes, les particuliers, les investisseurs, les universités, les entreprises et d'autres parties prenantes ont donné la priorité à l'utilisation du cyberespace en raison de son efficacité et de sa précision. Le cyberespace s'est présenté à l'humanité comme une alternative viable à la terre, à l'eau et à l'espace. Néanmoins, l'utilisation du cyberespace par le continent africain est défensive mais pas stratégique; l'utilisation stratégique du cyberespace peut servir de complément à la réalisation des intérêts nationaux fondamentaux. Les axes occidental, asiatique et américain se livrent à l'utilisation stratégique du cyberespace.

Mots-clés : Cyber, La cyber-sécurité; Cyber-attaque; Cyber guerre; Cyber-stratégie; La cybercriminalité; Cyber-armée

Introduction

The cyberspace has grown to the extent of triggering intellectual discourse within scholars' realm, political scientists, communication experts, multinational cooperation, nations, policy developers, and citizens at the bottom of the pyramid. Issues related to the cyber seem to be the nucleus of the national, organisation, and individual discussion due to the essential nature of the internet which made it a commodity whose importance is similar to the gift of nature such as water, air, and food. The use of cyberspace via internet in the contemporary world has proved beneficial to humanity at all levels; from the top of the hierarchy to the bottom, for one reason or the other. Before the emergence of the internet, fax, telephone, hardcopy documents and letters, and palpable or physical form of communication such as face to face chat were the dominant means of communication. But the ground-breaking innovation of the internet rendered some of the pre-modern means of communication obsolete. It reduced the relevance of modern ones such as postal mail, physical chat, and the excessive use of hardcopy documents. The introduction of the internet changed almost all conventional practices such as financial transaction, warfare, business, entertainment; in a nutshell, it triggered the explosion of Artificial Intelligence which subjected humanity to a situation which can best be described a double-edged sword. The laudable and gloomy aspect of the cyberspace accounts for the consciousness of cybersecurity, cyber defence, and cyberwar which occupies a vital space in national policy, and conventional forums since it is a development that is beneficial to the world and simultaneously poses challenges to the world. The contemporary world has now become a cyber-strategy theatre where states are individually and collectively crafting policies or strategies to mitigate the destructive use of the cyberspace. Against this backdrop, one can conclude that the cyberspace is anarchical, especially when viewed through a realist prism. The realist school of thought is glued to the assumption that the international community is anarchical due to the absence of a central authority to enforce an order. This view applies to the cyberspace, due to the lack of central authority capable of controlling the use of the cyberspace, and this has led to the emergence of cyber wars, scores of cyber strategies such as offensive and defensive approaches at the individual, unit, and global system level. The multiple threats posed by the use of cyberspace have subjected states to a burning desire to establish cybersecurity for the defence of digital infrastructure and curtail the protruding debilitating cyber war. Cyberwar would have appeared as a myth to many. Still, occurrences in the cyberspace between powerful actors in America, Eastern Europe, Africa Asia and other regions of the world proved the realness of cyberwar as a threat to internal and external sovereignty of states, especially to digital infrastructures which characterised the economic and political strengths of countries. This work aims to discuss cyber theatre, cyber strategy, and how the quest for cybersecurity has accelerated cyber defence and cyberwars. Central to the aim of this study is to answer the following questions; what threat does the unethical use of cyberspace pose to humanity and national sovereignty? How have states used the cyberspace for the advancement of national interest? Who are the actors in the cyberspace? Are African nations making strategic use of the cyberspace for the advancement of their national interests, respectively?

Conceptual Clarification

Cyber

Cyber is a prefix used for the description of physical activities linked with computer devices and the internet. For instance, in the 21st century, we have seen a surge in the use of cyber and computer-related tools and activities such as cyber-trade, cyber-communication, cyber-security, cyber-strategy, cyberwar, cyber-entertainment and cybercrime, cybereconomy, cyberbullying, webinar, cyber soldier, cyber-actor, and cybertutor. Cyber is concerned with anything that has to do with the internet; this means that the prefix cyber means internet of things. Any physical machine or activities connected to the internet is qualified to use the prefix 'cyber'. Cyber is anything involving, using, or relating to computer, specifically the internet (Cambridge University Press, 2020).

Cybersecurity

As illustrated above, the prefix 'cyber' denotes internet of things, meaning machine or physical activities linked to the internet. Therefore, cybersecurity means the censorship of the use or activities of the internet for the safety of information. Kaspersky defines cybersecurity as the censorship of computers, servers, mobile devices, electronic systems, networks, and data to pre-empt them from malicious attacks. Cybersecurity can be referred to as information technology security or electronic information security. It is a term applicable in multiple contexts, such as trade, politics, research, security, Intelligence, and production since central to them all is information (Kaspersky, 2020).

Cyberattack

Cyberattack is a strategic infiltration by an unauthorised individual or groups into the database of a nation, organisation or individual. A cyberattack could be politically or economically motivated. Kaspersky (2020) categorised cyberattack as a cyber threat and further maintains that it is politically motivated information gathering. Merriam-Webster (2020) defines it as an attempt to gain illegal access to a computer or computer system to inflict damages.

Cyberwar

Cyberwar is almost similar to cyber-attack; in that, it is unauthorised access of one country into the database of another country. Sheldon (2016), maintains that cyberwar, which is also known as cyber warfare is conducted from computers and internet linking them together, and is waged by states or their proxies against other nations. Cyberwars are usually waged against other governments and military networks to destroy, disrupt, take control of their devices or inflict pains. Cyberwars are also waged for cyber-espionage; this is often used for pilfering information. For instance, the U.S. justice recently accused China of Sponsoring two Chinese hackers who aimed to spy labs developing Covid-19 vaccines (BBC, 2020). Similarly, The race for COVID-19 antidote has triggered nuance of cyberwar as it was uncovered that China, Russia, and Iran as spies from the aforementioned countries targeted America biotech companies and research universities to pilfer data, according to a report of the American and British intelligence service (Lenthang, 2020).

Cyber-strategy

Cyber strategy differs from state to state; central to cyber-strategy is a national policy designed to mitigate cyber threats such as cyberwar, cyber-espionage and cybercrime, which poses a danger to national security. For instance, states of the world have strategies to pre-empt intrusion of hackers into their national database stored in the cyberspace. Each country has its National Cyber Security Strategy (NCSS) to obstruct unauthorised access to a national database. De Groot (2020), defined cybersecurity as measures established to protect networks, devices, programs, and data from attack, damage, or unauthorised use. Cybersecurity is equally information technology security (De Groot, 2020).

Cybercrime

It is an unethical use of the cyberspace, which is mostly targeted at individuals and organisations; central to cybercrime is the unlawful or unauthorised access to the repository or database of an organisation, or individual account to pilfer information of importance. Dennis (2020) defines cyber-crime also known as computer crime, as the use of computer for furthering illegal activities such as fraud, trafficking in child pornography, pilfering intellectual property, stealing identities, or invading privacy.

Cyber-armies

These are a section of the national troops whose activities are not on land, water and air, but in the cyberspace. Their actions are not directly visible but felt by the users of information communication technology. Cyber-armies are used chiefly for the protection of cyberspace, where states, corporations, and individuals have their repositories. They protect the country from cyberattacks launched by adversaries which could be other states, individual hacker or group hackers. Aschmann, Van Vuuren, and Leenen (2015:16), Defined cyber-army as a highly skilled information technology group of military personnel and civilians with a grave understanding of cyber skills and able to protect the military, state, national strategic infrastructures, and ability to launch cyberattacks.

Cyber Theatre as the Domain of Multifaceted Events

The significance of the internet in the contemporary world has led to the creation of an alternative world or realm where communication, transaction, agitation, coordination/strategies, and socialisation unfold; and this realm can be regarded as a cyber-theatre. It is a realm where physical activities or realities, and imaginations are transformed into the software which can be seen, and its effects felt in reality. It is a realm exploited by humanity in the contemporary world for various reasons such as mobilisation, coordination, dating, socialisation, database, research, financial transaction, governance and also military activities. Below are few extracted explanations of what a cyber-theatre is from the work of existing authors:

> “Dvizjenije aimed to involve the spectator both actively and totally in the event. Lev Nusberg, the initiator of Dvizjenije, describes cyber theatre as a model of the relationship between Machine and Man; so Cyber-theatre was a vision of man-machine symbiosis. It is the title and Nusberg's discussion point to the discovery of cybernetics, defined by Norbert Wiener in 1948 as the science of control and communication systems, in the animal and the machine (Chatzichristodoulou, n.d.).”

> "Twenty years ago, it was inconceivable for people to meet without a physical encounter. But today, as the web browser has become a cyber theatre – a proscenium stage with a kind of "performance-action" taking place in the cyberspace behind its arch. When you subscribe to a blog or follow a tweet, you are signing up to your first spectator's contract, which in time will be fulfilled with a subject in action. As Peter Brook puts it, a man walks across an empty space whilst someone else is watching him, and this is theatre. In the same manner, the basic formula of cyber theatre can be defined as such: a mouse is dragged along a standalone digital interface, performing a series of orders and events, whilst its first spectator, namely the operator in front of the screen, is watching it. As early as the Windows '98 era, virtual scenography has demonstrated how people use digital interfaces as a "stage," by changing wallpapers, icons, and mouse arrows. After inventing the mouse avatar, our contemporary Aeschylus created a second character for his tragedy, namely "My Computer," or "the little lion of ESM antivirus software." Eventually, the "Internet connection" moved cyber theatre out of the temple and turned it into a carnival for the masses. At first, cyberspace used reality as its playscript and emerged in the form of a theatre of imitation and reproduction. Later, with the introduction of Web 2.0, cyberspace started to evolve beyond a theatre of simulation into – in Baudrillard's terms – a field of "hyperreality." Eventually, with its "return to offline" (zaixian Xinhua: literally, “re-offlin(e)-ise"), the cyber theatre has substantiated itself as a space for public discourse with the mission to "reconstruct" collective imaginations. It is to say that cyberspace is translated into a template (a play script) for reality to alter and update itself, to achieve a theatricalised society of "hyper-hyperreality eventually." This circular process occurs continuously and scattered across time-space; wherein cyber theatre represents the online rehearsal for a series of offline performances. These repeated rehearsals are the trial and error of future possibilities, and the preparation for positive interventions into reality. Hence, cyber theatre is defined by the action of actors (persons-in-action) who apply new rules and change the order of the cyberspace; it differs from cyber drama, which uses cyberspace only for literary expression (Xiaoxing, 2017).”

The above extracts elucidated the concept of cyber theatre from a 20th and 21st-century perspective. The 20th century perspective of the cyber theatre was focused on cybernetics which deals with the control and communication in the animal and machine; this explains how the interplay between human and visual digital technology began. The 21st-century elucidation of cyber theatre is quite advanced in that it encompasses control of any system of communication using technology, or the interplay between human, technology, and communication. Human communication through technology has gone beyond audio and visual digitalisation to graphical, textual, audio and visual digitalisation exchange, making the cyberspace more realistic and relevant to humanity across the globe. For instance, in the contemporary world, we have seen scores of activities performed in the cyber theatre ranging from cyberwar to cyber business meetings, cyber entertainment, cyber businesses, and cyber political campaigns. The emergence of COVID-19, for example, proved the significance of the cyberspace to humanity as activities on land, water, and sky were suspended, activities in the cyber domain witnessed an acceleration. The All Peoples Congress (APC) which is the incumbent political party, for the first time in history anchored an emergency virtual National Executive Committee meeting as the COVID-19 pandemic new normal necessitated new normal and quarantine (The State House Abuja, 2020). Medeiros, Goldoni, Junior, and Rocha (2020), posits that COVID-19 pandemic panic was a driver of innovation as it accelerated the use of the cyberspace by multiple actors such as government parastatals and the private sector. Besides, they made emphasis on the transposition of the administrative apparatus into the cyberspace, which brought into existence the e-government approach. However, they acknowledged the inevitability of possible challenges that can transpire in coordinated cyberspace activities.

The relevance of the cyberspace in the 21st accelerated dependency between individuals, organisations, and states, increasingly making the world a global village through digitalised communication; Mansabach and Taylor (2011, pp. 180,181), assert that the proliferation of mass media and communication and transportation innovations has accelerated people from all walks of life, even in the rural areas of the world, to establish an opinion about events, and get involved in public issues in a manner which was impossible in the era that preceded the emergence of the internet; the internet also has now become a means to an end in the hand of both governments and anti-government groups across the globe.

However, Africa has been tagged hotspot of crimes related to the cyberspace due to clear cases of internet racketeers, but this does not exclude other regions of the world from the perpetration of cybercrime. Shreds of evidence proved that developed nations are equally perpetrators of cybercrime; however, crimes committed in the cyberspace, seem to be region-specific. Kshetri (2019) identified Africa as one of the fastest-growing regions in term of cybercrime, in as much as the region is equally a victim of incessant sporadic cyber-attacks. I.T. and business advisory firm Serianu located in Kenya reported that African economies lost a total of $3.5 billion to cybercrime in 2017 alone. Nigeria lost $649 million, Kenya lost $210 million; while the South African Banking Risk Information Centre (SABRIC), lost $157 million annually to cyberattacks. As explicated by Kshetri, Africa is a perpetrator and equally a victim of cyberattacks. It is equally an indication that Africa is not lagging in the active use of the cyberspace. However, the mannerism in which cyberspace is used in Africa compared to the rest of the world appears less strategic as the African governments are not famous for launching cyberattacks compared to the rest of the world. Kshetri (2019) noted that Africa is a pronounced victim of cyberattacks which she attributed to vulnerable systems and lax cybersecurity practices. Similarly, Oladipo (2015) reports that cyber-crime is threatful to Africa as a database across the continent is prone to attacks based on lack of adequate protection which gives ease of access to hackers.

Cyber Security Strategy

The internet is now the most crucial tool for facilitating the exchange of opinions, distribution of information and propaganda, movement of legal and illegal funds, and also coordination of activities. An economist, who answers to the appellation, Kenici Ohmae cited in Mansbach and Taylor (2012, p. 192), argues that “the introduction of the internet from the mid-1990s has successfully made the world of communications truly borderless.” Anything that is borderless naturally lacks absolute control since there are no restrictions; therefore, the borderless nature of the advanced 21st-century communication has led to the questionable use of the internet. It is a technology that enables global marketing, flexible production, e-commerce, online financial transaction, international exchange of opinion and ideas, also coordination and mobilisation of activities. The cyberspace is a terrain where the aforementioned activities thrive effortlessly; however, activities in such domain should be censored or controlled for the safety of humanity. Nevertheless, full restrictions cannot be guaranteed since no one has a monopoly over the cyberspace.

The Department of Defence ‘Dod’ (2018) asserts that “the opened and decentralised nature of the internet spurred them to seek or create strategies to curtail or curb the significant vulnerabilities it poses.” Similarly, Osho and Onoja (2013) maintain that when a crime is digitalised, it poses complications which makes it cumbersome compared to traditional crimes where felons can be easily tracked and questioned. States such as China, Russia, Iran, and North Korea have been identified as axes involved in the unethical and immoral use of the cyberspace; similarly, individuals and terrorist networks had spotted as sources staging cyber-attacks on states, individuals and organisations (Department of Defence, 2018)

The activities that unfold in the cyberspace entail good and bad; this is due to the anarchic nature of the cyberspace since it lacks a central controlling unit. As a result of this, the cyberspace in the 21st century transmuted into an arena of illegal and legal activities which paradoxically promote national interest and threaten the sovereignty of other states. The dual encapsulation of good and bad of the cyberspace has led nations, and the global community to a consciousness that spurred scores of national strategies designed to mitigate the threat in the cyberspace posed to individuals, organisations, states, and the world in general. The cyberspace is now a theatre that embodies scores of national cybersecurity strategies to mitigate the challenges posed by unethical users of the internet. However, the cyberspace remains a theatre of multiple online activities such as cybersecurity strategies, cyberwar, cyber-trade, cybercommunication, cyber-repository, cyber-entertainment, cyberattacks and crimes.

In a bid to curtail the protruding debilitating occupation of hackers in the cyberspace, nations individually and collectively formulated national cyber strategies to mitigate the intrusion of cyber attackers or hackers into their digital infrastructure, such as **cyber-physical system** entails electricity grid, water purification, traffic lights, and hospital. According to Porup (2017), plugging a power plant into the internet makes it vulnerable to cyber-attacks. These are the vulnerabilities that the primary actors in international political actors aim to address.

Each state has its national cybersecurity strategy; Nigeria, for instance, established the Office of National Security Adviser (Osho & Onoja, 2015, p. 122); Donald Trump's administration signed Executive

Order 13800, for strengthening the cybersecurity of federal networks and critical infrastructure (Trump, 2018). Nineteen countries have developed and published their National Cyber Security Strategy 'NCSS' also referred to as National Information Security Strategy (Luiijf et al., 2013). Countries individually established strategies to balance against cyber-attacks. The cyber theatre is an embodiment of cyber-defence, and it is in this domain that cyber war takes place. Countries of the world have put strategies in place individually to balance against trojans and cyber-attacks.

Media Foundation for West Africa 'MFWA' (2017), published Key Issues and Challenges policy brief on cybersecurity in Ghana in June 2017. It was reported that government and relevant stakeholders were involved in finding solutions to address problems of a cyberattack; nevertheless, National cyber Security Policy Strategy (NCSPS) was established in 2016 to address cybercrime in the country. Ghana NCSPS includes the Ghana Computer Emergency Response Team (CERT-GH). Also, the Data Protection Commission (DPC) was introduced to abate the spate of cyberattacks in the country. Unfortunately, cybersecurity issues persisted due to the following: the absence of cybersecurity consciousness, limited awareness on cybersecurity issues exuded by users such as businesspeople and private individuals; lack of legislation enforcement and law enforcement agencies low capacity in the detection, investigation, and persecution of internet-related crimes.

Similarly, South Africa has established several legislative frameworks which make up its cybersecurity policy. The legislations go thus: ECT Act, RICA Act, ICCMA, convention, Criminal Law Amendment Act, no 32 of 2007, Act No.65 of 1996, Act 34 of 1999 and Act 18 of 2004. The South African cybersecurity policy aims to create an environment that will guarantee trust and safe use of ICTs by establishing structures in support of cybersecurity to reduce cybersecurity threats and vulnerabilities, and foster co-ordination and cooperation between government and private sector. Besides, promote and strengthen cooperation to establish a culture of cybersecurity consciousness, and upgrade user’s inclination to technical and operational cybersecurity standards (Department: Communications Republic of South Afric, 2009).

Africa Cyber Threat Intelligence Report ‘ACTIR’ (2018), maintained that a new study from Cyber Security firm Jighi approved by the 2018 Africa Cyber Security Conference (ACSC) revealed the extreme to which cyberattacks has perforated the African cyberspace. It ill impacted the entire continent affecting investments, government agencies, institutions and people from all walks of life. Furthermore, the report highlighted the weak security architectures, scarce skilled personnel, unconsciousness of cybersecurity and absence of coordinated regulations across the African countries. The weak cybersecurity has accelerated the cyber vulnerability of the African continent. Jig recommended that users of the cyberspace should upgrade outdated systems, consider the hiring of skilled I.T. personnel, and perform regular infosec audit.

U.N. General Assembly Sixty-fourth session (2010), adopted a Resolution on 21 December 2009 for the creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures. The U.N. General Assembly recalled the following preceding resolutions:

53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007 and 63/37 of 2 December 2008 on developments concerning information technologies in the context of international security.

The above resolutions of the U.N. on cybersecurity is a collective active effort os nation-states to balance against cyberattacks as it threatens national and international order. The resolution offers state governments the privilege to establish individual National Cyber Strategy as an alternative to the collective approach. In a nutshell, the U.N. advocates a multilateral and unilateral approach to countering cyberattacks. However, the inevitability of cyberattacks indicates the anarchical nature of the cyberspace as it lacks central authority just like the global political domain. The neoclassical realist perspectives of international politics in the context of state behaviour and relations at the worldwide domain to a great extent mirrors the reality of cyberspace actors.

Cyber Security to Cyber Defence and Cyber War

The anarchical nature of the cyberspace left states with no option but to prioritise the security of digital infrastructure due to cyber-attacks, stages by adversaries within and outside the country. Despite national strategies adopted by states to curb the infiltration of hackers into national digital infrastructures, the cyberspace increasingly posed vulnerabilities hitherto. China adopted scores of a national strategy to censor citizens' use of the internet, simply to disconnect them from the outside world, but many Chinese groups outwitted the Chinese government.

As put by Mansbach and Taylor (2011, p. 192), events in China reflect the challenges states face in the cyberspace. In April 1999, the Falun Gong group organised a massive subtle protest in Beijing, in which they surrounded the building where China communist leaders reside. The Chinese leaders were frightened by how the Falun Gong group outwitted China's extensive surveillance system despite coordinating its activities through the use of email. It is proof that the cyberspace can be used to threaten national sovereignty; the Chinese leaders were subjected to the Falun Gong siege, which was strategically coordinated and mobilised in the cyberspace.

Furthermore, Mansbach and Taylor (2011, p. 192) stress that "the Islamic State of Iran was struck by a political event which revealed that cyberattack is a threat to national stability. In 2009, Iranians staged a mass protest against rigged presidential elections through the use of Twitter, Facebook, and YouTube to keep the world abreast regarding political unrest and disorder in the country". Social networks have proved to be a vital tool in the hand of spin-doctors, political agitators, and propagandist.

It is evident in Nigerian politics too, where some citizens and interest groups indulged in the spread of rumours. In 2018, a section of the Nigerian population agitating for balkanisation flooded the internet with a dish that President Mohammed Buhari died in a hospital in the United Kingdom where he went for medical help. In late 2018, the same Eastern agitators claimed that President Buhari is an impostor, replaced by one Jibril from Sudan after his demise in the United Kingdom. It is a piece of invalid information that cannot be blocked or restricted by the government due to the nature of the internet. A cyber threat can come in the form of propaganda or attack on a national database by internal or external hackers. Events of this nature led to the urgent need for states to prioritise national cybersecurity.

Cyber-attack can happen within a state, and it can equally be carried out from external territories. For instance, the Wikileaks was an inside job, whilst the Russian manipulation of a general election that brought President Donald J. Trump to power is an external manipulation of digital machines.

Africa has been identified as a victim of multiple cyber attacks. Check Point Software Technologies statistics released in October 2015 for its ThreatCloud World Cyber Threat Map claimed that Tanzania is the most victimised by cyberattacks. However, followed by Malawi, Namibia, Mauritius, Tunisia, Ethiopia, Nigeria and South Africa, which ranked better (67) compared to the rest of Africa. The report claimed that less developed world is often the target of less developed countries (Cyber Security, 2016). A cyberattack can be from ordinary individuals or state; however, cyberattack attacks lunched by states are considered cyberwar. The increase in cyberwars has led governments to individual creation of cyber warfare units as countries of the world indulged in cyberwar in the space. For instance, the U.S. Cyber Unit was established in 2009; similarly, North Korea and the United Kingdom created theirs too to balance against cyberattacks from known or unknown attackers.

Nigerian Army unveiled its Cyber Warfare Command in 2018 which was announced in 2016. Nigeria has been identified rejigging its cyberwar strategy as the country is a victim of cyber-terrorism as the militant Boko Haram exposed itself to the brutal use of the internet. Nigeria discovered that the Boko Haram uses a social media platform for recruitment, and equally defaced the Defence Headquarters website. Furthermore, it was found that the Boko Haram hacked the Independent Electoral Commission (INEC) database on the day of the presidential election. However, in 2016 the Nigerian Army made known her intention of taking its counterinsurgency to the cyberspace. The Nigerian Army Cyber Warfare Command will monitor, defend and launch an assault in the cyberspace through its denial of service (DDoS) targeted at criminals, nations and terrorists (O'Flahety, 2018; Technology Mirror, 2018). With the introduction of the Nigerian Army Cyber Warfare, Nigeria can boast of cyber-armies for the protection of her territorial integrity. However, most African nations are not known for waging cyberwars; yet, the continent has a bucket full of non-state-actor-cyber-armies using the cyberspace as a means to an end due to the prevalence of unemployment. For instance, much Nigerian youth has been incarcerated by the Western nations for cybercrimes. For example, an internet celebrity known as 'Hushpuppi' was arrested by the USA. Similarly, a group of Nigerian internet racketeers were arrested in the USA and in South Africa by the State Interpol. Also, this group of racketeers are equally arrested in Nigeria almost daily by the Nigeria anti-fraud agency (BBC, 2016; Karimi, 2020; news24, 2016).

However, Nigeria has launched cyber warfare on two occasions; first, against the terrorist group that attacked its cyberspace, and secondly, against the dissemination of fake news and hate speech in the wake of *END SARS* protest that rocked the country (Ndidi, 2020).

The threat to digital infrastructure can be debilitating in that it potentially disrupts cyber-physical systems. In the developed world traffic lights, electricity, trains, electricity grid, water purification machines and medical apparatus have all gone digital; an attack on the cyberspace might trigger national disruption or destruction of critical infrastructure that depends on the internet. Such an occurrence is a potential threat to internal and external sovereignty of the state. States realisation of the damaging effect of cyber-attack to digital infrastructure triggered the urgency to develop a national cybersecurity strategy to defend national cyberspace from internal and external intrusion.

National Cyber-Security Strategies

National cybersecurity is defined as an established or consolidated policy designed to deter internal and external intrusion to national digital infrastructure. It is also the ability to ensure the integrity, confidentiality, and availability of information (Porup, 2017). The European Union Agency Network and Information Security define NCSS as:

key policy feature, helping them to tackle risks which have the potential to undermine the achievement of economic and social benefits from cyberspace (Enisa, 2019).

Before the emergence of the internet, national security only covers four domains which are land, sea, air, and space. Still, the proliferation of the internet aroused the need for national governments to protect their respective cyberspace from cyber-attacks often staged by known adversaries searching for classified information of other states for strategic needs. America, European nations, Georgia, Estonia, and South Korea have suffered from cyber-attack from one or two of the following primary actors, China, Russia, North Korea, and Iran; also terrorists and fraudsters are equally identified as cyberspace attackers. The security threat posed by hackers rendered the cyberspace as the fifth domain, which needs to be protected by the state (Mansbach & Taylor, 2012, p. 306).

The Department of Defence (2018), in its cyber strategy, reports that "Adversaries prevented from engaging the United States and its allies in physical armed conflict found the cyberspace operation as a means to steal their technology, and disrupt their government, commerce, manipulate their democratic processes, and also threatened their critical infrastructure." Events of this nature account for the essential need for the state to have national cybersecurity. Technology information and classified information theft can pose a considerable challenge to national sovereignty. The Wikileaks intrusion hurts America hitherto. Cyberattacks often have a long-term debilitating effect on the attacked; this is why states are increasingly incentivising consolidation of national cybersecurity.

Clinton, Obama, and Trumps's administration respectively made a strong emphasis on the need to design effective cybersecurity due to multiple attacks the USA suffered from hackers based in the axes mentioned above (Mansbach & Taylor, 2012).

A cyber-attack in the USA led Clinton's administration to design a comprehensive computer monitoring system; the threat of cyber-attack triggered the consolidation of cyber games at the U.S. military academy. Obama's regime also created a cybersecurity office in the White House; Cyber Command was created by the U.S. Department of Defense (Mansbach & Taylor, 2012, p. 306).

The porosity of the cyberspace proved inevitable in the general election that brought President Trump to power, where the Russians influenced the American electoral process through the use of cyber-enabled information operations. China has a culture of eroding U.S. military better armed and the nation's economic strength by obstinately withdrawing or exfiltrating classified information from U.S. public and private sectors (Department of Defence, 2018). The internet subjects the USA to external threats. Still, the country remains glued to the use of the cyberspace and committed to the promotion of cybersecurity due to the strategic benefits the cyberspace embodies.

States often design or define their national cybersecurity strategy, according to their national needs or reality. Still, there tends to be some common ground in national cybersecurity strategy since cybersecurity aims at deterring cyber-intrusion from the unwanted axis or malicious users of cyber tools. The work of Luiijf, et al. (2013), also shows similarities in the comparative analysis of 19 national cybersecurity services.

The Office of the National Security Adviser 'ONSA' (2014), shares an identical cybersecurity view with Microsoft (Godwin & Nicholas cited, in Osho & Onoja, 2013, p. 123); the cybersecurity strategy of ONSA aims at addressing the following: cyber-crime, cyber terrorism, cyber espionage, online child abuse, and exploitation. The Trump administration 2018 cybersecurity strategy aims to address the following: defend the homeland by protecting networks, systems functions, and data. Promote American prosperity by nurturing a secure, thriving digital economy and fostering vital domestic innovation. Preserve peace and security by strengthening the ability of the United States - in concert with allies and partners - to deter and, if necessary punish those who use cyber tools for malicious purposes; and; expand American influence abroad to extend the fundamental tenets of an open, interoperable, reliable, and secure internet (Trump, 2018).

The Trump administration tends to bolster ties with the existing transnational platform such as United Nations Convention Against Transnational Organized Crime, the G7 24/7 network Point of Contact and the Budapest Convention, as a defensive measure against the cyberwar. But the question remains can cyber-attack, be altogether deterred in a society where cyberculture favours cyberspace vulnerabilities? It is a fact that hackers indulge in the use of popular social networks to infiltrate states digital infrastructure; for instance, the electoral process in the USA was manipulated by Russian hackers through social network generated data. The contemporary global cyberculture offers cyber warriors an ocean to swim freely. The USA presidential election was manipulated through social media platforms; this singular fact should discourage the use of Facebook, but shockingly the use of Facebook accelerated. Africa is one of the active users of Facebook; it is an indication that Africa will remain vulnerable to cyber warriors.

It is quite appalling that the axis 'China, Russia, Tajikistan, and Uzbekistan' the West labelled as homes to cyber attackers, in 2011 assent to the Initiative of the General Assembly of the United Nations for an 'International Code of Conduct for Information Security (U.N. cited in, Luiijf et al., 2013, p. 24). States have come to realise the debilitating effect of cyberwar on national security and have come to term to address cybercrime issues collectively. But the rationale behind individuals staging an attack on foreign territory digital infrastructure is beyond financial gains, there might be political motives to it, and it might be backed by states seeking to access classified information of another state. The fact that genuine hackers' identity cannot be identified in the cyberspace poses a considerable threat to the cyber world hitherto. And it subjects one to the question why is cyberwar an inevitable aspect of contemporary cyberspace despite partnership between states at the global level to mitigate cyber-attacks?

Cyber War

The cyberspace in recent years has turned to be a possible means to an end, in the hand of states, interest groups, organisations, researchers, defence department, and terrorists; the cyberspace is a theatre that encapsulates all sorts of actors. The porosity, and fluidity of the cyberspace increasingly pose challenges to national digital infrastructure and sovereignty. Adversaries that cannot balance against their rivals, or despise the use of confrontation, in reality, find the cyberspace as a relevant alternative to assert their radical ambition (Department of Defence, 2018; Mansbach & Taylor, 2012, p. 307).

The USA has been attacked in the cyberspace by small revisionist states such as Iran and North Korea. They are known for the indulgence in the malicious use of cyber tools to harm U.S. citizens and USA interest. The USA vulnerabilities to cyber-attack can be attributed to its civilian and military excessive dependence on cyberspace for almost everything (Department of Defence, 2018). Whatever threatens America's cyberspace, will simultaneously threaten the alternative four domains, and it is a potential source of espionage (Mansbach & Taylor, 2012, p. 30).

Mansbach and Taylor (2012, p. 306), defined cyberwar as the war in the cyberspace, which exposes physical, cyber machines to attacks from adversaries; this pushed many countries to prioritise the security of cyberspace. Cyberspaces are often attacked to cause destruction or disruption to plunge a state into disorder. Cyberspace vulnerabilities have threatened the United States, internal and external sovereignty. It gave small countries such as North Korea and Iran leverage to dare the superpowers; Mansbach and Taylor (2012, p. 307), referred to this as asymmetric warfare. The cyberspace over the years has proved to be a significant arena which advanced societies are now exploiting as the 5th warfare domain. Mansbach and Taylor posit that:

> "Instead of using explosives to kill and destroy the warrior of the future" may be armed "armed with a laptop computer from a motel room." "Hacking, virus writing, and crashing data information systems – as well as defending against enemy hackers and virus writers – may become core military skills, as important as the ability shoot." Future war "may see attacks via computer viruses, worms, logic bombs, and Trojan horses rather than bullets, bombs, and missiles" (2012, p. 306).

From the above premise, former President Obama declared that in today's world, terrorism could emanate not merely from a few extremist or adversaries in suicide costume but from the click of a button on the laptop 'a weapon of mass destruction'. He further said that from now, the networks and computers they depend on daily would be treated sensitively as a strategic national asset and protecting the digital infrastructure will be a national security priority. In his speech, he avowedly stated that the U.S. and Russia have engaged in talks with the aims of enhancing internet security and curtailing the possibility of cyber (Mansbach & Taylor, 2012, p. 306).

The above submission shows that protection of the cyberspace has gone beyond a national question, to a global problem which states are collectively aiming to address to mitigate the possibility of cyberwar. This observation validates the assumption 'from cybersecurity and cyber defense to cyberwar'. Cyberwar seems to be the new form of war states, and individuals use to meet certain political or economic ends.

The submission by former President Obama regarding cyberwar raised consciousness at the global arena regarding the future possibility of a cyberwar between states. But quite unfortunate that the long-term American adversary was accused of staging a cyber-war on America by manipulating the general election that brought President Donald J. Trump to power. It is quite appalling that despite the prevalence of national cybersecurity, national cyberspace is increasingly subjected to cyber-attacks from unknown persons. The most bewildering aspect of the intrusion into states cyberspace is that the countries of origin are often identified, but the hackers behind the cyberspace intrusion are often anonymous; this posed a considerable challenge to the cyber world hitherto. States inability to have absolute dominance in protecting classified information stored in national cyberspace has led to the proliferation of espionage. Espionage is a threat to the intellectual property of national defence, and critical national private investments such as banks, airlines, communication companies, hospitals, and any other organisation that uses cyber-physical instruments (Mansbach & Taylor, 2018, p. 306). Lack of absolute dominance over the information in national cyberspace has spurred the proliferation of espionage in recent years in the global cyberspace.

For instance, a Chinese-based electronic spying group called "Ghost-Net" in 2009 infiltrated computers across the globe; Ghost Net has the technological advantage to exercise full control over infected cyber-physical machines; it searches for information and downloads selected files. This device shows how cyber malware can be a threat to a sophisticated network or cyber-physical machines. Chinese officials intruded Google cyber citadel, and this led Google to evacuate China. There is also a record of Chinese and European hackers' infiltration of into 2400 private organisations and government computers to pilfer classified information for over 18 months.

Cyberwar capabilities to subject a nation or an organisation to collateral damage was evident in 2008 when America discovered that hackers had penetrated their electric grid, and planted software that can reduce the standard of the cyber-physical machine. As a result of multiple cases of cyber-attacks on American digital infrastructure, the Chinese government indulgence in hacking against the U.S., European, and Japanese industries and research facilities is quite gross. Exabytes of data have been pilfered from government facilities, industrial labs, and universities (Mansbach & Taylor, 2012, pp. 306, 307).

The cyberwar appeared to be a zeitgeist in the contemporary world, judging from the skilfulness of state-sponsored hackers in creating sophisticated malware designed to intrude in desired cyberspace; Mansbach and Taylor (2018, p. 307), posits that "Russian 'cyber warriors' are the most skilled compared to the Chinese hackers. In 2007 Estonia was a victim, and in 2008 Georgia was a victim of Russian based hackers who launched cyber-attack on them through a malware called 'Distributed Denial of Service' (DDOS). Estonia remains the first victim of Web War 1 due to its excessive dependence on internet connectivity”. The cyber-attack was triggered by the removal of a Soviet war memorial from central Tallinn; this is another example of states taking grievances from the land to the cyberspace.

North Korea, a well-known revisionist state in the context of international law, launched DDOS malware against the U.S. and South Korea digital infrastructure in 2009 following the cyberwar organised by the USA. The issue that was raised during this period was that should retaliation be considered, just how it is the rational response in a situation of physical armed attack (Mansbach, 2012, p. 307).

African countries cyber-armies are not notorious compared to countries such as Russia, USA, and China are well known for staging cyberwars. However, it is strictly for strategic purposes which in turn add value to the cyber attackers’ country. But in the case of Nigeria, cyberattacks are often launched by cyber-non-state-actors, often for personal gains as it was in the case of Nigerian internet racketeers apprehended by the USA in South Africa, Dubai, and in the USA.

Conclusion

In conclusion, cyberwar has turned to be an efficient tool in the hand of superpowers and small powers; it has triggered asymmetric warfare, a type of warfare that brings powerful and small power states to equal footing. In the contemporary world, offensive cyber capabilities are increasingly overshadowing defensive capabilities. National cyber strategies adopted by states has proved futile in curtailing cyber wars and cyberattacks as it is in the case of Africa, even the developed world despite their sophisticated cybersecurity mechanism. It might be because states find the cyberspace as a domain where national interests can be pursued, and also the fact that the cyberspace has no central control unit that can oversee the activities of users. The cyberspace in a deep-seated sense has helped China gain a technological advantage by pilfering of classified information from states across the globe. Similarly, Russia has positioned itself as an invisible cyber warrior by using its cyber-armies to launch scores of attacks on enemy axis, for instance, the infiltration in America’s election that brought President Donald J. Trump to power.

It was discovered in this study that the cyberspace is more anarchical compared to the internal terrain; in the international landscape, there is a collective body that relatively checks the excesses of states. Unfortunately, the cyberspace lacks a collective unit that can curtail the activities of cyber warriors; hence, no bulwark against the activities of cyber-soldiers and non-state-actor-cyber armies that can deter or regulate their activities. However, the intrusion of cyberwarriors into the repository of states, corporations, and individuals has been mitigated to some extent. However, the fact remains databases are still successfully attacked by cyber warriors.

The certainty of anonymity in the cyberspace has made the war on cybercrime a difficult one, in that both states, corporations, and individuals launched cyberattacks anonymously either to pilfer classified information or to extract financial resources. In this regard, Africa seems to be the most vulnerable due to its week cybersecurity strategy. However, the argument that Africa's cybersecurity is weak does not hold that much anymore, because cyber-warriors equally victimise countries that own strategic cybersecurity bulwark. For instance, it was discovered that hackers from Russia and China hacked into the COVID-19 research centres in Europe and America. This occurrence singularly validated the claim that the cyberspace is porous and anarchical. Cyberattacks can be a potential source of international conflict due to the inevitability of anonymity and immorality exuded by states and individuals due to the unethical use of information communication technology.

Finally, cyberwar and cyber-attacks are inevitable as they are a means to an end in an essential sense. Events have shown that states use cyberwar to advance their national interests. At the same time, non-state-actor-cyber-armies launched cyberattacks to pilfer financial resources as it is the case of attacks coming from Nigeria and other African countries. In a nutshell, the Asian, Western and American axes have been seen waging cyberwars and cyberattacks to meet specific national objectives which could be political or economic based. Contrariwise, cyberattacks launched by cyber-warriors in Africa alternates between terrorism and pilfering of financial instruments, however, the pilfered financial instruments is an income from the rest of the world, hence, an addition to Africas Gross Domestic Income (GNI). But the opportunity cost is that it drags the reputation of the continent in the quagmire of ridicule, and ruins online investment trust which can be a disincentive to the online market in that foreign investors might fill reluctantly in buying portfolio investment across the continent.

Similarly, the African continent has seen a surge in the use of cyberspace for political activities such as campaign, advocacy, and decry of bad leadership; however, the strategic use of the cyberspace in Africa has not come to the fore. The African cyber warriors limited the use of cyberspace to the monitoring of malicious activities. Still, the strategic use of the cyberspace capable of speeding the accomplishment core national objectives seem unconsidered. The USA, Western and Asian axis cyber-armies and non-state-actor-cyber armies have made headway in utilising the cyberspace as a tool for the advancement of national interest.

References

ACTIR, (2018). *Executive Summary of African Cyber Threat Intelligence Report (ACTIR).* [Çevrimiçi] Available at: https://www.africacybersecurityconference.com/reports-cyber-security-in-africa [Erişildi: 24 October 2020].

Aschmann, M., Van Vuuren, J. J. & Leenen, L. (2015). Towards the Establishment of an African Cyber-Army. *Journal of Information Warfare,* 14(3), pp. 15-29.

BBC, (2020). *US charges Chinese Covid-19 research 'cyber-spies'.* [Çevrimiçi] Available at: https://www.bbc.com/news/world-us-canada-53493028 [Erişildi: 23 September 2020].

BBC, (2016). *Online fraud: Top Nigerian scammer arrested.* [Çevrimiçi] Available at: https://www.bbc.com/news/world-africa-36939751 [Erişildi: 25 October 2020]

Cambridge University Press, (2020). *Cyber.* [Çevrimiçi] Available at: https://dictionary.cambridge.org/dictionary/english/cyber [Erişildi: 23 September 2020].

Chatzichristodoulou, M. (n.d.). *Cymposium.net.* [Çevrimiçi] Available at: http://www.cyposium.net/wp-content/uploads/2012/09/maria_text.pdf [Erişildi: 27 January 2019].

Cyber Security, (2016). *Africa in the cyber war.* [Çevrimiçi] Available at: https://www.securitysa.com/print.aspx?editorialtype=N&editorialid=53798 [Erişildi: 24 October 2020].

De Groot, J., (2020). *What is Cyber Security? Definition, Best Practices & More.* [Çevrimiçi] Available at: https://digitalguardian.com/blog/what-cyber-security [Erişildi: 23 September 2020].

Department of Defence, (2018). *Department of Defence Cyber Strategy,* Washington DC: DoD.

Department: Communications Republic of South Africa, 2009. *CYBERSECURITY POLICY OF SOUTH AFRICA.* [Çevrimiçi] Available at: https://www.ellipsis.co.za/wp-content/uploads/2011/02/CYBER-SECURITY-POLICY-draft.pdf [Erişildi: 24 October 2020].

Dennis, M. A., (2020). *Cybercrime.* [Çevrimiçi] Available at: https://www.britannica.com/topic/cybercrime#ref235699 [Erişildi: 24 September 2020].

Enisa, (2019). *National Cybersecurity Strategies.* [Çevrimiçi] Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies [Erişildi: 28 January 2019].

Karimi, F. (2020). *Feds used his posts to link him to alleged cyber crimes.* [Çevrimiçi] Available at: https://edition.cnn.com/2020/07/12/us/ray-hushpuppi-alleged-money-laundering-trnd/index.html [Erişildi: 25 October 2020].

Kaspersky, (2020). *What is Cyber Security?.* [Çevrimiçi] Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security [Erişildi: 23 September 2020].

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management,* 22(2), pp. 77-81.

Lenthang, M. (2020). *China, Russia and Iran 'have deployed spies to steal US vaccine research in an intelligence war targeting biotech companies and university research centers'.* [Çevrimiçi] Available at: https://www.dailymail.co.uk/news/article-8703843/China-Russia-Iran-deployed-spies-steal-vaccine-research-intelligence-war.html
[Erişildi: 23 September 2020].

Luiijf, E., Besseling, K. & Patrick, D. G. (2013). Nineteen National Cyber Security Strategies. *International Journal Criticial Infrastructure ,* 9(1/2), pp. 3-31.

Mansbach, W. R. & Taylor, L. K., (2012). *Introduction to Global Politics.* 2nd dü. New York: Routledge.

Medeiros, B. P., Goldoni, f. L. R., Junior, E. B. & Ribeiro da Rocha, H.(2020). The use of cyberspace by the public administration in the COVID-19 pandemic: diagnosis and vulnerabilities. *Revista de Administrção Pùblica,* 54(4).

Merriam-Webster, (2020). *Cyberattack.* [Çevrimiçi] Available at: https://www.merriam-webster.com/dictionary/cyberattack [Erişildi: 23 September 2020].

MFWA, (2017). *Cyber Security in Ghana: Key Issues and Challenges.* [Çevrimiçi] Available at: https://www.mfwa.org/wp-content/uploads/2017/09/cyber-security-Report.pdf [Erişildi: 24 October 2020].

Ndidi, O. (2020). *Army launches cyber warfare over hate speech.* [Çevrimiçi] Available at: https://thenationonlineng.net/army-launches-cyber-warfare-over-hate-speech/ [Erişildi: 25 October 2020].

News24, (2016). *Interpol arrests Nigerian accused in $60 million cybercrime.* [Çevrimiçi] Available at: https://www.news24.com/news24/africa/news/interpol-arrests-nigerian-accused-in-60-million-cybercrime-20160801-19 [Erişildi: 25 October 2020].

O'Flahety, K. (2018). *The Nigerian Cyber Warfare Command: Waging War In Cyberspace.* [Çevrimiçi] Available at: https://www.forbes.com/sites/kateoflahertyuk/2018/11/26/the-nigerian-cyber-wafare-command-waging-war-in-cyberspace/#4e2de4792fba [Erişildi: 24 October 2020].

Oladipo, T. (2015). *Cyber-crime is Africa's 'next big threat', experts warn.* [Çevrimiçi] Available at: https://www.bbc.com/news/world-africa-34830724 [Erişildi: 24 October 2020].

Osho, O. & Onoja, A. D. (2015). National Cyber Security Policy and Strategy of Nigeria: a Qualitative Analysis. *Internationa Journal of Cyber Criminology (IJCC),* 9(1), pp. 120-443The State House Abuja, 2020. *Address by President Muhammad Buhari at the Virtual Emergency Meeting of the NEC of the APC.* [Çevrimiçi] Available at: https://statehouse.gov.ng/speeches/address-by-president-muhammad-buhari-at-the-virtual-emergency-meeting-of-the-nec-of-the-apc/
[Erişildi: 24 October 2020].

Porup, J. (2017). *CSO.*[Çevrimiçi] Available at: https://www.csoonline.com/article/3242690/data-protection/what-is-cyber-security-how-to-build-a-cyber-security-strategy.html [Erişildi: 27 January 2019].

Sheldon, J. B., (2016). *Cyberwar.* [Çevrimiçi] Available at: https://www.britannica.com/topic/cyberwar [Erişildi: 23 September 2020].

Technology Mirror, (2018). *Nigerian Army Unveils Cyber Warfare Command.* [Çevrimiçi] Available at: https://technologymirror.com.ng/nigerian-army-unveils-cyber-warfare-command/ [Erişildi: 24 October 2020].

Trump, D. J., (2018). *Natıonal Cyber Strategy of the United States of America.* [Çevrimiçi] Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [Erişildi: 24 September 2020].

Trump, P. D. J. (2018). *National Cyber Strategy of the United States of America,* Wahshington DC: The White House.

UN General Assembly Sixty-fourth session, (2010). *Resolution adopted by the General Assembly on 21 December 2009.* [Çevrimiçi] Available at: https://undocs.org/pdf?symbol=en/A/RES/64/211 [Erişildi: 24 October 2020].

Xiaoxing, S., (2017). *The Theatre Times.* [Çevrimiçi] Available at: https://thetheatretimes.com/cyber-theatre-china-performance-action/ [Erişildi: 27 January 2019].