GLOBALIZATION AND CYBERTERRORISM IN NIGERIA: WHICH WAY FORWARD?

ALFRED A. UDOSEN  
Department of Computer Science,  
Babcock University, Ilishan-Remo, Ogun State, Nigeria  
udosena@babcock.edu.ng

&

GOODNEWS OSAH  
Department of Political Science and Public Administration,  
Babcock University, Ilishan-Remo, Ogun State, Nigeria  
osahg@babcock.edu.ng

Abstract  
The cyberspace is primarily concerned with the security, control, and protection of shared information that are vital for decision making processes in any type of communication network. Terrorists now threaten public security by using cyberspace and social media technology to create fear and spread violence as the ways of intimidating a government or the general public. The readiness to respond to these threats (both internally and externally) to security, requires a combination of civilian and military tools in addition to economic and diplomatic resources that are needed to inhibit threats and to moderate their effects. Revitalization and strengthening of the national orientation with a mandate on value re-orientation, equity, fairness and social justice in the international community is necessary especially in information sharing in order to put an end to the risk of cyberterrorism. Also cyber innovations open up new opportunities for public-private partnerships to foster security initiatives and promote better efficiencies in the affairs of the government.

Keywords: Boko Haram, Cyberspace, Cyberterrorism, Globalisation, Terrorism.

Introduction  
In the space of about thirty years, the internet has transformed from a US Department of Defense command-and-control network consisting of less than one hundred computers to a network that stretches across the globe (Collin, 1997) and by January 2019, out of the 7,519,028,970 people in the world, the global users of the internet had reached about 4.39 billion (Global Digital Overview, 2019). Thus, the internet can be said to be one of the fastest growing technology in the world today (Orngu, 2014). In the Western world, most especially, the internet has been extensively integrated into the economy, the military, and society at large (Collin, 1997).

Based on the foregoing, as the environment in which we live changes, its influence on the state of its security cannot be overemphasized. The advancing target of numerous participants has
affected the security environment and global instability, and conflicts may affect our own security and international relations. By coping with common threats and seeking to prevent them, security became a key factor in supporting the protection of critical infrastructures and the quality of life in the society, and this could only be guaranteed by good relations with neighbouring countries. The preparedness to respond to cyber threats (both internally and externally) requires a combination of civilian and military tools in addition to economic and diplomatic resources that are necessary to inhibit these threats and to moderate their effects (Podhorec, 2012).

Nigeria as a sovereign state has the responsibility of guaranteeing the security of the life and property of its citizens, protecting its territoriality and sovereignty, and guaranteeing its socio-political and economic stability. Nevertheless, since the end of the 20th century, both local and international terrorism and terrorism-related activities have threatened this protective function of the state as a result of the colonialization and globalisation agenda of the Western world (Olowojolu& Ake, 2015).

In Nigeria, the economic crisis in the 1980s saw the emergence of groups who were involved in terrorist related activities in the country. These groups include: numerous militant movements in the Niger Delta, Odua People Congress (OPC) in the South West, Arewa Youth Consultative forum in the North, Movement for the Actualization of the Sovereign State of Biafra (MASSOB) in the South East, Movement for the Survival of the Ogoni People (MASOP), Movement for the Emancipation of the Niger Delta (MEND), Ijaw Youth Council (IYC), Egbesu Boys of Africa (EBA).

With the aid of globalisation, the leader of the Al Qaeda network, Osama Bin Laden, had been able to communicate with terrorists in Nigeria through the media with the pledge to support the quest to assist them in destroying their country and its citizens (Njoku, 2011). Karon (2003) reported that, in February 2003, Osama Bin Laden stated that Nigeria is a country that was ripe for liberation, that is, Nigeria, as a country, was worthy of jihad.

According to Alao, Osah& Adam (2019), the Nigerian government claimed it had destroyed Boko Haram sect but, the truth in this 21st century, is that warfare had shifted from hardware to software as these assailant snow use both physical weapons of warfare and unconventional tactics to restrict the government. Beyond throwing bombs, crossing borders, and taking hostages, they now target critical national infrastructure by attacking the cyber security structure of Nigeria.

Globalisation
Fafowara (1998) argued that globalization deals with the increasing breakdown in trade barriers and the in increasing integration of world market. Also, Tony and Jan (2003), averred that globalization is the integration of not just the economy but culture, technology and governance. In the same vein, Onimisi (2014) asserted that globalization is the integration of political, economic, social, and cultural values across international boundaries. The growing financial transactions in the world market is an indication of the amassed intensity in the process of globalization and the opportunities it has brought to countries cannot be overlooked as globalization is a multifaceted, complex phenomenon.
Jean (2002) argued that the improvement in productivity and higher living standard were attributed to the much access to developed countries’ markets and technology transfer between several different countries. In the same vein, Ogbonnaya (2013) opined that the concept of globalization is used to represent the growing worldwide interdependence of the people and countries. Furthermore, globalization is viewed as the integration of everything with everything else, that is, the integration of finance, technology, and markets in a way that shrinks the world into a small size.

From the above definitions of the concept of globalization, scholars agreed that globalization is a process that promotes the destructions of barriers that existed previously among states of the world, therefore, fusing the world into a single entity or unit where barriers such as culture, governance, geography, and communication were extinct (Tomlinson, 1999). Suffice it to say that globalization has closed the gaps that existed among states as they are constantly interdependent in economic, socio-cultural, and political terms (Njoku, 2011).

However, globalization brought about new challenges like inequality across and within nations, financial markets volatility, growing insecurity, and environmental deterioration. Apart from these, a vast majority of developing countries separate from the process of globalization (Bretherton and Ponton, 1996). Furthermore, there is an increase in the criminal activities across national borders as a result of globalisation (Ahmed, 2016). Although, globalization gave rise to development in every area of our society from socio-cultural, political, economic, and technological aspects, it had, however, been argued that globalization begets terrorism (Njoku, 2011). Consequently, Cronin (2003) asserted that characterized by unpredictable and unprecedented threats from non-state actors, the present stage of international terrorism is not just a reaction to globalization but also its facilitator (Cronin, 2003).

Furthermore, because of the colossal advancement in technology, globalisation has enhanced intensely and this includes cross border data flow, satellite networks, the internet, global telecommunication infrastructure, and wireless telephones were all credited to globalization (Adesina, 2012). This amalgamation of the world into a global village for the good of all was, however, the basis on which terrorist groups perpetrated cyber terrorism. The cyber domain involves the electromagnetic spectrum to house, transfer, and edit information through physical infrastructure and virtual networks.

During the Cold War, computers were relied heavily upon by the national security community (Roberts, 2019). Rourke (2005) highlighted that over the last 20 years, the effects of globalization have brought about a huge difference between poor and rich countries, thereby heightening hostilities and violence among the poor, marginalized countries located in the Third World against the Western pioneers of globalization and its antecedent characteristics, expressed in economic and political terms.

Fayomi et al, (2011) asserted that the internet sped up an exponential ever increasing interconnectivity and communication worldwide. This unification of divers resources brought about globalization that has resulted in several benefits such as convenience and
comfort by an improvement in the standards of living in the developing world. However, it also birthed new weapons of resistance for organisations that sought to oppose certain political measures and ideologies. Thus, it is possible for people to die as a direct consequence of a cyberterrorist attack and that such an attack is imminent (Collin, 1997).

Much of the activities and its consequences of globalisation goes way beyond the territorial framing of the state and gave rise to ethnic violence, human and drug trafficking, the increase in arms proliferation, cyber-attacks, and global crime (Davies, 2003). The struggles to be updated with developments in the cyberspace, based on real-time interconnectedness and interdependence, is made complicated by globalization process and this makes military and industrial technologies to be vulnerable as information flows at the speed of light, shortening decision making cycles and reaction times (Roberts, 2019). However, cyberspace according to Roberts (2019) is a combat zone that has industrial control systems and critical infrastructure instead of combat aircraft, tanks and military maritime vessels. And based on the flexibility of cyber dynamics, the policies of a company or government will continue to lag behind new and available technologies. Thus, to secure virtual and physical networks from hackers, new levels of encryption and security measures were necessary. In addition, these hackers sell patented industrial information to competitors, destroying a company from within through cyber interruption by exposing company secrets, and use illegally obtained information to conduct insider trading (Roberts, 2019).

The Origins of Cyberterrorism
The term ‘cyberterrorism’ was coined in the mid-1980s by Collin (2003), a Senior Research Fellow at the Institute for Security and Intelligence in California. Hence, the thief of today can steal more with a computer than with a gun and the terrorist of tomorrow may be able to do more damage with a keyboard than with a bomb (National Research Council, 1991).

Pollitt said that cyberterrorism is composed of two elements: cyberspace (a place where computer programs function and data moves) and terrorism (the use of force or violence and a political motivation) (Pollitt, 1998). Hence, Minei and Jonathan (2012) concluded that cyberterrorism is the amalgamation of cyberspace and terrorism and Denning (2000) added that this union brought about a threat of attacks or an actual unlawful attacks against computers, computer networks, and the information stored so as to intimidate or coerce a government or its people in furtherance of political or social objectives that could cause violence against persons or properties, cause or fear, death or bodily injury, explosions, or serious economic loss to the victim.

Elsewhere, Devost, Houghton& Pollard (1997) defined information terrorism as the intentional abuse of a digital information system, network or component toward an end that supports or facilitates a terrorist campaign or action. Consequently, information terrorism can be said to be forms of attacks that would not necessarily result in violence against humans but it might incite fear that can be characterised as terrorist. Hence, cyberterrorism could be said to be the introduction of sophisticated computer viruses introduced into computer-controlled systems used for communications, banking, life support, and manufacturing that could cause in massive disruption of highly organised and technological societies (Collin, 1997).
Terrorism and Cyberterrorism in Nigeria

Poverty, which is an end-product of the effects of globalization facilitated by the Bretton Woods institutions, such as the World Bank, the World Trade Organization (WTO) and International Monetary Fund (IMF) that are to a great extent controlled by the Western industrialized capitalist states, is one of the root causes of terrorism in the Third World. The economic policies of these institutions have enhanced the attack on the economies of the Third World countries, especially in Africa, and ensured perpetual domination. The effects of these policies, such as the Structural Adjustment Program (SAP), have resulted into extreme poverty of the people and have caused hatred towards their governments, which were in support of these institutions (Njoku, 2011; Adekanye, 2008).

Nigeria, like other Third World countries, has had its fair share of the evil effects of globalization, aiding, and leading to terrorist activities (Osah, 2017). The several policies of the IMF and World Bank that were sold to the governments in the 1980s had led to inexpressible economic hardships on the citizens. This caused various groups to react against these policies, violently. Hence, these issues gave rise to terrorist violence in Nigeria, ranging from the militants in the Niger Delta, who used terrorist tactics to fight the government, believing they were agents of foreign capital. Then the Boko Haram fighters, who believing that the government were the cause of their plight, tore their university and college certificates out of frustration and poverty, and destroyed the properties and institutions of both individuals and the government (Njoku, 2011). Boko Haram, due to their modes of operations, were said to be one of the deadliest terrorist groups in the world (Alao, Osah & Adam, 2019).

According to Title 22 of the United States Code, Section 2656f (d), Terrorism is defined premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience. Thus, it is safe to state that cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents (Pollitt, 1998).

Basically, these terrorist organisations attract attention by posting roadside bombing, and a significant portion of society views the decapitation of hostages and terror propaganda videos. In fact, some jihadist websites have video games where users could act as holy warriors killing government soldiers. Their familiarity with technology made it simple and efficient for them to accomplish their nefarious goals. Thus, these terrorists now threaten public security by using cyberspace and social media technology to create fear and spread violence (Ogunlasna, 2019).

Cohen and Felson (1979) argued that crimes occur based on a person’s involvement in daily routine activities. Terrorist groups, preferably, use social media as an efficient and convenient tool for disseminating information because it has the ability to spread short messages that may be blended with images, texts, and voice notes (Ogunlana, 2019). However, the spreading of hate speech, violence related information, and racist statements over the internet has raised numerous legal questions (Nagpal, 2002).
In the viewpoint of Roberts (2019), social media became a medium for advancing propaganda, personal aggrandizement, political agendas, and influencing public opinion. Shackelford (2013) observed that cyberattack could be broken into four main categories: criminal activity, espionage, terrorism, and cyber warfare. Hathaway, et al (2012) sees cyberattack as any action taken to demean the functions of a computer system or its networks for political or national security or hinder the effective governance of any country. Attacks involve the use of sophisticated coordination among several hackers across international boundaries with the aim of making financial or military gains, with clear and self-reinforcing motivation (Kim, et al, 2012).

With the effort to protect its cyberspace and its telecommunication infrastructures from terrorist attack, the Nigeria government has spent a huge sum of money, giving much attention to cybercrimes like fraudulent online financing and fundraising activities (Ogunlana, 2019). The Global Organized Crime Project of the Center for Strategic and International Studies in 1998, viewed cyberterrorism as a part of Information Warfare (IW)(Global Organized Crime Project, 1998). The electronic age brought about the emergence of cyberterrorism that consists of two modern fears – fear of terrorism and fear of technology. Even with the use of relatively simple means in the future, the information infrastructure of any country could be attacked by any international terrorist groups with a clear capability by using the internet and other modern means for their own communications. Hence, cyberterrorism was viewed as traditional terrorist tactics that has a new strategy employing new tools and exploiting new dependencies (Conway, 2007).

While cybercriminals seek for opportunities to gain personal benefit from the proceeds of crimes, cyberterrorists are disciplined, trained, and committed actors who are motivated by radical ideology, religion, or political agendas through effective communication and proper planning. Additionally, through information operation, a country can engage in cyberterrorism against another country, or they can participate in cybercrime to steal proprietary information or trade secret from another country, as the case may be. The organisation discusses openly by using social media platform and they coordinate their secure conversation with encryption technology (Ogunlana, 2019). According to Pagliery, Crawford & Ashley (2015), this method of secretive communication, also known as “going dark,” remains one of the noteworthy challenges facing counterterrorism officials, police, and the intelligence community all over the world.

With the use of websites, blogs, YouTube, Twitter, Facebook, and other social media platforms, these cyberterrorists have been able to promote their nefarious activities because it allows easy dissemination of information beyond geographic locations, thereby, recruiting people beyond borders (Ogunlana, 2019). Amongst many other cyberattacks on the USA, in 2000, the Pakistani hacker, the self-styled Dr. Nuker, who took credit for the crack against the American Israel Public Affairs Committee, said he was the founder of the Pakistani Hackerz Club, with the aim of hacking for the injustice going around the globe, especially with Muslims (Schwartz, 2002). In the viewpoint of Baken (2013), the terrorist group operating from Africa, including the notorious Boko Haram (Jamā’aAhl al-sunnah li-da’wawa al-jihād), a Sunni group preaching religious extremism and Jihad in Nigeria, is basically influenced
by Islamic State of Iraq and Syria (ISIS). The group renamed itself as “Islamic State’s West Africa Province” (ISWAP) in April 2015. By using advanced technology like encrypted media such as Telegram to pass messages among members about clandestine operations, it oversees the propaganda routine of Boko Haram against the Nigerian State. Boko Haram (also known as Jama’ at Ahlissunnah lid-da’wawal-jihad that means western education is evil), a militant Islamist group over the years, has maximized the use of technology for spreading violent religious philosophy and hate messages, raising funds illegally, recruiting members, planning, and executing their attacks, leaving the Nigerian government confused about how to deal with them (Ogunlana, 2019).

According to Onimisi (2014), the activities of Boko Haram, in the name of religion and with no clear structure, is greatly influenced by the implications of globalization on Nigeria’s security. They use YouTube to threaten people through messages by inducing fear to force the Nigerian government to agree to their demands. In 2014, for instance, Boko Haram used YouTube to announce the abduction of more than 276 schoolgirls in Chibok town of the Northern Borno state (Daniel, & Maiangwa, 2014). Thereafter, they have spread to other parts of Nigerian states of Adamawa, Bauchi, Kano, Kaduna, and Yobe (Ogbonnaya & Eligiamuose, 2013).

Strategic messaging and communication, electronic jihad has become the reality of modern-day terrorism with the use of online media technologies to propagate sophisticated multidimensional information (Ogunlana, 2019). Schools, government agencies, churches, police stations, UN building in Abuja and bombing in market places (on market day) are some of the series of their attacks (Onimisi, 2014).

That they successfully execute these attacks proves that the government lacked the capacities to curb this emerging trend. While terrorism in Nigeria is as a result of colonialism, the long existence of terrorism could be said to be a result of globalization, with the terrorists comfortably using tools of globalization to execute their nefarious acts to the detriment of the government. These activities could develop into much more dangerous levels as government activities were taken online due to the large presence of cyber criminals commonly referred to as “yahoo yahoo boys” and hackers (Njoku, 2011).

But, Hübschle (2005) traced the pattern of terrorism in Africa to atrocities of the colonialist what is termed “colonial terror”. The colonial terror is a distinct form of terrorism perpetuated during colonial and post-colonial period. Therefore, a public culture was created in the Nigerian polity, in which the citizenry was inclined to commit acts of violence in response to exploitative colonial policies. To mention a few of their nefarious activities is the bomb blast at the Nyanya park outskirts of the Federal Capital Territory Abuja in 2014. In the Northern part of Nigeria and the entire country, Boko Haram has gained unauthorized access to the State Security Services (SSS), the Nigeria Secret Police, to retrieve vital information about government officials to target them for terror attacks, in the era of globalization (Oluwafemi & Onoja, 2015). Others instances include the attacks in during Independence Day celebrations, and in Jos, the Plateau state on Christmas Eve in 2010 (Njoku, 2011). Michael (2001) highlights that Boko Haram have no clearly defined ideas but they sought for an Islamic state ruled by Sharia law (Onimisi, 2014; Daniel & Maiangwa, 2014).
Cyberterrorism, according to Fayomi, et al (2011) has a global origin with every country or organization being a potential target. In most countries, it is an obvious threat to effective governance and national security. Cyberterrorism, in the viewpoint of Alao, Osah & Adam (2019), is a conglomeration of cybermetrics and terrorism. Also, it could be said to be the illegal use of computer or computer network to deliberately unduly compel, damage, seriously intimidate, harm, destabilize or coerce a government or international organization to do or prevent them from doing a particular thing in furtherance of the terrorist’s socio-economic, political or religious agenda. Interestingly, these cyberterrorists are commitment to staying a step ahead of other internet users whether governments or security agencies in order to make it difficult to pin down their activities.

According to (Podhorec, 2012), in this information age, the superiority of information is one of the main goals of NATO (North Atlantic Treaty Organization) transformation processes. As such, the aim of information security is to eradicate the challenges of operating information systems and communication in order to achieve high resilience, reliability and effectiveness. However, cyberattacks can be said to be a security threats that do not directly affect the security of a country but threaten its allies. They may be a new form of criminal or terrorist attack, or a new form of warfare that might be used to destabilize societies. However, leaking and interfering with strategic information of organisations and states may threaten strategic interests. Alao, Atere & Alao (2012), quoted retired Major Chris Moghalu of the United States of America’s military who said that Boko Haram received over $70 million, from Al-Qaeda groups in Saudi Arabia and the UK, between 2006 and 2011 for its insurgent activities in Nigeria. The identification and control of all the interconnected operations in an organisation is a requirement for the effective operations of such an organization (Podhorec, 2012).

**Fig 1: Nexux between globalisation, terrorism, cyberterrorism, and insecurity**

![Diagram showing the nexux between globalisation, terrorism, cyberterrorism, and insecurity.](image)

**Source: Authors’ construction**

Activities that define cyber-terrorism include posting offensive content on the internet, sending pornographic e-mails to minors, defacing webpages, stealing and posting credit card information on the internet, using a computer to cause damages, and clandestinely redirecting internet traffic from one site to another, etc (Podhorec, 2012).
With the constant changes in the cyber domain, the international law governing it struggles to stay constant and relevant to it in attempts to construct enforcement mechanisms (Roberts, 2019). The tools and methodologies of cyber terrorism include but are not limited to Trojans, denial of service attacks, worms, cryptography, and viruses (Nagpal, 2002). Karascasulu (2006) argued that today, global terror is a giant problem for all humanity.

Benson (2014) argued that as terrorists increased their use of the internet, security apparatus too have greatly outpaced them, thereby reducing the rise in cyberterrorism. The world’s first cyberattack that threatened the national security of an entire state occurred in Estonia in April 27, 2007. And in a few hours, the culprits hacked and crashed the websites of leading banks, newspapers and government communication systems were compromised as well. Thousands of zombie private computers around the world were used to carry out this attack (Shackelford, 2010). Other states that were attacked include Lithuanian, South Africa, Belarus, and Nigeria was not left out as it has been attacked more than any other country in Africa, and the third in the world after the United States and Britain respectively (Chiroma, Abdulhamid, Ya’aGital, Usman, &Maigari, 2011).

**Cyberterrorism and Globalisation**

With the consideration of the aforementioned, Nelson, Choi, Iacobucci, Mitchell& Gagnon (1991) defined cyberterrorism as the unlawful destruction or disruption of digital property in order to compel governments or societies in the pursuit of goals that are religious, ideological or political. According to Foreign Broadcast Information Service (FBIS) (2002), the Japanese government deem cyberterrorism as seriously affecting information systems of both private companies and government ministries and agencies by gaining illegal access to their computer networks and destroying relevant data.

Cyberterrorism is associated with hacking, hacktivism and cracking. It started with disrupting activities on the internet as a way of drawing attention to some political demand, to former employers hacking business’ systems with the aim of stealing, altering data, or engaging in other malicious activities. Initially, hacking was anchored on two ideologies, firstly, the sharing of information freely and a prohibition against harming, altering, or destroying any information that was discovered through this activity. Hence, hackers were no longer seen as explorers but malicious intruders (Collin, 2003).

Urbas and Choo (2008) asserted that it was in 1837 that telecommunications technology was developed and thereafter, the first cybercrime was committed around 1867. According to Ali, Anjariny, Habib & Nyakwende (2018), the Federal Bureau of Investigation (FBI) terms cyberterrorism as any criminal activities carried out with the aid of computer systems and telecommunication networks with the intention of inciting violence, including destruction and disruption of services. This was corroborated by Grabosky& Smith (1998) who recorded cases of illegal interception.

Majorly, this hackers or terrorist are usually young and vulnerable males (Taylor, 1999).Moreso, these hackers commit acts that are not just of disruption, but destructive and may end up in the killing of people that may hinder their course (Collin, 2003). Basically, information about the vulnerabilities of different systems are usually shared online between
hackers on computer web sites, bulletin boards, news groups, and other forms of electronic association, and this information can be gotten without stepping ones’ foot in the target country.

Cyber-terrorists are professionals, also known as cyber mercenaries that are highly skilled based on training from government agencies or corporate intelligence departments that work on the open market as the real threat. Examples are the Colombian drug cartels and the Amsterdam-based gangs that are rather unpopular unlike amateur hackers who receive most publicity (Hoo, Goodman & Greenberg, 1997).

Christen, Denney, and Maniscalco (2002) argued that Kevin Mitnick, the world’s most famous computer hacker, though unpopular, was labelled a “computer terrorist” by the US Department of Justice. Furthermore, cyber-terrorists have the tendency to crash computer networks, causing functional paralysis and even significant financial loss that could threaten lives or even kill for any reason (Hoo, Goodman & Greenberg, 1997).

In Nigeria, Gantz (2013) from his study indicated that the agents of cyberattacks entrench or implant fake software with dangerous malware as a way of preying on unsuspecting computer users who are unaware of the potential dangers in this software. Cyberattack crimes have outweighed illegal drug trafficking in all measure and in every 3 seconds, the identity of an individual can be gotten, an unprotected computer system without an effective security system, that is connected to the internet can become infected within four minutes (Fayomi, et al, 2011).

Cyberattacks have been widely acknowledged as computer-to-computer attacks undermining the confidentiality, integrity, and/or availability of computers and/or the information they hold (Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue & Spiegel, 2012). According to Aliyu (2012), finding how to defeat international terrorists and to promote their economic interest and democratic values was the major security threat to some powerful nations like the USA and its allies as the security threat differs amongst nations. However, Nigeria as a sovereign state has its own peculiar security threats that are based socio-economic and political circumstance (Onimisi, 2014).

Although they use the internet as a site for political action, hacktivists are not cyberterrorists since they are mainly engaged in disruption and not destruction (Deibert, 2003). On the other hand, cyber criminals are said to be primarily concerned with making illegal financial gains, as their motives, with the use of the computer over the internet instead of attacking the internet infrastructure itself (Mates, 2001). Their activities include the theft of electronic funds, the theft of credit card information, cyber extortion, and outright fraud (National Communications System, 1991).

Martin, Susanne, and Leonard (2016) asserted that transnational terrorists apply online tactics like cyber-mobilization and computer malware as economic weapons. Ogunlana (2019) argued that the internet facilitates transnational terrorism by influencing particular anonymity, abundance of information, and the cheap nature of online communications. And Minei & Matusitz (2012) added that these communication networks and social media give
room for unions to form, and the spread of important information tolerates individuals who are influenced by the terrorist messages to act and attack their targets.

Of late, social media platforms have become part of everyday life and terrorists use these platforms to disseminate messages of fear and spread hate and violent religious messages to attract young people to join them. Experts have singled out Twitter as the most popular platform among terrorist organizations like British Jihadist, working for ISIS in Syria, threatened the United States of America, using Twitter (Berger, 2015). Thus, social media has heightened the recent upsurge of lone wolf terrorism around the world (Stuart, Jarvis & Chen, 2017). Also, they inspire these lone wolves to commit acts of terror against their native land on their will. In addition, they engage in cybercrime such as hacking, identity theft, extortion, cyber exploitation, money laundry to fund their terrorist operations, illegal gambling, the distribution of child pornography, and phishing scams. They are known to target and rob public institutions like offices, banks, and businesses, and they are financed either through virtual or physical means (Ogunlana, 2019). Copyright infringement, bullying, and cyber stalking are some of the other crimes of cyberterrorism (Fayomi, et. al., 2011).

One major disadvantage of globalization is that it has caused a complex network of illicit markets, which consists of trafficking of drugs, human organs, and arms, prostitution, smuggling, cybercrime such as child pornography and slavery. Transnational networks have been improved by both the criminals and the terrorists to increase their activities, strategies, and logistics to operate across the continents (Ahmed, 2016). However, Michael Vatis, former head of the US National Infrastructure Protection Center (NIPC) on the other hand, viewed hacktivists as committers of low-level cyberterrorism (Denning, 2000). Therefore, Collin (2003) concluded that cyber-terrorism is when cybercrime is used to enhance terrorism through fear, oppression, and intimidating their victims. And Adomi & Iggun (2008) argue that cybercrime is an illegal act that is performed with the use of computers and computer networks to create and distribute malware, and involves impersonation, denial of services, the disturbance of network traffic, extortion, and the distribution of child pornography. However, the thin line between cybercrime and cyberterrorism cause researchers and the media to use both terms interchangeably but they can be differentiated by the motives, targets, and the actors.

While cyberterrorists are driven by motives such as ideology, political change, religion, social change, or vengeance as a way of intimidating a government or the general public, cybercriminals launch attacks for personal financial interest (Ogunlana, 2019).

Cyber terrorism is another emerging trend of terrorism in Nigeria. Although Nigeria is still struggling to reach a level of Information and Communication Technology needed to electronically run every activity of the government, if the government successful takes all its activities online, the existence of cybercriminals in the country is a warning sign of a possible bleak future with an estimate of about 80 million computers in Nigeria. Each of these computers could be a foot soldier, even by an attacker in another country to achieve a deadly goal, without the suspicion of the owners. There are many incidents of how cybercriminals and hackers have swindled individuals and corporate entities in and outside the country and these hackers or cyber criminals, popularly known in Nigeria as “yahoo yahoo boys,” could
be hired by these terrorist groups to jeopardise the nation’s network system in the nearest future (Njoku, 2011).

**Impact of Terrorism/Cyberterrorism on Globalisation**

ISIS, over the years has, been the most powerful terrorist organization in modern history, having sophisticated cyber capability. ISIS, in collaboration with other terrorist groups like Boko Haram and Al Shabab, by using over 21 languages over the internet, has recruited many young jihadis through YouTube videos, memes, tweets, and other social media postings and flooding the cyberspace for their sympathizers to retweet, like, or endorse their materials to recruit members into their folds (Allison, Speckhard, & Yayla, 2017). With the illegal trafficking of firearms according to Olowojolu and Ake (2015), human security became a challenge in Nigeria. Inarguably, the leading example of social globalization that brings about terrorist military globalization is the Al Qaeda network that is known worldwide and operates in more than sixty countries (Economist, 2001).

The failure of many Arab-Muslim countries to deal effectively with the conditions within their own countries gave rise to the Islamic fundamentalism, Al Qaeda’s network that has been supported and strengthened over time (Economist, 2001). These terrorist organisations have a global reach; they mobilize new members and instil loyalty among their followers through persistent and clear communication. By decentralising their activities, they make it rigorous to target them through conventional military tactics, and using violence to threaten them does not create any positive effect. Hence, the need for an innovative strategy to deal with threats from these cyberterrorists. However, they are susceptible to deception and failure in cyberspace as much as they succeed in it as well (Schultz, 2015).

In 2013, Nigeria that boasted of about 29% internet penetration rate with about 40 million internet users and 70 million users were projected in 2015, the highest in Africa, had suffered for years from cyber related crimes (The Guardian Nigeria, 2013). Isaac (cited in the Guardian Nigeria, 2013), reported that Nigeria was a fast emerging market and risked higher foreign invasion of cyber-attacks because of the rate of internet utilization. It is this influx of foreign investors into the country that has put the country on the international spotlight in contemporary cyber related crimes. The cyberattacks activities dominant in Nigeria include hacking, yahoo attack, cyber stalking, pornography, credit card or ATM fraud, software piracy, salami attack spoofing, internet relay chat (IRC) crime, denial of service attack, virus dissemination, phishing, cyber defamation, cyber plagiarism, and cyber terrorism (Olusola, Samson, Semiu & Yinka, 2013).

Niger Cyber Hacktivists, a group of Nigerian hackers, attacked government sites including the National Poverty Eradication Programme website and the Niger Delta Development Commission, posting a letter protesting against misappropriation of funds by the government and the country’s Freedom of Information Act. Later in January 2013, the Economic and Financial Crime Commission (EFCC) was attacked in response to reports of corruption. Cyberattacks, in the form of denial-of-service and computer bugs, cost the Nigerian government about $200 million annually. The exponential growth in mobile telecommunication users and the rise in social networking, potential sources of globalization, especially among the multitudes of unemployed youths in Nigeria are the twin factors that
have contributed to the increase in cyberterrorism in Nigeria. However, the existing fitness to prevent, screen or track cyber security issues is relatively low as a result of the forces of globalization (Ogunlana, 2019).

The way forward
Worthy of note is that the objectives of the terrorists in Nigeria are achieved through the mass media. This, they achieve by manipulating the populace with fear and terror of impending attacks. Recently, there have been reported cases of threats to attack Lagos and Abuja. These threats were quickly disseminated and created the impression that the government could no longer protect its citizens from the activities of these terrorists. There are several ways in which the government can adopt in order to put cyberterrorism to check, they include the following recommendations:

1. The government should develop models for implementing principles which modify risk assessment, the proposal and implementation of security, security management and repeated security evaluation.
2. All the staff of an organisation are needed for the security of the information systems within such organisations in addition to the involvement of external entities and third parties as well.
3. The preparation, training, and education of personnel in the field of cyber security both locally and internationally including the Nigeria Police and other security agencies, and the transfer of technology between countries should be encouraged by the Nigerian government.
4. Counterterrorism measures and robust cybersecurity technologies and tools such as denial of the enemy, cyber sanctuary, and the elimination of terrorist resources that enable the group to conduct cyber mobilization and recruitment are to be adopted. Also, the creation of a secure environment, including comprehensive and integrated information operation (IO) are critical factors to consider for counterterrorism operations.
5. The enactment of laws by the judiciary and its enforcement will contain cybercrime, cyberterrorism, and other related offenses such spreading violence and hate speech should be encouraged. Also, law enforcement and intelligence agencies of some countries can use AI and machine learning to detect, take down faster than humans can do, and respond to different kinds of cyber threats in the abuse of cyberspace is expedient. In addition, Dialogues universal legalisations are necessary in order to build an understanding of these issues between countries.

Conclusion
Obviously, the explosion of internet and websites operations advanced innovation and development in different spheres of the Nigerian economy. Business networking and communication channels that have enhanced globalization and faster dissemination of ideas in different human endeavours have greatly increased via the use of internet but the rigor and negative results associated with this current development in the use if the internet and web activities have threatened internet users and cyber domains in general. Since traditional law and international agreements cannot easily resolve these challenges that are created by increased connectivity, it is necessary that the internet frontline gets a proactive defense because censorship and the removal of terrorist content are reactive and not effective.
Since the government’s counter-narrative efforts in combatting online terror acts have proven abortive, there is a need for finding a strategic solution to combat these extremist narratives in the cyberspace with growing fear that terrorists can execute more destructive acts. Internet users should be guided both technical and legally so as to discourage their involvement in terrorist enticement through the publicity of violent ideology and spread propaganda on social media. Thus, if Nigeria must claim decimating the Boko Haram insurgents, and remain the giant of Africa, this publication recommends that the Federal Government must display sincere commitment with huge investment in not only in military (hardware) warfare but to cyberterrorism through establishing effective institutional mechanisms for managing cyber security; funding and implementing the measures established in line with international best practices. The government should also ensure that adequate funding is made for security and infrastructural development of all parts of Nigeria, in addition to investing in research for local capacity building to detect, deter, and effectively respond to threats emanating from internet sources. If there is co-operation amongst all the countries of the world in regard to cyberterrorism, then the menace will be resolved in a way that will guarantee a sustainable future.

References
The Brookings Institution.


Guardian (2004). Suspect Links e-mail Address to Al Qaeda. August 5, p.1


Propaganda.” GSCP Policy Paper 2: 4. Available at: https://www.jugendundmedien.ch/fileadmin/user_upload/3_Medienkompetenz/Gege


