ALSYSTECH
Journal of Education Technology

e-ISSN : 2988-442X
p-ISSN : 2988-4403

Index : Dimensions, Scilit, Crossref, Garuda, Semantic, Google Scholar, Base, etc

https://doi.org/10.58578/alsystech.v2i3.3237

ISSUES AND PERSPECTIVES ON CYBERTERRORISM AND INFORMATION SECURITY IN NIGERIA

Josiah Sabo Kente & Jesse Ishaku
Nasarawa State University, Keffi, Nigeria; Taraba State University, Jalingo, Nigeria
drjosiahsabokente@nsuk.edu.ng; jesseishaku@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
Jun 17, 2024	Jun 20, 2024	Jun 23, 2024	Jun 26, 2024

Abstract

The advent of information and communication technology (ICT) and the internet in Nigeria offer endless opportunities and also raise a lot of concerns bothering on cybercrime, cyberterrorism, information and human security. Recently, Nigeria has experienced an unprecedented surge in cybercrime, with potentially disastrous consequences for the country's socioeconomic and sustainable growth. Consequently, the complexities and horrific nature of cyberterrorism in recent times have increased proportionately which calls for prompt action. This study therefore, examines the effects of cyberterrorism on information and human security in Nigeria. Anchored on the technology-enabled crime and risk society theory and integrative literature review approach, the study revealed that, aside from the fact that information security is important for the continued existence of individuals, organisations and government in Nigeria, different terrorist and secessionist groups in Nigeria such as Boko Haram have been using the Nigeria's cyberspace to mobilize and train its members, raise funds as well as propagate their nefarious agenda. The study however recommends among many things that, the Nigerian government should strengthen the Cybercrime Prohibition and Prevention Act 2015 while also ensuring the establishment of strong legal, institutional and security frameworks in line with the United Nations Security Council Resolution 2341 (2017) and the United Nations Global Counter-Terrorism Strategy (GCTS) in order to fight cyberterrorism in Nigeria.

Keywords: Cybercrime, cyberterrorism, information security, Nigeria

INTRODUCTION

The development of the Internet in the 1970's by the United States Department of Defense and the subsequent adoption of this ground-breaking technology the world over has indeed revolutionized and redefined almost all the facets of human existence. The technological advancements of faster and smarter microprocessors as well as the development in rugged optical cables has actually accelerated the transmission and processing of information across frontiers. The World Wide Web, which was first utilized by businesses as an electronic billboard for their goods and services, evolved into an engaging marketplace for consumers to trade commodities and information. Platforms for digital media have been seen as being crucial for society in the twenty-first century. They have proven helpful in almost every element of human life. Digital media has shown to be highly beneficial in areas of society including politics, religion, the economy, health, and agriculture, among others. Email for instance, has become one of the main platform for business and personal interactions because it allowed for almost instantaneous sharing of information.

According to Athique (2013), the prevalence of digital media platforms is significantly altering how individuals interact with one another. He continues, that because of how digital media platforms have been embraced in modern culture, people do not have time to consider the repercussions of such acceptance. The advent of digital media has led to changes in both media consumption and sharing practices. Social networks and digital platforms are used to spread media material and sell promotions in the twenty-first century

(Nayyar & Watson, 2016). Any type of communication that is encoded in a machine-readable manner is referred to as digital media. Using electronic devices, such media enables the creation, viewing, distribution, alteration, and preservation of material. To summarize, digital media platforms produce, process, store, and retrieve material primarily using codes. Compared to their analog equivalents, they are more user-friendly and can handle larger amounts of information. Social media, digital photos, video games, software, web pages, digital video, and websites are a few examples of digital media. Digital music (like MP3), data and databases, as well as electronic literature, are more examples (Koehl, 2013; Dewar, 1998).

Consequently, there are worries that digital media could present a challenge to cyber security, as cyber security issues have continued to resurface in the face of increasing digital media options, leading to a number of cases of cybercrimes, even though it can be argued that digital media platforms have made task execution and information sharing a lot easier. As access to information becomes easier and spread of information moves at the speed of light; and as innovation keeps advancing, so do the benefits and the challenges. The over dependence on this technological development has created numerous dangers and vulnerability for people, government and businesses (Aboelfotoh & Hikal, 2019). Through the use of electronics and the internet, ICT has unified many economies throughout the globe. ICT and computer networks are currently used by many business entities, including banks, to carry out both simple and complex activities. Anyone may now purchase goods on the electronic market, including cybercriminals. According to projections, global expenditure on cyber security would rise from $75 billion in 2015 to $170 billion in 2020, a 126% increase (Ibrahim, 2019). While corroborating, Anthony, Ishmael, Santa, Shemyakin, Stanull, & Vandeweghe (2016) state that, people, organizations and modern society are overly reliant on technology as a whole. However, although technology brings about ever-greater benefits, it also poses threats and provides a place for cybercrime, modern undercover work, digital attacks; and protecting this has thus become a topmost priority.

It is worthy to note that, cybercrime or cyberterrorism is actually a transnational issue that requires a multifaceted approach to better understand and subsequently solve some of the challenges associated with it. For instance, according to Gehem, Usanov, Frinking, & Rademaker, 2015), there have been numerous researches that assessed the causes, element and dangerous implication of cyberterrorism. The multiplicity of these reports indicate the rising consciousness of citizens, business organisations and establishments as well as the governments across the globe. Because millions of computers are interconnected globally, this makes it even easier for cybercriminals or cyberterrorists to perpetrate their heinous deeds from the comfort zones of their homes. The danger to an individual is when they access an unprotected website and gets vulnerable, and the potential risk for an organization is when its internal network is compromised, rendered unreachable for 24 hours, or have its trade secrets stolen, while governmental risk is when cybercriminals or cyberterrorists restrict public websites or disclose official documents online (Brenner & Koops, 2006). According to Adebayo (2017), the broadest definition of cybercrime is any illegal conduct involving an information technology infrastructure, including unauthorized access, information blockage, framework impediment, misuse of gadgets, fake (ID theft) and electronic fraud. Based on the foregoing, there has been increased worry about how susceptible the Nigerian Internet space is to criminal activities. Therefore, this study examines the issues and perspectives on cyberterrorism and how it has affected information and human security in Nigeria.

Statement of the problem

Cyberterrorism typically have gravely detrimental effects on the security of information, money, and people. This elevates the subject of cyber security danger to a severe one that requires experts and academics to give it their full attention. However, the rise of digital media and its subsequent adoption and use by the general public have caused cyber security issues. Tension about the connection between digital media and cyber security concerns has increased due to the rise in cybercrimes (Asogwa, 2020). Since the turn of the century, Internet use in Nigeria has grown. From 3.5% in 2005 to 47.4% in 2014, the population's proportion of internet users rose noticeably (WDI, 2016). Similar to this, it has been predicted that tele-density in Nigeria will keep rising over time (Asemota, Ogujiuba, Aderemi, & Mustapha, 2015).

In Nigeria, the widespread use of the Internet has had unexpected consequences, serving as a shelter for criminals. Despite growing awareness and focus on the problem in Nigeria and throughout the world, cybercrime has remained a difficult problem. For instance, in 2016, 43% of all financial losses from fraud were attributable to cybercrime (Ibrahim, 2019). Welfare losses, business interruption, profit reduction/rising operational costs, revenue losses, etc., have a detrimental impact on people, businesses, and the government at large. This constitute a problem for the growth and development of the Nigerian state.

Theoretical framework

The technology-enabled crime and risk society theory serves as the foundation for this study. One academic who highlights the applicability of the technology-enabled crime theory to the expanding telecommunications sector is McQuade (2006). He points out that, it covers offenses that are directly perpetrated against computers and computer systems and are sometimes referred to as high tech crimes, computer crimes, or cybercrimes. He makes the argument that the use of the Internet or other technology aids in the commission of conventional crimes and can take the form of fraud, scams, threats, or harassment, which adds complex problems to prosecuting traditional crimes. Additionally, McQuade (1998) notes that it might be challenging to comprehend and manage sophisticated criminality, especially at first, due to obstacles brought on by periodic technical rivalry between law enforcement and criminals. This suggests that criminal elements would always try to reinvent their criminal inclinations, and that security services will likewise make an effort to decipher and prevent new types of crimes.

Practically, technology-enabled crime theory is a synthesis of many criminological ideas that aims to improve societal comprehension of why crimes connected to computer and telecommunication technologies are getting harder to stop, investigate, and manage (Essays, UK, November 2013). Given that it may be challenging to describe criminal conduct using only one theory, Patchin & Hinduja (2011) put an emphasis on the usefulness of the poor self-control theory and the strain theory. According to Grabosky & Smith (1998), recent telecommunication crimes include illegal telecommunications interception, electronic vandalism and terrorism, stealing communications services, telecommunications piracy, pornography and other objectionable content, telemarketing fraud, electronic funds transfer crime, and electronic money laundering.

The technology-enabled crime theory is relevant to this study because terrorists increasingly use information technology to raise money, rally followers or recruit, plan attacks, and watch security services in order to make the government appear helpless to deal with the issue. This erodes public morale toward the government and the security agencies' commitment to stop terrorist crimes. The theory emphasizes the threats posed by emerging forms of cybercrime, transnational crime, and terrorist networks that defy conventional methods of criminal justice and security measures for preventing and controlling crimes, even though technological development has more benefits than drawbacks. As a result, it offers information about how to comprehend the modern tools and methods that cybercriminals, particularly terrorists, utilize in this respect. This explains why Cruz (2013) claims that despite the fact that social, economic, and political transformations have been facilitated by the development of the internet over the past two decades, geography has been rendered obsolete because national borders have become nebulous and porous.

On the other hand, Beck (1992) popularized the risk society theory, which was connected to a transition from the traditional to the industrial society and towards a new contemporary risk society that is frequently personalized, global, and self-confrontational. A risk society is seen as a methodical approach to addressing the dangers and insecurity that modernisation itself introduces. According to the idea, given the characteristics of contemporary societies, risk tends to increase as social systems of production, consumption, governance, and technology control become more complicated (Jonathan, Nick, & George, 2004). This prompted Beck (1992) to claim that danger is increasing in modern society more so than it is decreasing as a result of scientific and technical advancement. This was made possible by the Internet revolution and the rising use of mobile devices, which allowed for immediate communications, banking, financial transactions, and learning throughout the globe as the world has become a global village. This is made simple by the fact that millions of individuals across the world have simultaneous access to computers and other usable electronic devices, making it possible to carry out terrorist actions, peddling, fraud, and frightening images.

This theory is relevant to this paper because, in recent years, criminals under all guises, insurgents, thieves, kidnappers, and terrorist organizations have used the Internet just as successfully and effectively as innocent and honest users to show off their skills, incite fear, and carry out their nefarious operations. The ease with which people may use the internet, in fact, cannot help but aid terrorists in their efforts to coordinate attacks, exchange experiences, recruit foot troops, raise and transfer money. It follows that the inappropriate uses for which internet infrastructure has been put are raising the stakes for the entire system and posing a danger to people's security.

Conceptual Clarification

Cyberterrorism

Cyberterrorism is a combination of two (2) words – "cyber" and "terrorism. Conceptualising cyberterrorism therefore requires that the two (2) words "cyber and terrorism" be explained in order to put things in proper perspectives. "Cyber" as a standalone concept may be referred to as the generic term used to explain things that are associated with the computer and the internet as well as their services and/or uses. It also encapsulates information and communication technologies as well as the cyberspace generally. According to Jongman (2004) the definition of what constitutes terrorism stems majorly from the domain of the United States and its agencies. US Department of State defines terrorism as "premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents, usually intended to influence an audience." Terrorism is an anxiety-inducing pattern of recurrent violent action, used by (semi-) clandestine individual, group, or state actors for specific, illegal, or political purposes. Unlike assassination, the primary targets of terrorism are not the direct targets of violence (Jongman, 2004). It is the "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological" (US Department of Defense).

Cyberterrorism on the other hand, entails the use and deployment of communication, computer and internet networks to cause fear, intimidation, injury and havoc as well as unleash violence on an unsuspecting audience or government for the purpose of achieving selfish and often nefarious goals by the perpetrators. Cyberterrorism also refers to any deliberate or inadvertent attempt or activity on computers, networks, or other devices with the goal of impeding any government endeavor to accomplish anything by a method of remote or near access, either directly or through a proxy.(Gérôme, 2017 as cited in Ahmad, 2019). According to Heickero (2007), cyberterrorism refers to actions taken against vital information infrastructure, whereas traditional terrorism implies the use of violence or threats of violence in order to further a cause. Denning (2004) sums up the idea of what could be termed as cyberterrorism as thus:

> Cyber-terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers,

networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Information Security

Information security can be quite difficult to define depending on the perspective or the angle one looks at it from. According to Lundgren & Möller (2019), defining information security can be divided between "soft issue information security" (such as humans, organizations, culture, ethics, policies, and law) and more technical issue information security. They however sum up the definition of information security into what they called the dominating CIA definition of information security in the literature based on the triad properties as thus:

1. Confidentiality: "Property that information is not made available or disclosed to unauthorized individuals, entities, or processes;
2. Integrity: "Property of accuracy and completeness,
3. Availability: "Property of being accessible and usable upon demand by an authorized entity" (Lundgren & Möller, 2019, p. 420-421).

On his part, Aliyu (2023), information security is the practice of safeguarding data by reducing or eliminating the likelihood of improper or unauthorized access to it, as well as the illegal use, exposure, disruption, erasure, corruption, alteration, assessment, recording, or devaluation of data. It also includes planned measures to lessen the adverse impact of those kinds of situations. Consequently, the primary objective of information security is to safeguard the availability, confidentiality, and integrity of data so that policies may be implemented effectively and without impeding the growth and productivity of not only organisations but government as well.

METHODS

The integrative literature review approach is employed in this research study to thoroughly examine the topic under examination. An integrative literature review method is a non-experimental approach where researchers systematically search, categorize, and thematically analyze previous qualitative and quantitative research studies on the topic under investigation in order to objectively critique, summarize, and draw conclusions about the subject matter (Christmals & Gross, 2017, p. 7). From the foregoing, it is obvious that the above method has the potency to enable the researchers to objectively critique, summarize and make conclusions from data obtained from the literature on cyberterrorism, information security and digital media in Nigeria.

RESULTS AND DISCUSSION

Cyberterrorism and Information Security in Nigeria

Globally, according to Conway (2008), numerous events that occurred after the fall of the USSR brought attention to the expanding role of information technology in matters of both domestic and international security. Examples include the advanced IT skills used by US forces in the first Gulf War (1990-1991); and the expanding worldwide scope of media coverage as seen in the battles in Somalia (1993) and the Balkans (1992-1999). The May 2007 cyberattack(s) against Estonia and the growing use of the Internet for "infowar" by al-Qaida and a variety of other sub-state political violence groups have drawn a lot of attention to the increased system failures brought on by hacker's activities. These and other incidents emphasized the increasing reliance of governments, especially the US, on information technology, which raised concerns about a fundamentally new security threat: the potential for information systems to act as both weapons and targets of attack. An almost obsessive focus on the potentially catastrophic risks posed by cyberterrorism has been a significant component of the post-11 September 2001 measures to bolster US "homeland security." One of the major fears was that "opponents of the US, unable to defeat US forces on the traditional battlefield, might explore new means to inflicting harm on the lone surviving superpower" (Pollard 2004, p.43).

A research published in June 2001 found that 75% of Internet users worldwide think cyberterrorism exists. In a study done in 19 major cities throughout the globe, it was discovered that 45% of respondents agreed fully that "computer terrorism will be a growing problem,” while 35% agreed somewhat (Poulsen, 2001). A 2003 survey by Federal Computer Week and the Pew Internet and American Life Project found that about half of US citizens worry that terrorists will launch cyber-attacks on those critical infrastructures that operate the banking, energy, and transportation sectors. In a July 2002 survey by the American Business Software Alliance, 82% of information technology professionals were reported to believe that US businesses were unprepared to deal with cyberterrorism (King, 2002). According to “globalization 4.0”, a study from the World Economic Forum (WEF), more organizations than ever are conducting business online (Davos, 2019). However, many political, military, business, academic, and media commentators have predicted deadly terrorist attacks on (and with the assistance of) the computerized infrastructures that now form the essential foundations of regular urban life not only in the US but in other countries as well.

Based on the aforementioned research evidences and figures, there is a clear demonstration that businesses, governments and individuals the world over are concerned about information security as well as cyberterrorism and its damning consequences. Nigeria as a country can never be an exception to this looming danger posed by cyberterrorism. Consequently, attacks by cybercriminals pose serious risks to corporate organizations and the financial sector in Nigeria. As a result, businesses and financial institutions with more than 50 years of experience, such as Leadway Assurance Nigeria and Bode Ogunleye & Associates, have a Cyber-risks insurance policy to guard against cyber-attacks (Businessday, 2021). However, a team with extensive knowledge of cyber-security breaches created the policy. As a result, new techniques are required to aid, in the case of an incident, prevent future financial loss due to cybercrime owing to its prevalence (Raji, 2022).

Nigeria's history with cybercrime has made it one of the most popular channels for corporate espionage and money laundering. In other words, cybercrime has an impact on all sectors, including financial services, e-commerce, insurance, airlines, media, oil and gas, and education (Omodunbi, Odiase, Olaniyan & Esan, 2016). Vulnerability remains a concern for Nigerian corporate enterprises, nevertheless. Vulnerability factors include the growth of cybercafés, unemployment, poverty, and factors like corruption, a lack of infrastructure, lack of national functioning databases, and lack of standards in national central control, and domestic and international law enforcement. Additionally, the porous nature of the Internet is a factor that has increased the vulnerability of people, companies, and Nigerian residents to cybercrime (Adebayo, 2017).

Furthermore, Nigeria's decision to become cashless has increased the risk of cybercrime. In order to develop new approaches to assess and survey the assurance of data and information for businesses and individuals, professionals are compelled to research these vulnerabilities in order to look into the problems of data security, information insurance, and network safety. Cyberattacks are expensive and can cause a range of issues, including monetary loss, reputational harm, and psychological pain. They may also have an impact on people's social networks and organizational tools. Depending on the type of attack, a company's network and system maintenance and security expenses may change.

Be that as it may, the need to urgently safeguard data and other organizational resources from exposure to hackers' activities has been driven by the spate of growing digital footprint prevalence and complexity in cyberattacks. Because of the additional expenses for boosting security against cyberattacks, this has led to an increase in the cost of adopting ICT within institutions. According to Gartner (2018), global investment on information security will more than double to $124 billion in 2019. However, some security analysts predict that spending on cybercrime will increase fourfold from its 2015 level to over $2.1 trillion by the end of 2019 and will exceed investment on cybersecurity by a factor of more than 16 times.

Afolabi & Raji's (2022) proposal for security intelligence can be one of the techniques to be utilized proactively in order to address cybercrime threats in companies. According to Crump (2015), security intelligence is a crucial component and the foundation upon which choices about enterprise security should be made. In any event, new varieties of cybercrime risks that often result in information loss and data misuse have emerged concurrently. As a result, maintaining information security in complex frameworks is substantial and crucial, especially in organizations where a larger number of people are using the internet to collaborate. Therefore, security intelligence examines information vulnerability, methods for protecting an organization from internal and external threats, and techniques or tools for gathering and analyzing such information to support organizational policymakers.

Interrogating the Implications of Cyberterrorism in Nigeria

The cyberspace is the nervous system of the nation's infrastructure and is comprised of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructure work (National Strategy to Secure Cyberspace, 2003). The widespread use of internet services and the revolution in information technology have made it easier to do business internationally and bridge communication gaps between people and countries (Alao, Osah, & Adam, 2019). This interconnectedness offered by the cyberspace has made end users of internet services to deploy these opportunities and facilities to perpetuate different malicious and nefarious actions, the generic name of which is called cybercrime. Duson & James (2020) support that, with the development of computers, the internet, and other technical advancements, criminals began to engage in horrific illegal and antisocial behaviour. Cybercrimes include a wide range of illegal actions, including financial fraud, computer hacking, downloading pornographic photos from the internet, virus attacks, stalking, and building websites that incite hatred. Although cybercrimes may be defined as crimes that use networked technology as a medium (Wall, 2007), they are among the crimes with the fastest growth rates in the world (Erhabor, 2008).

Conway (2008) notes that several events after the fall of the Soviet Union demonstrated the increasing impact of information technology on the domains of both domestic and global security. Numerous political, military, business, academic, and media pundits have predicted lethal terrorist attacks on (and with the assistance of) the computerized infrastructures that today form the essential foundations of daily urban life in the United States. This assertion however does not preclude the Nigerian state as there are quite a number of instances where terrorist groups cash on the availability of the information and communication technology infrastructure to perpetuate and propagate their heinous agenda. While corroborating, Duson & James (2020) state that, attacks on the websites of the Nigerian government were said to have increased by around 60% in 2012. The conventional weapons used by conventional terrorists are no longer in the hands of cyberterrorists; instead, they have access to an entirely new arsenal of digital weaponry that can be used from anywhere in the globe to strike a target (Ayres & Maglaras, 2016).

Furthermore, although the internet has had a positive impact on businesses, organizations, and governments through the simplification of processes like sorting, summarizing, coding, editing, and the generation of customized and generic reports in real-time, it has also had unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft, and a burgeoning haven for cybercriminal miscreants to perpetrate their insidious crimes (Balogun & Obe, 2010).

Cybercrime such as identity theft, piracy and hacking have proven to negatively impact different economies of the world (Olusola, Ogunlere, Ayinde & Adekunle, 2013; Micheal, 2012; Shehu, 2014). Lieberthal & Singer (2012), observe that, the issue of cyber security has led to mistrust in the US-China relationship which equally suggest that such a mistrust can have an adverse effect in the world's economy generally. Also, cyber security threats are found to hit the stock markets to a large extent (Loeb & Zhou, 2011). In Nigeria for instance, software piracy, pornographic contents, phishing, and cracking are some of the cybercrimes that are prevalent (Olusola,Ogunlere, Ayinde & Adekunle, 2013). According to Moses, Targema & Ishaku (2022), the increasingly acknowledged link between careless use of social media platforms and the nation's increasing level of insecurity has provided reason for governmental actors' increased efforts to control social media use in Nigeria. This is because there are security threats in almost every region of the nation, and these threats together are currently boiling the political system.

According to Asogwa (2019), cybersecurity lapses may have detrimental effects on finances, data recovery times, and reputation as they are found to affect businesses both at the local and international levels especially as it pertains information/data security as well as profit maximization of different organisations. At least one cyber security breach occurs in a year for two out of every ten nonprofit companies (19%) and more than four out of ten profit-based enterprises (43%), 74% of enterprises and 53% of all nonprofits organisations feel that cyber security is a top priority for their organisations, two out of ten charities (21%) and less than three out of ten corporations (27%, compared to 33% in the previous 2017 study) have a documented cyber security policy or policies respectively (Department for Digital, Culture, Media and Sport, 2018). This statistics point to the fact that, not only do organisations around the globe needs to prioritize cyber security, but the government as well.

Consequently, increased system failures brought on by hacker activity have received a lot of attention lately, as demonstrated by the May 2007 cyberattacks against Estonia and the growing use of the internet by al-Qaida and numerous other sub-state political violence groups for "infowar" operations (Cobway, 2008). Similarly, the Boko Haram terrorist sect in Nigeria for instance, are seen to have used and deployed varying communication technology gadget made possible by the internet in showing the whole world how dangerous and deadly their attacks could be. This act of terrorism by the Boko Haram sect using the cyberspace can be aptly called "cyberbokorism." Be that as it may, every nation, including those with sophisticated technology capabilities like the United States, are now at risk of cybercrimes since they (cybercrimes) have developed past traditional crimes (Laura, 1995). If developed countries of the world such as the US is at risk of cybercrime as a result of how sophisticated technologies are as well as the paradigm shift from traditional to advanced cybercrimes in recent times, the resulting effect is that, developing countries such as Nigeria are more susceptible to cyberattacks/cyberterrorism than ever before. Be that as it may, the key to achieving global cyber security is the adoption by all nations of appropriate legislation prohibiting the misuse of Information and Communication Technology (ICT) for illegal or other purposes, including actions intended to compromise the integrity of national critical information infrastructures.

CONCLUSION

Cybercrime the world over has become an issue of grave concern as both individuals, organisations and government are trying so hard to protect their information and critical infrastructures from the activities of cyber criminals, hackers, and cyber terrorists. Terrorism in whatever guise, threatens the continued existence of human person as well as undermines government's efforts towards information and human security. Undoubtedly, as the development in information and communication technology (ICT) and the internet become rapid and permeates every facets of human endeavour, terrorist groups are also utilizing these opportunities and potentials to recruit new members, disseminate propaganda, train existing members, communicate, plot, raise funds, incite violence, perpetuate and execute their evil and heinous agenda. Sadly, cyberterrorism and its accompanying effects in Nigeria has become so rampant and glaring as different terrorist and secessionists groups have resort to using the porous nature of the Nigeria's cyberspace to inflict harm and pain, stir emotions, cause violence and disaster thereby undermining Nigeria's national security and development.

Be that as it may, the Nigerian government should strengthen the Cybercrime (Prohibition and prevention) Act 2015 in order to squarely address the issue of cyberterrorism and ensure the protection of information and data in the country. Also, the Nigerian Communication Commission (NCC) and Nigeria Information Technology Development Agency (NITDA) and other critical stakeholders should prioritize and organise awareness campaigns in order to highlight the dangers of cybercrimes and its ensuing consequences both on the perpetrators, the unsuspecting individuals and the government. Finally, strong legal, institutional and security framework should be established by the Nigerian government in line with the United Nations Security Council Resolution 2341 (2017) and the United Nations Global Counter-Terrorism Strategy (GCTS) in countering cyberterrorism in Nigeria.

REFERENCES

Aboelfotoh, S. F., & Hikal, N. A. (2019). A review of cyber-security measuring and assessment methods for modern enterprises. *JOIV: International Journal on Informatics Visualization*, *3*(2), 157-176.

Abraham, D. (2020). Impact of digital media on society. *International Journal of Creative Research Thoughts (IJCRT).*

Adebayo, A. (2017). *Cybercrime investigation and digital forensics*. Institute of Security Nigeria.

Afolabi, M. B., & Raji, G. A. (2022). Defeating the 21st century demon "Cybercrime" on corporate bodies in Nigeria: Is security intelligence a weapon? A quantitative study. *F1000Research*, *11*, 983.

Ahmad, A. S. (2019). Cybercrime and the sociological implication in the Nigeria's tertiary education system. *Fudma Journal of Sciences*, *3*(1), 249-257.

Alao, D. O., Osah, G., & Adam, E. M. (2019). Unabated cyber terrorism and human security in Nigeria. *Asian social science*, *15*(11), 1911-2017.

Anthony, M., Ishmael, M., Santa, E., Shemyakin, A., Stanull, G., & Vandeweghe, N. (2016). Estimating probability of a cybersecurity breach. *Risk Management*, *12*.

Araromi, M. (2018). Cyber-Terrorism under the Nigerian Law: A New Form of Threat or an Old Threat in a New Skin? *SSRN 3286617*.

Ayres, N., & Maglaras, L. A. (2016). Cyberterrorism targeting the general public through social media. *Security and Communication Networks*, *9*(15), 2864-2875.

Asogwa, C E. (2019). Public perception of the influence of digital media on cyber security in Nigeria. *Universal Journal of Electrical and Electronic Engineering 6*(5): 366-372, 2019 http://www.hrpub.org. DOI: 10.13189/ujeee.2019.060507

Asogwa, C. E. (2020). Internet-Based Communications: A Threat or Strength to National Security? *Sage Open*, *10*(2), 2158244020914580.

Asemota, O. J., Ogujiuba, K., Aderemi, T. A., & Mustapha, S. (2015). Modelling and Forecasting Teledensity using Univariate Time Series Models: Evidence from Nigeria. *International Journal of Statistics and Applications*, *5*(6), 279-287.

Athique, A. (2013). *Digital media and society: An introduction*. John Wiley & Sons.

Balogun, V. F., & Obe, O. O. (2010). E-crime in Nigeria: Trends, tricks, and treatment. *The Pacific Journal of Science and Technology*, *11*(1), 343-355.

Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17). Sage.

Brenner, S. W., & Koops, B. J. (Eds.). (2006). *Cybercrime and Jurisdiction: A Global Survey*. MC Asser Press.

Carnegie Endowment for International Peace. (2019). Timeline of Cyber Incidents Involving Financial Institutions. https://carnegieendowment.org/specialprojects/protectingfinancialstability/ timeline.

Christmals, C. D., & Gross, J. J. (2017). An integrative literature review framework for postgraduate nursing research reviews. *Eur J Res Med Sci*, *5*(1).

Conway, M. (2008). Media, fear and the hyperreal: The construction of cyberterrorism as the ultimate threat to critical infrastructures.

Crump, J. (2015). *Corporate security intelligence and strategic decision making*. Crc press.

Department for Digital, Culture, Media and Sport (2018). Cyber security breaches survey 2018.https://assets.publishing.service.gov.uk/media/5adf222ce5274a0d8209473e/Cyber_Securi ty_Breaches_Survey_2018_-_Main_Report.pdf

Denning, D. E. (2000). Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives. *Focus on terrorism*, *9*(1), 71-76.

Dewar, J. A. (1998). The information age and the printing press: Looking backward to see ahead.

Duson, N. A., & James, S. D. (2020). Cyberterrorism and the protection of critical information infrastructure in Nigeria: A Legal Assessment.

Erhabor, I. M. (2008). Cybercrime and the Youths (PGDE Thesis). *Department of Education, Ambrose Alli University, Ekpoma, Nigeria*, 37.

Gartner, S. (2018). Information security spending. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwideinformation-security-spending-to-exceed-124- billion-in-2019

Gehem, M., Usanov, A., Frinking, E., & Rademaker, M. (2015). *Assessing Cyber Security: A meta analysis of threats, trends, and responses to cyberattacks*. The Hague Centre for Strategic Studies.

Grabosky, P. N., & Smith, R. G. (1998). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. Transaction Publishers.

Heickero, R. (2007). Terrorism online and the change of modus operandi. *Swedish Defense Research Agency, Stockholm, Sweden*, 1-13.

Ibrahim, U. (2019). The Impact of Cybercrime on the Nigerian Economy and banking system. *NDIC Quarterly*, *34*(12), 1-20.

Jackson, J., Allum, N., & Gaskell, G. (2004). *Perceptions of risk in cyberspace*. Foresight Directorate.

Jongman, A. J. (2017). *Political terrorism: A new guide to actors, authors, concepts, data bases, theories, and literature*. Routledge.

King, B. (2002). Fear and lockdown in America. *wired. com. Online.*

Koehl, S. (2013). We need to act to prevent a digital dark age. *Wired: http://www. wired.com/2013/05/we-need-to-act-to-prevent-a-digital-dark-age/*

Laura, A. (1995). Cybercrime and national security: The role of the penal and procedural law. *Nigerian Institute of Advanced Legal Studies.* http://nials-nigeria.org/pub/lauraani.pdf

Lieberthal, K., & Singer, P. W. (2012). *Cybersecurity and US-China relations*. Brookings.

Lundgren, B., & Möller, N. (2019). Defining information security. *Science and engineering ethics*, *25*, 419-441.

Michael, K. (2012). Book review: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. *Computers and Security*, *31*(4), 634-635.

Moses, J. M., Targema, T. S., & Ishaku, J. (2022). Tale of an ill-fated scapegoat: National security and the struggle for state regulation of social media in Nigeria. *Journal of Digital Media & Policy*.

Nayyar, S., & Watson, W. T. (2016). Digital media and society implications in a hyperconnected era. In *World Economic Forum*, 1-64.

Olusola, M., Samson, O., Semiu, A., & Yinka, A. (2013). Cybercrimes and cyber laws in Nigeria. *The International Journal of Engineering and Science*, *2*(4), 19-25.

Pew Internet & American Life Project (2003) *Survey with Federal Computer Week Magazine About*

Pollard, N. A. (2004). Indications and warning of infrastructure attack. *Terrorism in the Information Age: New Frontiers*, 41-57.

Poulsen, K. (2001). Cyber terror in the air. *SecurityFocus. com*, *30*.

Shehu, A. Y. (2014). Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession. *Online Journal of Social Sciences Research*, *3*(7), 169-180.

World Bank Group. (2016). *World development report 2016: Digital dividends*. World Bank Publications.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.