Socio-Technical Perspectives On Cybersecurity: Nigeria's Cybercrime Legislation In Review

Wilson Nwankwo, Kingsley Chiwuike Ukaoha

Abstract: This paper is an attempt to analyze Nigeria's principal cybercrime legislation from social, technical and legal perspectives in a bid to highlight some perceived gaps, which may hamper the expected goals of the law. An exploratory narrative-textual case study approach is adopted in this paper and emphasis is made on some grey areas identified in the law. The points discussed include the concept of critical national infrastructure vis-à-vis critical infrastructure, and the responsibilities of some vital agencies and ministries. A careful review of the legislation in comparison with international best practices showed some inadequacies owing to supposedly undefined scope of application. Consequent upon the foregoing, this paper concludes that while the principal legislation on cybercrime is praiseworthy, there is need to amend the extant law to provide for a more robust legislation that is both reactionary and effectively proactive in promoting other spheres of cybersecurity.

Keywords: Cybercrime, Cybersecurity, Cyber law, Law enforcement, Crime, Forensics

1. INTRODUCTION

Cyberspace as it is today may be simply regarded as a conglomerate of human users of Internet resources, Internet-enabled and connected devices, and the services run by such devices. Though the above description has become a global perspective, history has it that the term has its origin in the Sci-fi writings and movies of the 1980s. The term emanated from William Gibson's Burning chrome [1] a story he published in 1982. However, Cyberspace became much popular following Gibson's novel, Neuromancer [2] published in 1984. According to the New World Encyclopedia [3], Cyberspace is derived from two words: Cybernetics and Space. Whereas Cybernetics as a term is a complex and often confusing term among computer scientist as it has no uniformly agreed definition though many had construed it to mean the "study of control and communication in animals and machine" having regard is to Nobert Werner who is popularly regarded as the first to have defined the term in 1948 in his book[4], "Space" is construed to reflect the conventional unlimited physical space that envelopes all interactions and communications among devices, machines, humans, animals, etc. It is instructive to note that William Gibson the globally acclaimed originator of Cyberspace had in the documentary "No maps for these territories" released in 2000, asserted that he chose the term as a buzzword devoid of no real meaning. According to him, "All I knew about the word 'cyberspace' when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page"[5]. From the above affirmative it may be safe to assert that William Gibson may not have had any contact or regard to Werner's 1948 book hence could not have coined the word from Cybernetics. Be that as it may the context of Cyberspace has grown beyond Gibson's buzzword of the 1980s. This paper is more tilted towards the 'good', the 'bad', and the 'ugly' about the 21st Cyberspace which could be more accurately described as a global technology-driven socially active space comprising billions of information communication technology and service infrastructure such as telecommunication networks, Internet, computer-based systems, processes, and human users. At present, Cyberspace is often used to mean the global Internet and that is the position maintained in this paper.

- *Wilson Nwankwo is an Associate Professor and Director of Centre for Professional Training and Development at Edo University Iyamho, Edo State, Nigeria. Mobile: +2348037636067. E-mail: nwankwo.wilson@edouniversity.edu.*
- *Kingsley Chiwuike Ukaoha is an Associate Professor at the University of Benin, Nigeria. E-mail: kingsley.ukaoha@uniben.edu*

1.2 Effect of the Cyberspace on Social, Economic, Technological, and Cultural Development

We are living in a global village wherein the Internet has continued to contribute to outstanding developments in every facet and sector of human endeavour. Often times some internet applications are so amazing and outside the common boundaries of progressive predictions of science itself. One wonders what the present age could have looked like without the Cyberspace. With ongoing and outstanding daily developments, some school of thought have argued that the man-machine war era as predicted by Science fiction in the early 1980's and scientific writings **[6],** [7] on ICT development [8], [9], **[10]** is before us. Without equivocation the Cyberspace have significantly reformed the following sectors:

i) Education[11], [12],[13],[14]
ii) Trade and Commerce
iii) Manufacturing and Production
iv) Banking and Finance
v) Agriculture
vi) Public service
vii) Law enforcement, Crime Control and Administration of Justice[15], [16],[17], [18],[19]
viii) Politics and Governance[20], [21]
ix) Healthcare delivery
x) Social relations
xi) Media and Communication

Essentially, there is no sphere of human activity that is not practically affected by the Cyberspace. Notwithstanding the tremendous positive impact recorded over the years as to the use of the Internet and allied resources, the world is witnessing a corresponding substantial negative impact owing to the exploitation of the Cyberspace by miscreants and criminals whose activities on the Internet and Computer resources are geared towards causing havoc to legitimate owners or users of such resources. Digital security especially cybersecurity has become a major factor

affecting global economy, governance, peace, and safety. According to EUI (2019) there are four indicators or pillars that could be used to assess the safety of a city (by extension a society) and these include personal, infrastructure, health and digital security [22]. Digital security has become a household issue as more economies, organizational processes, social systems, etc. become dependent on the cyberspace. A digitally unsafe environment is likely to deter the socioeconomic growth of that society. For instance, Tokyo is rated as the safest city in the world having ranked 1st in the 2019 edition of the EIU's safe cities index report whereas Lagos is ranked 58th. The implication is that Tokyo is likely to attract more investment and socioeconomic growth than Lagos. Owing to the complexity and virtual nature of the Cyberspace, such exploitations are without geographical boundaries, often overwhelming, hence demands more effort and resources on the part of resource owners as well as the regulatory agencies and law enforcement. Consequent upon the consistent rise in cyber threats, cyber terrorism, and cyber-attacks across the globe, it behoves on collective effort involving governments, experts, and organizations, to harness resources towards preventing and controlling the menace of cybercrime. This brings to bear the concept of digital security, which encompasses citizen awareness of cyber or digital threats, policies, public-private partnerships, deployment of advanced technology, and dedicated cybersecurity teams.

1.3 Aim and Objectives of the Study

The aim of this discourse is to draw a critical review of the principal cybercrime legislations in Nigeria especially the Cybercrime (Prevention, Prohibition, etc.) Act from the standpoint of Social, Legal, Information and Communications Technology trends and practices with a view to identifying challenges that may hamper the implementation of the law. The objectives of this paper are to:

a. Review the principal Cybercrime legislation in Nigeria vis-à-vis some international cybersecurity legislations and policies, in the face of changing trends in information technology practices and operations
b. Identify some gray areas that may pose challenges in the implementation of the said law
c. Examine the Evidence Act[23] especially as it affects the admissibility and relevancy of electronic evidence in the prosecution of cybercrime cases.
d. Identify steps and programs that may help boost the existing laws and policies on cybersecurity
e. Draw appropriate conclusions that would enhance implementation of the anti-cybercrime policies and frameworks in Nigeria.

1.4 Nature of Cybercrime

With an understanding of the Cyberspace as presented earlier, Cybercrime may be described as any crime or offence against the legitimate use of the Cyberspace. Though Cybercrime may be defined in different perspectives, it is generally agreed by most authors and researchers in the Cybersecurity domain that Cybercrime is a category of offences wherein the computer or computerized system is either the object of the crime or deployed as the means or vehicle to committing the offence. However, some have argued that the term "Cybercrime" is a misnomer[24]. As simple as it may sound, Cybercrime does not have a global flavour in the sense that what is coded as a crime in the cyberspace in one jurisdiction may not be absolute in another Jurisdiction. Consequent upon such circumstances, every sovereign nation may have offences which it recognizes as forbidden acts for which defaulting persons are to be punished or fined subject to the provisions of the nation's extant laws. It is also instructive to note that there are crimes that are often grouped as crimes against humanity and such crimes are recognized and given due force of law regardless of the jurisdiction where such offences are committed in line with Rome Statute of the International Criminal Court[25].

1.5 Cybersecurity and Cyber Law: A Nexus

Cybersecurity is a relatively new term often taken to have same meaning as older terms such as: Information security, Computer security, System security, etc. which have been in use for decades. It may be submitted that Cybersecurity is preferred to the older terms having regard to the activities in the evolving cyberspace, which are neither restricted to computers alone nor restricted to information. Cybersecurity is considered a multidisciplinary domain drawing from Computing and Information Technology, Engineering, Sociology, Philosophy, Psychology, and Law. However, the most prominently harped elements in Cybersecurity are Information Technology, and Legal Regulatory Instruments (LRI) collectively classified under the theme 'Internet Law' or what may be specifically referred to as Cyber Law in recent times. Though Cybersecurity and CyberLaw are clearly distinctive in terms of domain of study, application, and usage, it is evident that Cyber Law has a direct nexus to Cybersecurity as it covers the legal and legitimate regulatory measures that are formally designed and often legislated upon to prevent and control infringement of rights and privileges in the cyberspace. It is however, instructive to note that not all Cyber Laws are designed for Cybersecurity purposes. One must not lose track of the primary context of Cybersecurity may be construed as the totality of mechanisms including technologies, procedures, policies, and regulations employed to protect computer systems and allied resources from theft, damage, disruption of utilization, and misdirection[26] of services provided by such systems. The following sections are brief discussions on the vital elements of Cybersecurity.

1.5.1 Components of Cybersecurity

Cybersecurity may be described in terms of legal and socio-technical [27] system with many components. There is no uniform classification as Cybersecurity is still an evolving field with authors, researchers, and experts discussing the subject from different perspectives, for instance, the three elements: Confidentiality, Integrity, Availability often regarded as the **CIA[28]** triad had for a long time been documented as the components of computer security. Bill Rosenthal [29] had identified three elements of Cybersecurity as comprising Technology, Policy, and People. However, in this paper, the basic components are shown in the diagram in Figure 1. In the diagram, we have

recognized seven key components with humans or people at the heart of the system:

i. Human/People/Organizational element
ii. Software/Application security
iii. Network security
iv. Disaster Recovery and Business Continuity Planning
v. Information security
vi. User Education
vii. Legislation and Policy

The human or people component of cybersecurity is a very important element due to the fact that all other elements revolve around it and no matter how sophisticated the technological elements are, a weakness in the human element will render the entire pursuit a nullity. The Human element is connected to user education and legislation components. The human element can make or mar cybersecurity policies, legislation, procedures, and protocols. Without a consistent and well-structured end user education and reviews, organizational weaknesses, vulnerabilities and loopholes in a system will remain serious bottlenecks to securing any critical information infrastructure.

1.5.2 Legislation and Policy aspects of Cybersecurity

The legislation and policy element of cybersecurity is of key interest in this paper. The spate of breaches on the use of Internet resources has been on the rise in the last two decades across the globe. It is in this regard that the United Nations has been consistent on deliberations on the subject matter since 1998 when the Russian Federation introduced a draft resolution [30] on “Developments in the field of information and telecommunications in the context of security" to the United Nations General Assembly’s First Committee. There has been series on resolutions shaping security in the digital world. Many scholars and writers in different fora with various perspectives to curtailing the challenges that affect not only Nigeria and the rest of the world have discussed the menace of cybercrimes. The current picture of cybercrime legislation is dynamic, indicating ongoing legal reforms and increasing recognition, that cybercrime requires a legal response across multiple areas whether criminal, civil, or administrative. The technological developments associated with cybercrime imply that while traditional laws can be applied to some extent, legislation must also grapple with new concepts and objects, such as intangible ‘computer data,’ not traditionally addressed by law[31]. Cybercrime is a complex subject owing to its interdisciplinary connections. Considering this fact, various categorization had been made as captured in figure 2. Figure 2 is an illustration of the various perspectives of cybercrime using a triangular pyramid. The three edges of the triangle represents the technological perspective, the sides represent the legal or criminological perspective whereas lying within the pyramid is the socio-political perspective. Having regard to Figure 2, it is instructive that legislations and policies must therefore consider such complexities during the initiation, drafting and passage of bills, and prosecution of cybercrime related offences respectively.

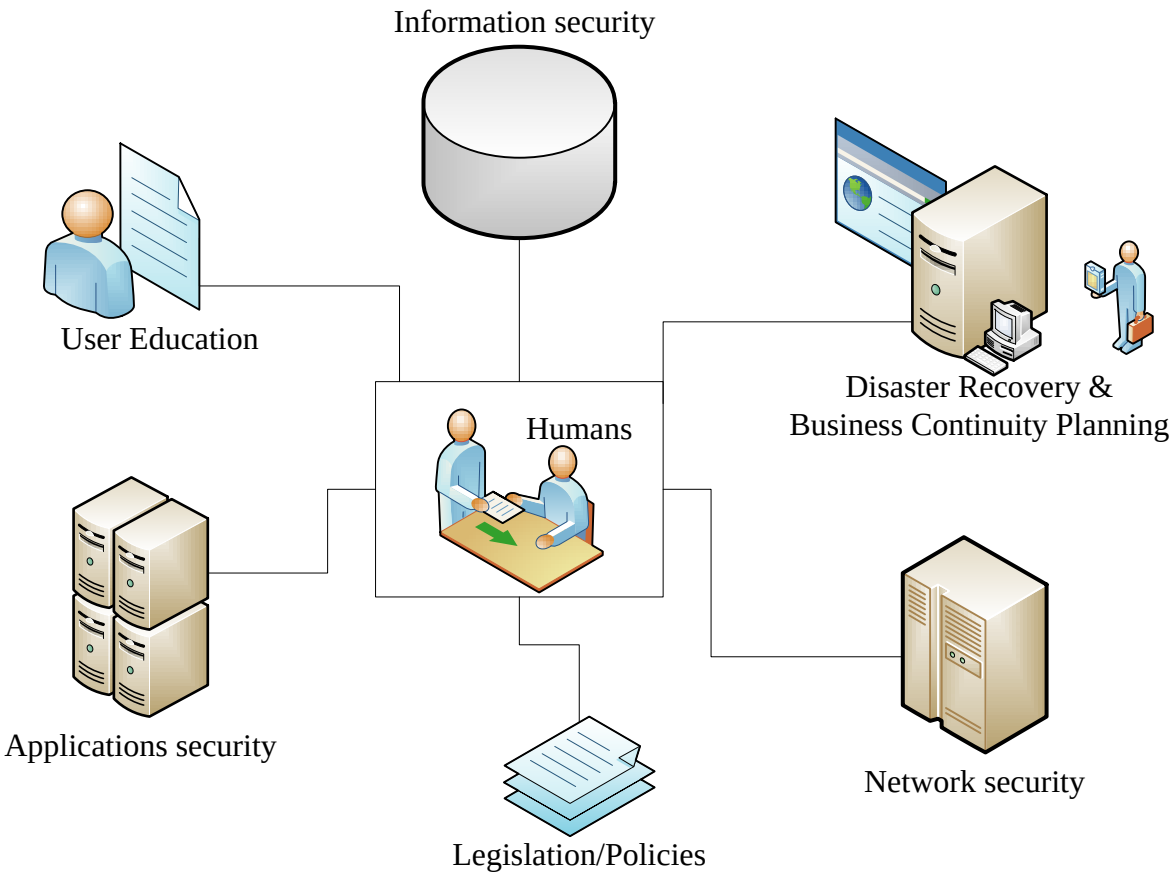

Figure 1: Components of Cybersecurity

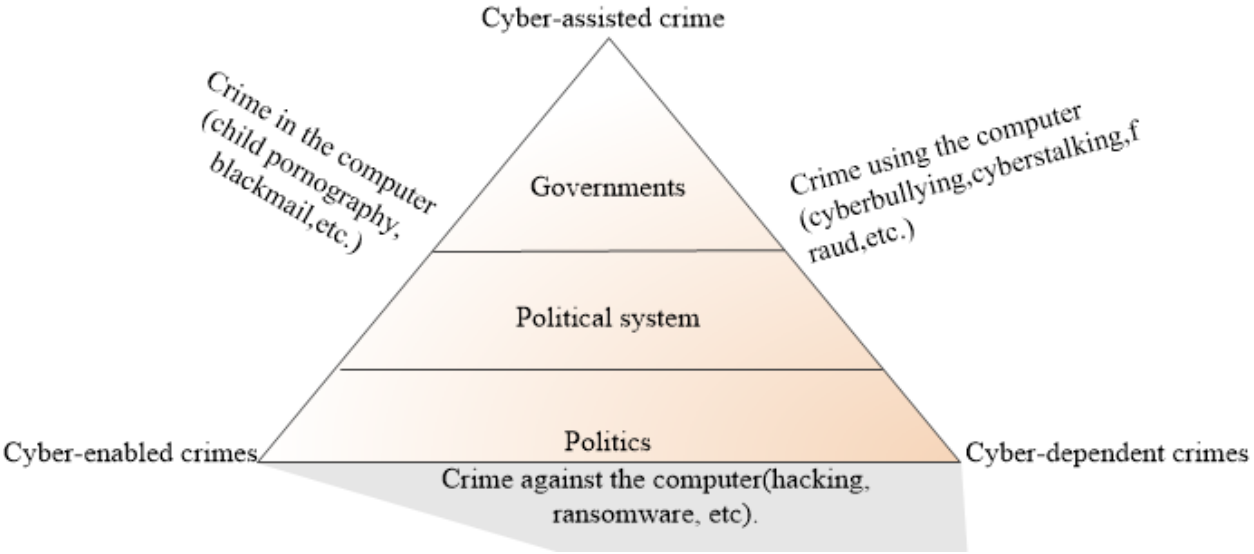

Figure 2: Representing the posture of cybercrime in different perspectives

1.6 Role of Cybercrime Legislation: The Global Perspective

Cybercrime is a global phenomenon and unlike other conventional crimes that are confined within a given geographical location, a criminal activity in the cyberspace may be categorized as transnational in that it may involve two or more countries or even continents. The effects of cybercrime may be devastating not just to a victim but to the integrity of any nation with high spate of such crimes in the comity of nations. The foregoing underlies consistent and ongoing efforts of global [32], [33], [34], [35], [36] and regional agencies [37], [38], [39],[40],[40] alike towards the design and implementation of appropriate cybersecurity policies in addition to individual government policies and laws[41]. The role of cybercrime law [42] is summarized by the provisions of the United Nations Office on Drugs and Crime (UNODC) as follows:

> *Cybercrime law identifies standards of acceptable behaviour for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilitates cooperation between countries on cybercrime matters [43].*

Thus, the role of cybercrime legislations and policies is provide rules, guidelines, practices, and standards of behaviour that regulate all operations and transactions in the cyberspace irrespective of the parties involved. A legislation provides the platform, standards, actions that control the public and private persons; hence legitimate grounds for law enforcement, order, and good governance [44]. A vibrant legislation must as a matter of functionality include very clear rules of conduct of persons, evidence, criminal procedure, punishments, investigative procedures, responsibilities of persons and organizations; and mechanisms that potentially mitigate risk burdens and vulnerabilities of individuals, organizations, and infrastructure. A cybercrime legislation should contemplate trends in technologies hence should cover vital areas of substantive, procedural and preventive law.

2. METHODOLOGY

This paper follows an exploratory narrative-textual case study (ENTCS). We considered this approach appropriate due to the nature of the study as well as the unavailability of substantial quantitative secondary data especially on cybersecurity and cybercrime policies in Nigeria; hence, we focused on published and unpublished materials including policy documents. We placed major emphasis on review of relevant regional and local legislations as well as technological perspectives and regulatory practices especially in the field of Computing and Information Technology. Some of the sources of data are:

a) ITU guide on Cybersecurity[45]
b) Budapest Convention on Cybercrime[46]
c) African Union's Convention on Cyber Security and Data protection
d) Southern African Development Model Law[47]
e) Directive on fighting cybercrime within ECOWAS[48]
f) Constitution of the Federal Republic of Nigeria[49]
g) Cybercrime Act[50]
h) Economic and Financial Crimes Commission Act[51]
i) Advance Fee Fraud and other Fraud Related Offences Act
j) Relevant Laws on Evidence[52]
k) NCC Guidelines for Internet Service Providers[53]
l) Cybersecurity and other Cybercrime policy documents[54]

First, we collected data from online databases, web portals, digital libraries, and texts. Second, we did a review of the legislations and policy documents with emphasis on relevant provisions especially on areas that require modification or enhancement having regard to changing trends in the society. Third, we extracted relevant sections in those documents that we considered needful for issue formulation, analysis and further discussion. In some cases, we drew a comparative analysis in order to buttress arguable points raised. We made submissions on a case-by-case basis.

3. RESULTS AND DISCUSSION

3.1 Results

Applicable laws and policy instruments

Table I shows the applicable legal instruments and policies relating to cybersecurity in Nigeria and their effective dates. In the case of legislations, the date of passage into law by the national assembly or by relevant government agency are taken as the effective dates.

TABLE I: CYBERSECURITY INSTRUMENTS IN NIGERIA

S/N	Short Title	Category	Effective date
1	Cybercrime (Prevention, Prohibition, etc.) Act	Legislation	2015
2.	Advance Fee Fraud and other Fraud Related Offences Act	Legislation	2006
3.	Terrorism Prevention Act	Legislation	2011
4.	Economic and Financial Crimes Commission Act	Legislation	2004
5.	National Communications Commission Guidelines for Internet Service Providers	Policy	2003
6.	National Cybersecurity Strategy	Policy	2014
7.	Risk-based Cybersecurity Framework and Guidelines for Deposit Money banks and Payment service providers	Policy	2018

Law enforcement authorities

The law enforcement authorities in respect of cybersecurity and cybercrime are:

i. Economic and Financial Crimes Commission (EFCC)
ii. The Nigeria Police Force

Supervisory authorities

The supervisory authorities include:

i. The National Security Adviser
ii. The Attorney General of the Federation

3.2 Discussion

Nigeria's Anti-Cybercrime legislation and other related legislation

The principal anti-cybercrime legislation in Nigeria is the Cybercrimes (Prevention, Prohibition, etc.) passed into law in 2015. A comparative study of this cybercrime legislation revealed some marked similarities with international and regional covenants, laws, and related documents on cybercrime. For instance, the legislation is in tandem with some provisions made in the African Union convention on Cybercrime and Personal data protection; ECOWAS Directive on fighting cybercrime, Budapest convention, and Southern African Development Model Law, among other relevant policy documents. Nevertheless, Nigeria has some peculiarities in its socio-political and economic systems that need be taken into consideration while enacting any law to ensure that such law would be yield the anticipated results during implementation. Some criticisms had been raised in different quarters on some areas that require amendment in the principal cybercrime legislation. In this paper, we have presented a different line of argument in our quest to contribute towards ensuring that the cybercrime legislation yields ultimate results for the benefit of all Nigerians in particular and the world at large.

3.2.1 Critical Infrastructure, Critical Information Infrastructure, and Critical National Information Infrastructure

Critical infrastructure in its basic context refers to those infrastructure that are so vital to the socio-economic well-being of any organization or society. To this end, it follows that critical infrastructure may be private or public. As ICT operations are often transnational, for instance, the use of the Internet in making inter-continental banking payments; it follows that there is an interplay between private and public facility. In such cases, a private facility is as important as a public facility since damage to the private facility may give rise to sub-normal, sub-optimal or a total failure of the public facility. According to the International Telecommunications Union, critical infrastructure [55] in the context of cybersecurity is defined as: "…electronic systems, devices, networks, computer programs, electronic data, vital for:

(i) the security, defense or international relations of ; or
(ii) the existence or identity of a confidential source of information relating to the enforcement of criminal law; or
(iii) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation, public key infrastructure, payment systems infrastructure or e-commerce infrastructure; or
(iv) the protection of public safety including systems related to essential emergency services such as police, civil defense and medical services;
(v) the purpose declared as such by the [appropriate ministry or office of enacting country] in accordance with the prescribed procedure; or
(vi) containing any data or database protected as such, by any other law;"

In a similar vein, the African Union Convention on Cybersecurity and Personal Data Protection did not use the term "Critical Infrastructure" but instead adopted the term Critical Cyber/ICT Infrastructure. Accordingly, Critical Cyber/ICT Infrastructure means "Cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability, and for the sustainability and restoration of critical cyberspace". We found a similar provision in Section 3(9) of the Southern African Development Model Law [56] on Computer crime and Cybercrime. In that section, Critical Infrastructure implies "computer systems, devices, networks, computer programs, computer data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters". In what seems like a departure from international global perspective on critical infrastructure in the context of Cybersecurity and Cybercrime, Section 58 of Nigeria's Cybercrime legislation defines critical infrastructure as: "Systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country". The Act also introduced the term "Critical National Information Infrastructure" in its explanatory memorandum wherein it stated thus:

> *"…This act also ensures the protection of critical national information infrastructure, and promotes cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights".*

Suffice it to say that the African Union's perspective is perfectly in agreement with the use of the term 'critical Infrastructure' by the ITU. Their position differs from the broad meaning given to Critical Infrastructure in Section 58 of Nigeria's Cybercrime law wherein no reference was particularly made to ICT. It is instructive to note however, that terms Critical Information Infrastructure and Critical National Information Infrastructure as used in the body of the Act when taken together with the explanatory memorandum presupposes that the Critical infrastructure

defined by the legislation could be at best be construed within the context of ICT. This view may be supported by the fact that both Critical Information Infrastructure and Critical National Infrastructure were not expressly defined in the Act. In respect of Critical National Information Infrastructure, regard may be had to section 3(1) of the Act, which provides as follows:

> *"The President may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or Traffic data vital to this country that the incapacity or Destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure".*

Thus, it may be submitted that the inconsistency in the use of terms introduced some element of ambiguity as what constitutes Critical National Information Infrastructure and Critical Information Infrastructure respectively. The ambiguity is further buttressed by the fact that the legislation does not expressly delineate the components of such infrastructure but delegates such responsibility to the President and the National Security Adviser (who is mandated to chair the Advisory Council).

3.2.2 Registration of Cybercafés under the Cybercrime Act

The Principal legislation vests the power to register cybercafés on the Computer Professionals Registration Council of Nigeria (CPN). Other than registration with CPN, no further reference was made to the role CPN is to play in the regulation of Cybercafés nor was there any further responsibilities vested on the CPN to enable it drive the prevention of cybercrimes in Nigeria. We submit that the responsibility vested on the CPN therein is an aberration or simply a misplacement of responsibility. Mere registration of Cybercafés with CPN as provided by the principal legislation does not vest any crucial responsibility on the CPN having regard to its existing regulatory and supervisory powers. It may be recalled that CPN is a body duly created by an Act [57] of parliament and vested with the power to regulate Computing and Information and Communications Technology practice (including cybersecurity) in Nigeria. The powers of CPN include control, supervision [58] and regulation [59] of ICT profession and practice in Nigeria. In other words, the powers of CPN does not only include registration of practitioners but also the accreditation [60] of Institutions (be it academic, professional, specialist ICT services) as well as the determination of what constitutes standard in the training and practice of computing and computing machinery. Section 42 of the Cybercrime Act created the Cybercrime Advisory Council and vested on it the responsibility to:

> *"formulate policies and guideline for the implementation of the Act; advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues; establish a program to award grants to institutions of higher education to establish Cyber security Research Centers to support the development of new Cyber security defences, techniques and processes in the real–-world environment; contributing to towards the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria".*

As important as the said Advisory Council is to the implementation of the Cybercrime Act, an average person could have considered the inclusion of the CPN (as the sole Computing and ICT regulatory agency of the government) as just a norm. However, it is instructive to note that the CPN is not included in the membership of the Advisory Council. Express exclusion of the CPN in the Act is considered a serious error of omission or commission as CPN is a key player in the promotion and control of ICT and Computing practices as well as the computing machinery around which cybersecurity revolves.

3.2.3 Registration of Cybercafés under the Advance Fee Fraud and other related Offences Act

Section 13 of this law provides as follows:

> *"(1) Notwithstanding the provisions of the Nigerian Communications Commission Act 2003 or the provisions of any other law or enactment, any person or entity who in the normal course of business provides telecommunications or internet services or is the owner or person in the management of any premises being used as a telephone or internet cafe or by whatever name called shall-*
>
> (a) Be registered with the Economic and Financial Crimes Commission;
>
> (b) Maintain a register of all fixed line customers which shall be liable to inspection by any authorized officer of the Commission; and submit returns to the Commission on demand on the use of its facilities…"

Though this Law was in force before the Cybercrime Act, no reference was made to it in the Cybercrime Act. Having regard to the subsisting provision in the old law it is reasonable to submit that a duplicity of this role in the cybercrime Act. The responsibility of the Economic and Financial Crimes Commission (EFCC) as a law enforcement agency is understood as applied to cybercafés however, the role of CPN was not defined.

3.2.4 Reactive versus Proactive Provisions towards Cybercrime

The principal legislation is praiseworthy in that it has made vital and succinct provisions as to measures that are to be employed in detecting and prosecuting cybercrime including the provisions for punishments and fines. Notwithstanding the advisory council the law empowers with the responsibility of formulating anti-cybercrime policies, majority of the provisions are best regarded reactionary as against proactive measures some of which could have been articulated in the main body of the legislation. Cybercrime is a global phenomenon and research has shown that persons within the age group of 15-24 are most vulnerable[61] to it. It therefore follows that if this age group is captured in the scheme of things especially as it affects cybersecurity and cybercrime education and training programmes, it would go a long way in reducing cybercrime among the youths. The Federal Ministry of Youth and Sports has the mandate to that promote and enhance the development of the Nigerian youth and the protection of their interests. The Ministry has the National Youth Service Corps (NYSC) as one of its parastatal. We submit that the legislation would have had an extensive impact of it had contemplated the socio-economic role of this ministry and mandated it to ensure that cybercrime and cybersecurity training are made compulsory in the NYSC service programmes. NYSC receives and conducts orientation programmes for tens of thousands of graduates from tertiary institutions in Nigeria every year. The inclusion of cybercrime awareness and cybersecurity training could go a long way to acquainting the youths with cybersecurity consciousness thus helping check the menace of cybercrime.

3.2.5 Education and allied programs on Cybercrime and Cybersecurity

Legislation on cybercrime is at best an aspect of a cybersecurity programme, other aspects including training, education, technical, technological, and political. The training, education, technical, and technological elements are all interwoven. This is because human capacity development is fostered by training and education, and directed to the production and advancement of technical manpower. Advances in technological products are the result of research, and development in technical education, and affect trends in technology. Consequent upon the foregoing, we submit that education is a key player and moderator in the domain of cybersecurity. According to ITU [62], "…it is important to develop a general cybersecurity culture in order to raise the level of understanding of each member of the cybersecurity chain. A cybersecurity culture deals with key economic, legal, and social issues related to information security in order to contribute to helping countries get prepared to face issues and challenges linked to information and communication technologies (ICT) deployment, uses and misuses". ITU further states that citizens need be provided with the appropriate information related to cybersecurity issues. Appropriate information in the context of ITU is hinged on sufficient awareness and education as this will contribute towards preventing deviant behavioural tendencies in the society especially in respect of cybercrime. The principal legislation appears to recognize the need for research and development on cybersecurity under section 43, which provides for the functions of the Advisory council. According to the section 43(d) & (e), the Advisory Council, which is responsible to the National Security Adviser, shall: "Establish a program to award grants to institutions of higher education to establish Cyber security Research Centers to support the development of new Cyber security defences, techniques and processes in the real–-world environment; and promote Graduate Traineeships in Cyber security and Computer and Network Security Research and Development". Nevertheless, it could be deduced that said provision reckoned neither with the Federal Ministry of Education (FME) nor with its parastatals such as the National Universities Commission, National Board for Technical Education, etc. This position is conclusive on examination of the membership of the Advisory Council on Cybersecurity. Neither the FME nor any of its agencies is included as a member of the Advisory Council. We submit that Cybersecurity like any other Computing field is at best understood through the creation and implementation of appropriate curricula to drive the various educational programmes offered in the secondary and tertiary institutions, which are under the purview of the Ministry of Education, the custodian of the National Policy on Education. It is a wonder how education and research on cybersecurity would advance without the major drivers of the education and research sector. Therefore, we submit that a harmonious relationship between the National Cybersecurity Policy and the National Policy on Education could have had more impact on the preventive and corrective measures towards checking cybercrime and boosting cybersecurity in the country.

3.2.6 Diversification of responsibilities on cybersecurity programmes

The principal cybercrime legislation vested the implementation of the national cybersecurity strategy on the office of the National Security Adviser who is also chairs the Advisory Council. Considering the above provision vis-à-vis the organizations and population of Internet users in Nigeria, we submit that there is a need for a more collective approach to achieving the national cybersecurity goals. All agencies that contribute to the economic development of this country should be integrated into the programme. The cases of the Central Bank of Nigeria (CBN) and National Communications Commission (NCC) are worthy of note. In June 2018, the CBN produced its cybersecurity framework[63] directed to all Deposit Money Banks (DMDs) and Payment Service Providers (PSPs) in the country. By the said document all operators in the banking subsector are required to implement the articulated cybersecurity programmes. Similarly, Section 5 of the NCC guidelines for all Internet Service Providers (ISPs) provides as follows:

> *"ISPs must ensure that users are informed of any statements of cybercrime prevention or acceptable Internet use published by the Commission or any other authority, and that failure to comply with these acceptable use requirements may lead to criminal prosecution, including with respect to:*

(a) unlawful access or fraudulent use of a computer;
(b) identity theft, impersonation or unauthorized disclosure of access codes;
(c) unlawful interception, or any form of system interference;
(d) violation of intellectual property rights;
(e) any other use for unlawful purposes, including terrorism, promoting racial,
religious or other hatred or any unlawful sexual purposes"

The above provisions would substantial guide to service providers and their clients. These measures are subtle preventive measures that are apparently effective. It is interesting to note that the above agencies belong to different sectors in the economy with their guidelines defined to meet the needs of their respective sectors. Consequently, it is important to carefully identify the needs of each sector or subsector of the economy and mandate the regulator of such subsector or sector to provide cybersecurity framework or guidelines instead of concentrating all powers on the office of the National Security Adviser. Devolving the powers to the regulators of the various subsectors would be more efficient and effective in the pursuit of the national cybersecurity goals.

3.2.7 Electronic evidence in the prosecution of cybercrimes: An examination of Nigeria's Evidence Act

The Evidence Act (also known as the Evidence Law) is the primary legislation guiding the way evidence in respect of civil and criminal wrongs during legal proceedings are presented in the law courts in Nigeria. Nigeria's substantive Evidence Law came into force on 3 June 2011. This procedural law is has been hailed as remarkable following its attempt to tackled the inadequacies of the repealed law (Evidence Act 2004). There are two salient provisions that are vital to this discussion:

i. Section 84
ii. Section 255

Section 84 dwells on admissibility of statement in document produced by computers. Section 84 (1) provides that in any proceedings, a document produced by a computer shall be admissible if direct oral evidence of the facts stated in the document would be admissible if the conditions specified in Section 84 (2) are satisfied. Section 84(2) is to the effect that there shall be a proof that the computer in question is used to store or process information in the ordinary course of the activities of the type from which the information is derived, and that the computer must have been operating properly, or if not operating properly, the period for which it was not operating properly was not such that could have affected the production of or accuracy of the contents of the documents. Section 84(4) is to the effect that where an electronic is desired to be given during a proceeding, a certificate identifying the document including any device involved in its production, and signed by a person occupying a responsible position in relation to the operation of the device or management of activities from which the document emanated, shall be required. Though the Evidence law does not preclude any other laws in force from specifying the format, nature, rules of electronic or digital evidence especially in respect of relevance and admissibility during prosecution of cybercrimes, it should be recalled that emphasis is often made to it during most civil and criminal proceedings in Nigeria's law courts. To this end, its provisions should be clear and elaborate to drive future trends. The clause contained in Section 84(2) of the said law poses some technical challenges in the face of the escalating cyber threats, vulnerabilities, and attacks in the cyberspace. A given instance is distributed attack, which may be ongoing on a computer without the knowledge of the user or manager of the department, or domain in which the computer is located. Section 255 empowers the Minister of Justice who doubles as the Attorney General of the Federation to make regulations prescribing further conditions in respect of the admissibility of any class of evidence relevant under the Act. Notice a similar provision in Section 57 of the Cybercrime law, which empowers the Attorney General of the Federation to make orders, rules, guidelines or regulations that may provide procedure for the prosecution of all cybercrime cases in line with national and international human rights standards, among other provisions. It therefore follows that the Attorney General can extend the provisions on Section 84 of the Evidence Act in respect of the admissibility and relevance of electronic evidence. According to Ajayi (2011), the Evidence Act is praised in many quarters for its flexibility. Notwithstanding the popular position that the provisions in the Evidence Act and Cybercrime Act in respect of the mandate of the Attorney General of the Federation, are purportedly drawn to afford flexibility[64] in the face of changing trends in both cybercrime, and prosecution in the law courts, we submit that powers vested on the Attorney General of the Federation are somewhat excessive and could be easily exploited to incriminate and victimize some individuals who are perceived as enemies of the Government.

4 CONCLUSION

In this paper, we have made an attempt to critically review the principal cybercrime legislation from a sociotechnical and professional dimension. We have drawn the following conclusions:

i. Whereas the principal cybercrime legislation is a plausible instrument for fighting cybercrimes in Nigeria, it is instructive to eliminate any clog in the wheel of the legislation which may hamper the smooth implementation of the law. Duplicities in the apportionment of responsibilities should be removed. This does not only apply to the Cybercrime Act but other related legislations wherein different agencies are given responsibilities on often very related matters.
ii. More resource should be channeled to proactive measures other than reactive measures. This is because, as population grows, there is likely a corresponding growth in the crime rate where proactive measures are not entrenched. Reactive measures such as those spelt out in the cybercrime Act can easily wear out state resources especially with the exponential increase in cybercrimes.
iii. Since the cybersecurity need of each subsector in the economy may differ, the cybercrime or related

legislations should be amended to grant powers to the regulators of the said subsectors to develop and implement cybersecurity polices and frameworks that meets the need of their subsectors.

iv. Scope of application should be clearly defined to avoid any misinterpretation during prosecution of offences related to cybercrime.

REFERENCES

[1] W. Gibson, Burning Chrome, Reprint edition, New York: Harper Voyager,2003.

[2] W. Gibson, Neuromancer, 1st edition, New York: Ace books, 1984

[3] New World Encyclopedia [online] http://www.newworldencyclopedia.org/entry/Cyberspace (Accessed 4 June 2019)

[4] W. Norbert, Cybernetics: Control and Communication in the Animal and the Machine, Cambridge, Massachusetts: MIT Press,1948

[5] N. Mark, C. Paine, P. Mark, M. Buffet, T. Gorai, No maps for these Territories, Docurama films , United States of America, 2000

[6] R. Kurzwei, The Age of Intelligent Machines, Cambridge, Massachusetts: MIT press, 1990

[7] R. Kurzweil, The Age of Spiritual Machines: When Computers Exceed Human Intelligence, New York: Penguin, 1999

[8] B. James, "Rise of the machines: has technology evolved beyond our control?", The Guardian, 2018 https://www.theguardian.com/books/2018/jun/15/rise-of-the-machines-has-technology-evolved-beyond-our-control- (Accessed 3 July 2019)

[9] E. Musk, Artificial intelligence is our biggest existential threat, The Guardian, 2014 https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat (Accessed 9 July 2019)

[10] V. Mnih et al., "Human-level control through deep reinforcement learning", Nature, Vol.518, pp 529–533, 2015

[11] W. Nwankwo "Promoting Equitable Access to University Education through Online Learning Systems", World Journal of Engineering Research and Technology, Vol.4, Issue 2, pp. 517-543, 2018

[12] D. Mahalakshmi et al., "A Study on Cyberspace and its Impact in Society", International Journal of Research in Management & Technology (IJRMT), Vol.6, No.1, 2016

[13] R.H. Puspita, and D. Rohedi, "The Impact of Internet Use for Students", IOP Conference Series: Material science and Engineering, Vol. 306 Issue 012106, 2018.

[14] M. Neil, "The Impact of the Internet on the Educational Systems in the New Millennium", Education., Vol. 122, No. 1, 2001

[15] J. Byrne, & G. Marx, "Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact", Maklu-Uitgervers, Voor Belgie, 2011.

[16] W. Nwankwo et al(2018). "The Role of Social Information Technology in curbing Corruption", American Journal of Embedded Systems and Applications. Vol. 6, No. 1, pp. 56-68,2018. doi:10.11648/j.ajesa.20180601.18

[17] J.S. Hollywood, et al., "Emerging Technology Trends and Their Impact on Criminal Justice" [online]. Rand Corporation, 2018. www.rand.org/t/RR1987 (Accessed 2 August 2019)

[18] F. Ibikunle, & B. Adefihan, 'Effectiveness of Information and Communication Technology (ICT) in Policing in Nigeria', Scottish Journal of Arts, Social Sciences and Scientific Studies,Vol.11, No. 2. pp.90-103, 2013.

[19] O.C. Eneh, 'Technoscience in Crime Detection and Control: A Review', Journal of Applied Sciences, Vol.10, No. 17, 2010

[20] W. Roger, 'Citizen Electronic: Marx and Gilder on Information Technology and Democracy', Journal of Information Technology Impact, Vol. 1, No. 1, pp. 20-22, 1999.

[21] Essays, UK., "Impact of Communication Technology on Politics and Economics", 2018. [Online] https://www.ukessays.com/essays/politics/impact-communication-technology-politics-6000.php?vref=1 (Accessed 20 August 2019)

[22] Economist Intelligence Unit," Safe Cities Index 2019: Urban security and resilience in an interconnected world", London: The Economist Intelligence Unit Limited,2019

[23] Evidence Act 2011, Laws of the Federation of Nigeria 2011

[24] K. Dashora, 'Cyber Crime in the Society: Problems and Preventions', Journal of Alternative Perspectives in the Social Sciences, Vol 3, No 1, pp.240-259, 2011

[25] Rome Statute of the International Criminal Court 1998

[26] D. Schatz, R. Bashroush, J. Wall, "Towards a More Representative Definition of Cyber Security",

Journal of Digital Forensics, Security and Law, Vol. 12, No.2.,2017

[27] G. Baxter, & I. Sommerville, 'Socio-technical systems: From design methods to systems engineering ', Interacting with Computers, Vol. 23, Issue 1.pp 4–17, 2011

[28] M. Bishop, Introduction to Computer Security, 1st Edition, Boston: Addison-Wesley Professional, 2004

[29] B.Rosenthal, "The Three Elements of Cyber Security"[online], 2016. https://logicaloperations.com/insights/blog/2016/10/25/446/the-three-elements-of-cyber-security/ (Accessed 20 August 2019)

[30] A.S. Anatolij, International information security: description and legal aspects, Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2007

[31] K.H. Mohammed, Y.D. Mohammed, A.A. Solanke, "Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria," International Journal of Cybersecurity Intelligence & Cybercrime, Vol.2, No.1, pp. 56-63, 2019

[32] United Nations, "Resolution 65/230 adopted by the General Assembly during Twelfth United Nations Congress on Crime Prevention and Criminal Justice", 2010

[33] UNODC, "Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 25 to 28 February 2013. https://undocs.org/UNODC/CCPCJ/EG.4/2013/3

[34] United Nations, "Resolution 28/1: Strengthening the engagement of all members of society in crime prevention", 2019

[35] United Nations, "Resolution 26/4: Strengthening I nternational cooperation to combat Cybercrime", 2017

[36] United Nations, " DOHA Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation", New York: United Nations, 2015

[37] UNODC, "Capacity-building on cybercrime and e-evidence: The experience of EU/Council of Europe joint projects 2013-2017", Geneva: United Nations, 2017

[38] African Union, "Convention on Cyber Security and Personal Data Protection. 23rd Ordinary Session of the Assembly, Malabo", Equatorial Guinea, 2014

[39] ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response, 2014

[40] J. Hakmeh, 'Cybercrime Legislation in the GCC Countries Fit for Purpose?', International Security Department. Royal Institute of International Affairs, 2018

[41] Council of Europe, Budapest Convention on Cybercrime, 2001

[42] Cybercrime (Prohibition, Prevention, etc.) Act 2015

[43] UNODC, Draft Comprehensive Study on Cybercrime. pp 51-116, 2013.

[44] M. Andrea, "The Importance of Effective Cyber Crime Legislation. Presentation at the Organization of American States (OAS) REMJA Meeting, WASHINGTON DC, 2016.

[45] ITU, Cybersecurity Guide for Developing Countries, Geneva, Switzerland, 2009

[46] Budapest Convention on Cybercrime 2001

[47] Southern African Development Community (SADC) Model Law 2012

[48] ECOWAS, Directive C/dir. 1/08/11 on fighting cybercrime within ECOWAS. 66TH Ordinary session of the Council of Ministers, Abuja Nigeria, 2011

[49] Constitution of the Federal Republic of Nigeria 1999[as amended]

[50] Economic and Financial Crimes Commission (Establishment) Act, Laws of the Federation of Nigeria 2004

[51] Advance Fee Fraud and other Fraud Related Offences Act 2006

[52] National Communications Commission Guidelines for Internet Service Providers, 2003

[53] National Cybersecurity Strategy 2014

[54] Commonwealth, Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences relating to computer information, Ukraine,2001

[55] ITU, Electronic Crimes: Knowledge-based Report. Establishment of Harmonized Policies for the ICT Market in the ACP Countries., pp1. Geneva, 2013

[56] Southern African Development Community (SADC) Model Law,2012

[57] Computer Professional Registration Council of Nigeria (CPN) Act Cap C22 Laws of the Federation of Nigeria 2004

[58] Section(13) of Control and Supervisory Regulations of the Computer Professionals Registration Council of Nigeria, 2004

[59] Section 1(2) of the CPN Act 2004

[60] Section 19(a) Control and Supervisory Regulations of the Computer Professionals Registration Council of Nigeria

[61] O. Atte & K. Teo, 'Young people as victims of crime on the internet: A population-based study in Finland', Vulnerable Children and Youth Studies, Vol. 8, No.4, pp 298-309, 2013. DOI:10.1080/17450128.2012.752119

[62] Cybersecurity guide for developing countries, Geneva, 2001

[63] Central Bank of Nigeria, Risk-based Cybersecurity Framework and Guidelines for Deposit Money banks and Payment service Providers, 2018

[64] O. Ajayi, 'Knowledge exchange: An overview of Salient provisions in the Evidence Act 2011', 2011. https://www.olaniwunajayi.net/wp-content/uploads/2016/03/Overview-of-the-Evidence-Act-2011.pdf [Accessed 3 August 2019)