Carnelian Journal of LAW& POLITICS
Vol. 4 No. 1, 2022
https://carnelianjournal.com

Cyber-Terrorism and Its Implication for Telehealth in Nigeria: Imperatives for a Legal Framework

Titilola Adegbile, LL. B, B.L (Ife), LL.M
Doctoral Candidate,
Babcock University,
School of Law & Security Studies,
Iperu, Ogun State, Nigeria.
adegbile0489@pg.babcock.edu.ng

Titilayo Aderigbigbe, BA, LLB, LLM (Ife), BL, Ph. D (Medical Law) Kent
Professor of Law,
School of Law & Security Studies,
Babcock University, Ilisan-Remo, Ogun State.
aderibigbet@babcock.edu.ng,

Abstract

There are about 8 billion people in the world; about 62.5% of them are internet users. Therefore, the world has moved from being a "global village" to a "global cyber village". Technological and innovative disruptions are being experienced across all human endeavour including healthcare, the latest being ChatGPT. Advancement in technological innovations has become part of human existence even in the area of healthcare. Security is therefore a core concern and is fast taking up cyber and technology dimensions, giving rise to phenomenon like cyber-terrorism. Using a desk-based doctrinal research methodology, this study investigates cyber-related statutes for adequacy of a legal framework for cyber-terrorism in the light of healthcare and telehealth in Nigeria. Findings from this research show that there is no singular legislation that adequately addresses cyber-terrorism in Nigeria's healthcare system. This is an imperative for a dynamic and young population like Nigeria. Furthermore, the supremacy clause of the constitution makes it difficult to make policies on healthcare and cyber terrorism without a a specific legislative intervention. The available statutes on healthcare are insufficient to address both telehealth and its cyber-security challenges like cyber-terrorism. The extant cyber-related legislations envisage and provide a basis for addressing cyber-challenges to healthcare in this study. The study concludes that there are inadequate legislative modalities to guide the application of these

cyber-related legislations to protect the health sector and its users. The study recommends that Nigerian legislature formulate telehealth policies that addresses the urgent abysmal telehealth infrastructure and cyberterrorism in her healthcare system.

Keywords: Healthcare, Tele-health, Legislature, Cyberterrorism,

1.0 Introduction

The entire Nigerian Legal framework is based on the 1999 Constitution of the Federal Republic of Nigeria (as amended)[1] with provisions that make its supremacy expressly, clear and non- negotiable. Section 1 (1) of the 1999 Constitution provides that —(1) 'This Constitution is Supreme, and its provisions shall have binding force on all authorities and persons throughout the Federal Republic of Nigeria'.[2] This supremacy of the constitution is backed by the inherent 'inconsistency principle' in Section 1(3) through which it extends its supremacy beyond persons and authorities. Section 1(3) provides that "If any other Law is inconsistent with the provisions of this Constitution, this Constitution shall prevail, and that other Law shall to the extent of the inconsistency be void.".[3] In another light, while Section 1 (1) of the 1999 Constitution applies the supremacy of the constitution over authorities and persons, Section 1(3) applies the constitutional supremacy over laws, policies, and regulations.

The constitutional supremacy enshrined in section 1 (1) has however been given a borderless jurisdiction by virtue of section 1 (2). This borderless jurisdiction extends the application of constitutional powers to authorities, persons, laws, policies, and regulations equally operating outside the physical and legal Nigerian jurisdiction, subject to the precedent of acts or attempt to control the Government. Hence, section 1(2) provides that "The Federal Republic of Nigeria shall not be governed, nor shall any person or group of persons take control of the Government of Nigeria or any part thereof, except in accordance with the provisions of this Constitution".[4]

This borderless supremacy nature of the Constitution is instanced in its section 12 (1) that provides that "12.—(1) No treaty between the Federation and any other country shall have the force of law except to the extent to which any such treaty has been enacted into law by the National Assembly." This is clear that even where the Government of the Federation has acceded to treaties of any international body, (either by virtue of its being a member of an international body, or cooperating on an international project), the treaty, agreement or instrument acceded to, does not influence the operations or form part of the Governing authority of any person or groups in Nigeria if it has not been enacted as a law of the Federation by the Nigerian National Assembly. Hence, no person or group of persons outside Nigeria

[1]Constitution of the Federal Republic of Nigeria (CFRN) 1999 (with 1st, 2nd, 3rd & 4th Amendments) <https://www.comstituteproject.org/constitution/Nigeria_2011.pdf?lang=en> accessed 10 March 2022

[2] CFRN 1999, s 1 (1)

[3] CFRN 1999, s 1 (3)

[4] (CFRN) 1999, s 1(2)

can take control of the Government even through legal instruments except in accordance with the provisions of the constitution.

Control as defined by the Black's Law Dictionary means "To exercise power or influence over; To regulate or govern; To have a controlling interest,"[5] this makes the nature of control of a government within this context to be open ended and not limited to treaties or agreements between the Federation and any other country. International treaties or agreements are efforts for united global actions on a cause or a goal. They further aim to have a global uniform influence over Governments of nations across continents, for global positive impact. Treaties however, do not foreclose the possibility of illegal and unauthorized attempts by any person or a group of persons to attempt to exercise undue and unconstitutional control over the Government of the Federal Republic of Nigeria. In fact, the accession of a treaty or its ratification can make a nation be a target of unconstitutional control or influence of its government. This is s terrorism.

2.1 Terrorism

Terrorism as a concept has evaded definition in Nigerian legislation but not in legislations of other jurisdictions like the United States of America and the United Kingdom.

Terrorism according to the United States of America (US) Department of Defence is "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."[6] A more extensive definition of Terrorism was given in the United Kingdom Terrorism Act 2000, which stated that:

> (1) In this Act "terrorism" means the use or threat of action where-
> (a) The action falls within subsection (2).
> (b) The use or threat is designed to influence the government or to intimidate the public or a section of the public , and
> (c) The use or threat is made for the purpose of advancing political, religious, or ideological cause.
> (2) Action falls within subsection (1) if it-
> (a) involves serious violence against person.
> (b) involves serious damage against property,
> (c) endangers a person's life other than that of the person committing the action.

---

[5] Bryan A. Garner (Ed), *Black's Law Dictionary* (West Group: St. Paul, Minn, 1999)

[6] Don John Omale, "Terrorism and Counter Terrorism in Nigeria: Theoretical Paradigms and Lessons for Public Policy,' (2013) 9 (3) *Canadian Social Science,* 96-97 <https://www.google.com/url?sa=t&source=web&rct=j&url=http://www.flr-journal.org/index.php/css/article/viewFile/j.css.1923669720130903.2916/4264&ved=2ahUKEwiJw_Pa7Lf-AhUkgv0HHeHRArcQFnoECAcQAQ&usg=AOvVaw2-Y2N4a9lMjkJWv0tV4h4O> accessed 10 April 2023

(d) creates a serious risk to the health or safety of the public or a section of the public, or
(e) is designed seriously to interfere with or seriously to disrupt an electronic system.

In November 2004, the Secretary-General of the United Nations Report described terrorism as any act "intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act".

The principal legislation on Terrorism is the Terrorism (Prevention and Prohibition) Act, 2022 that commenced on I2lh Day of May 2022. It is a 16-part legislation with 100 chapters, whose aim is to provide "for effective, unified and comprehensive legal, regulatory and institutional framework for the detection, prevention, prohibition, prosecution and punishment of acts of terrorism, terrorism financing, proliferation and financing of the proliferation of weapons of mass destruction in nigeria ; and for related matters"[7]

This Terrorism legislation itself does not contain any definition of terrorism. Rather, it provides extensive description of "acts of terrorism" in Section 2. It is important to note that the section 2 of the Terrorism Act can be regarded as the "relevancy sustainability provision". This is because of the depth of foresight employed in drafting this section, as most of the acts of terrorism described here have not been witnessed in Nigeria as of date, but they have been experienced in some parts of the world. BCRN weapons for instance are unknown to the generality of Nigerians. Hence, in the event that these acts of terrorism begin to come into play, this Terrorism Act will be relevant in providing an initial legal and statutory framework in dealing with such acts of terrorism.

The Terrorism (Prevention and Prohibition) Act 2022 is today Nigeria's principal legislation on Terrorism in Nigeria, but not the lone legislation intended to address terrorism in Nigeria. However, in the light of this present discussion, the Cybercrime Act, which is rarely mentioned on issues of terrorism becomes important due to the prevailing physical conventional form of terrorist activities being experienced in Nigeria. The Cybercrime Act provides for a kind of terrorism which has been forecasted to be the next form of terrorism likely to be experienced in Nigeria, following its surge all over the world; that is, Cyber-Terrorism.

2.2 Cyber-Terrorism: Definitions

[7] Terrorism (Prevention and Prohibition) Act 2022, Title <https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.nfiu.gov.ng/Home/DownloadFile%3FfilePath%3DC%253A%255CNFIU%255Cwwwroot%255Cdocuments%255CTPp_DFV8G6&ved=2ahUKEwifqqeo7bf-AhW3VaQEHQpdCKwQFnoECAcQAQ&usg=AOvVaw0KIeZCRWPpd8Rt2W0djKu8> accessed 10 April 2023

Cyber-Terrorism according to Denning 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".[8]

In this definition is evident the concept of "unlawful attacks and threats against computer, networks and information stored therein" which is similar to the perspective of the Terrorism Act. The Act sees a computer, network and information stored therein as likely objects of a terrorist attack and even defines 'acts of terrorism to include attacks against computer and or systems and/or networks, designated as critical national information infrastructure or not, but of which an attack against to further intimidate or coerce a government or with any intention to do any acts as stipulated in Section 2 (3) of the Terrorism Act 2022'.

This definition of terrorism in the Terrorism Act as encompassing elements of cyber-terrorism is equally found in the definition of terrorism in other jurisdictions. For instance, the Security Legislation Amendment (Terrorism) Act 2002 of Australia defines "terrorism" as actions that "seriously interfere with, seriously disrupt, or destroy, an electronic system including, but not limited to, an information system; a telecommunications system; a financial system; a system used for the delivery of essential government services; a system used for, or by, an essential public utility; or a system used for, or by, a transport system."[9] Equally in Malaysia, under its Penal code, terrorism is defined to include an act or threat of action "designed or intended to disrupt or seriously interfere with any computer systems or the provision of any services directly related to communications infrastructure, banking or financial services, utilities, transportation or other essential infrastructure."[10] Same definition of terrorism as including cyber-terrorism is equally reflected in the definition of Terrorism in the UK Terrorism Act, as early reproduced.

---

[8] US House of Representatives Special Oversight Panel of Terrorism Committee on Armed Services (2020) '*Cyberterrorism: Testimony of Denning'*
<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> accessed 10 April 2023

[9] Marcus Araromi, "Cyber-terrorism Under the Nigerian Law: A New Form of Threat or an Old Threat in A New Skin? Cyberterrorism Under the Nigerian Law, available at
<https://ssrn.com/abstract=3286617> accessed 10 April 2023

[10] Malaysian Penal Code Chapter VIA, section 130B; M.A Araromi, *ibid*

These definitions appear however as a square peg in the round hole of cyber-terrorism as provided in Section 18 of the Cybercrimes Act, which itself does contain provisions safeguarding the computer or computer systems or networks from unlawful attacks. However, it also emphasises that a computer network or system can itself be a means or source of such unlawful attacks. This may definitely enlarge the definition of persons within the Cyberterrorism context of terrorist attack, as to include that a computer system or network can be *a* "person" perpetuating terrorist attacks on its own, having been set in motion by a human person.

The acceptance of the convergence of terrorism with computer, computer networks or systems as the fulcrum of cyber-terrorism is widely seen in many attempts at defining Cyber-Terrorism. Mark Pollit,[11] defines it as "the premeditated, politically-motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents". [12] Cyberterrorism according to Nazura and Pardis is "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. Furthermore, an attack should result in violence against persons or property, or at least cause enough harm to generate fear." [13] Araromi brings these definitions into context, which allows a convergence of NDPR, Terrorism Act and Cybercrime Act into the Cyber-terrorism jurisprudence. She defines it as "a pre-meditated use of the cyberspace or information systems to launch attacks against computers, computer systems or computer networks with the purpose of attacks on non-combatant person(s) that seriously interfere with, seriously disrupt, or destroy information infrastructures, including, but not limited to, an information system; a telecommunications system; a financial system; a system used for the delivery of essential government services; a system used for, or by, an essential public utility; or a system used for, or by, a transport system in order to cause serious harm, violence or intimidate or coerce the targets with the motive of advancing political, religious, social or ideological agenda". [14]

It is noteworthy that the inclusion of the concept of "computer, computer systems, and/or networks and information contained therein" in globally acceptable definitions and discussions on cyberterrorism, clearly marks out cyber terrorism from terrorism in the traditional sense of it, most of which is envisaged in the Nigerian Terrorism Act. However, where the Cybercrime Act and the Nigerian Data

---

[11] An FBI agent

[12] Zahri Yunos, 'Putting Cyber terrorism into Context', *STAR In-Tech* (2009) <http://www.cybersecurity.my/data/content_files/13/526.pdf> accessed 10 April 2023

[13] Nazura Abdul Manap and Pardis Tehrani, 'Cyber Terrorism: Issues in Its Interpretation and Enforcement' (2012) 2 (3) *International Journal of Information and Electronics Engineering*, 409-410 <http://www.ijiee.org/papers/126-I149.pdf > accessed 10 April 2023.; Marcus Araromi, *supra* n9

[14] Araromi, *supra* n9

Protection Regulation (NDPR) are interpreted with the Terrorism Act, 2022, then, cyber-terrorism appears.

2.2.1 Cybercrime Act 2015 and Terrorism (Prevention and Prohibition Act) 2022

Cyberterrorism as a term is found in only one legislation in Nigeria, which is the Cybercrime Act 2015. However, what entails cyber-terrorism is aptly covered and provided for in the Terrorism (Prevention and Prohibition) Act 2022.

The Cybercrime Act 2015 has its objective outlined in Section 1, as an act that is to "a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; (b) ensure the protection of critical national information infrastructure; and (c) promote cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights."[15] The Cybercrime Act introduces a new paradigm to terrorism in Nigeria by virtue of its Section 18 titled "cyber-terrorism". In this section, it provides that "(1) Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment." This section does mention terrorism, but it does not define terrorism. It states that [ii]*(2) For the purpose of this section, "terrorism " shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended. "* The Terrorism (Prevention) Act, 2011 as amended has been repealed and succeeded by the Terrorism (Prevention and Prohibition) Act 2022. [16]

Terrorism, therefore, as defined by the Terrorism (Prevention and Prohibition) Act 2022 remains applicable to the Cybercrime Act 2015. It also means that in matters of terrorism and cyberterrorism, the Cybercrime Act, and the Terrorism (Prevention and Prohibition) Act 2022 provide joint and complementary statutory framework.

The origin of the cyberterrorism provision in the Cybercrime Act can be traced to its objectives as outlined in Section 1. The Cybercrime Act 2015 states particularly in section 1 (b) that the objective of the Act is "(b) ensure the protection of critical national information infrastructure." The Act however does not define what a critical national information infrastructure is. The closest so defined in the Act is the "critical infrastructure" which "means, 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;"[17] Inspite this express omission of clear definition, it does not undermine

---

[15] Cybercrimes (Prevention and Prohibition) Act 2015, s 1 < https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf&ved=2ahUKEwiF4K2-7rf-AhXYUqQEHRgFBuIQFnoECAoQBg&usg=AOvVaw05eMIXyEnbHv1_bRmjUfdk> accessed 10 April 2023

[16] Terrorism (Prevention and Prohibition) Act 2022

[17] Cybercrimes (Prevention and Prohibition) Act 2015, s 58

the fact that the protection of "critical national information infrastructure" is central to jurisdiction of the Cybercrime Act. This is not however peculiar to Cybercrime Act 2015, as the Terrorism (Prevention and Prohibition) Act 2022 also extensively provides for the protection of critical national information infrastructure.

2.2.2 Critical National Information Infrastructure

The Terrorism (Prevention and Prohibition) Act 2022 in its Section 1(a) states *inter alia* that one of the objectives of the Act is "to provide for- (a) effective, unified and comprehensive legal, regulatory and institutional framework for the detection, prevention, prohibition, prosecution and punishment of acts of terrorism, terrorism financing, proliferation and financing the proliferation of weapons of mass destruction in Nigeria." In Section 2(1) of the same act, it prohibits all acts of terrorism, and in subsection (3) of section 3, it describes acts that will constitute acts of terrorism.

Acts of terrorism are defined and described as "an act willfully performed with the intention of furthering an ideology, whether political, religious, racial, or ethnic," and which *inter-alia* involves, causes, or results in "(iii) destruction of Government or public facility, a transport system, an infrastructural facility, including national critical information infrastructure, a fixed platform located on the continental shelf, a public Cap. place or private property, which may likely endanger human life or result in major economic loss," and "(xi) the disruption of any computer system or the provision of services directly related to the supply of water, power, communications, infrastructure, banking or financial services, utilities, transportation, other essential infrastructure or any other fundamental natural resources, the effect of which is to endanger human life,"[18]

While the cybercrime Act 2015 provides for the protection of "critical national information infrastructure", the Terrorism (Prevention and Prohibition) Act 2022 provides for the protection of "national critical information infrastructure". Similar to the Cybercrime Act 2015, the Terrorism (Prevention and Prohibition) Act 2022 does not define what a national critical information infrastructure is. This may appear as an omission, but a closer examination of the Terrorism (Prevention and Prohibition) Act 2022 shows otherwise. Section 2 (3) (g) (xi) of the Terrorism (Prohibition and Prevention Act) 2022 provides that

> 3) In this Act, "act of terrorism" means an act wilfully performed with the intention of furthering an ideology, whether political, religious, racial, or ethnic, and which—
> (g) involves, causes, or results in—
> (xi) the disruption of any computer system or the provision of services directly related to the supply of water, power, communications, infrastructure, banking or financial services, utilities, transportation, other essential infrastructure or any other fundamental natural resources, the effect of

[18] Terrorism (Prevention and Prohibition) Act 2022, s 2 (3)(g)((xi) b

which is to endanger human life".[19]

2.2.3 Computer Systems Protection

The Terrorism Act 2022 itself does not define what a computer system is, nor does it give any hint. Therefore, recourse is made to the Cybercrime Act 2015, which states that a 'Computer System' "refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated or interactive processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components, which may stand-alone or be connected in a network or other similar devices. It also includes computer data storage devices or media".[20]

In defining a critical Infrastructure, the Cybercrime Act 2015 didn't use the term "computer networks" or "computer system" but "means, systems and assets" thereby making it difficult to readily place "computer or computer systems" within the context of a critical national information infrastructure. Yet, the definition of "critical infrastructure" in the Cybercrime Act 2015 can be placed within the context of "computer systems" as specifically used in Section 2(3)(g)(xi) of the Terrorism Act 2022.[21] The Cybercrime Act 2015 however in Part II does gives a clear description of what a critical national information infrastructure is.

Part II of the Cybercrime Act 2015 provides for the protection of critical national information infrastructure. Section 3 under that Part II provides for the designation of certain computer systems or networks as critical national information infrastructure. It states in subsection 1 of section 3 that

> (1) 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.[22]
>
> In addition, the designation act of the President will include the

[19] Terrorism (Prevention and Prohibition) Act 2022, s 2 (3)(g) ((xi) b

[20] Cybercrime Acts 2015, s 58

[21] xi) the disruption of any computer system or the provision of services directly related to the supply of water, power, communications, infrastructure, banking or financial services, utilities, transportation, other essential infrastructure or any other fundamental natural resources, the effect of which is to endanger human life.

[22] Cybercrimes (Prevention and Prohibition) Act 2015, s 3(1)

> prescription of "minimum standards, guidelines, rules or procedure in respect of - (a) the protection or preservation of critical information infrastructure; (b) the general management of critical information infrastructure; (c) access to, transfer and control of data in any critical information infrastructure; Designation of certain computer systems or networks as critical national information infrastructure, (d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any designated critical national information infrastructure; (e) the storage or archiving of data or information designated as critical national information infrastructure; (f) recovery plans in the event of disaster, breach or loss of the critical national information infrastructure or any part of it; and (g) any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure."[23]

Offences and penalties, including offences against critical national information infrastructure and tampering with critical infrastructure are also provided for in Part 111 of the Cybercrime Act 2015.[24] The penalty for offences against national information infrastructure includes an imprisonment of 10 years or less without an option of fine for any offence punishable under this act committed with intent against any critical national information infrastructure.[25] Also, where the intention and act against any critical national information infrastructure results in grievous bodily harm to any person, such an offender on conviction will be liable to a maximum imprisonment of 15 years or less without an option of fine;[26] and in the event that there is a death of a person, the offender will be liable on conviction to life imprisonment.[27]

It is however not impossible that an offender can be convicted concurrently on these three nature of offences against critical national information infrastructure and sentenced accordingly. It also does not bar a corresponding conviction under the Terrorism Act 2022.

2.2.4 Data Protection

Worthy of note is the conferment of "data" with the status of being a part of or even a critical national information infrastructure. An inference can be drawn from Section 6 of the Cybercrimes Act 2015 which provides that "1) Any person, who without authorization, intentionally accesses in whole or in part, a computer system or network for fraudulent purposes and obtain data that are vital to national

[23] Cybercrimes (Prevention and Prohibition) Act 2015, s 3

[24] Cybercrimes (Prevention and Prohibition) Act 2015, part III

[25] Cybercrimes (Prevention and Prohibition) Act 2015, s 5 (1)

[26] Cybercrimes (Prevention and Prohibition) Act 2015, s 5 (2)

[27] Cybercrimes (Prevention and Prohibition) Act 2015, s 5 (3)

security, commits an offence...."[28] This means that going by section 18 of the Cybercrimes Act and now Section 6, a computer system or network can be accessed in whole or part, and data vital to national security can be obtained, either for terrorism purposes or fraudulent purposes. It also means that a computer system or network need not be designated as a critical national information infrastructure, before a breach of its data, can be for the furtherance of terrorism intent, acts and purposes and correctly regarded as acts of terrorism.[29] An implication of the combined reading of Section 18 and Section 6 is that rather than use a computer system or network or have unauthorized access and use of a computer system or network in furtherance of acts of terrorism, data that is critical to national security can be accessed and used instead. The status and security of "data" as part of a critical information infrastructure or even as a critical national information infrastructure is adequately provided for in Section 3 (2) (c) - (g) of the Cybercrime Act.

Data according to the Cybercrime Act 2015 is defined to mean "representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer"[30] It also defines other forms of data such as "content data" which means "the actual information or message sent across during a communication session;"[31] "computer data" as including "every information including information required by the computer to be able to operate, run programs, store programs and store information that the computer user needs such as text files or other files that are associated with the programme the computer user is running"[32] and "traffic data" as "any computer data relating to a communication by means of a computer system or network, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."

The Terrorism Act in its own context makes provision for data, which it defines accordingly as "information generated, sent, received or stored that can be retrieved by electronic, magnetic, optical or any similar means;" [33] and metadata as "data that provides information about other data", yet it does not designate data as a or a part of the critical national information infrastructure to be protected, neither does it provide for the protection of data generally. The reason is not far-fetched. It uses the word "data" in relation to "communication"[34] which law enforcement agencies

[28] Cybercrimes (Prevention and Prohibition) Act 2015, s 6 (1)

[29] Cybercrimes (Prevention and Prohibition) Act 2015, s 18, s 6

[30] Cybercrimes (Prevention and Prohibition) Act 2015, s 58

[31] Cybercrimes (Prevention and Prohibition) Act 2015, s 58

[32] Cybercrimes (Prevention and Prohibition) Act 2015, s 58

[33] Terrorism (Prevention and Prohibition) Act 2022, s 68 (5)

[34] Cybercrimes (Prevention and Prohibition) Act 2015, s 95 (h); the Act does not define communication but uses the word "communication data". It however defines electronic communication as "communications in electronic format, instant messages, short message service (SMS), e-mail, video, voice mails, multimedia message service (MMS), Fax, and pager;". The definition of electronic communication fits into the concept of communication data as used in the

are empowered to obtain from a communication service provider[35] or relevant "data", which is held by any person, agency, or organisation [36] that are all useful for the purposes of preventing or investigating acts of terrorism.[37]

2.2.5 Nigerian Data Protection Regulation (NDPR) 2019

It is important to say that in addition to the Cybercrimes Act and the Terrorism Act, The National Data Protection and Regulation (NDPR), equally provides for the protection of data as a part of or a critical information infrastructure.

The NDPR promulgated in 2019 by the National Information Technology Development Agency (NITDA, hereinafter referred to as the Agency) as statutorily mandated by the NITDA Act of 2007. It recognises that "many public and private bodies healthcare providers have migrated their respective businesses and other information systems online." And that "iinformation solutions in both the private and public sectors now drive service delivery in the country through digital systems. These information systems have thus become critical information infrastructure which must be safeguarded, regulated and protected against atrocious breaches; COGNIZANT of emerging data protection regulations within the international community geared towards security of lives and property and fostering the integrity of commerce and industry in the volatile data economy; CONSCIOUS of the concerns and contributions of stakeholders on the issue of privacy and protection of personal data and upon evaluation of the grave challenges of leaving personal data processing unregulated." [38]

The NDPR 2019 defines "data" as "characters, symbols and binary on which operations are performed by a computer, which may be filed or transmitted in the form of electronic signals or stored in any format or any device." [39] It defines "Personal Data" to mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP

Cybercrimes Act

[35] Terrorism (Prevention and Prohibition) Act 2022, s 68 (2) (a), (3)

[36] Terrorism (Prevention and Prohibition) Act 2022, s 3 (h)

[37] Terrorism (Prevention and Prohibition) Act 2022, s 68 (1) and (2)

[38] Nigerian Data Protection Regulation (NDPR), The Preamble < https://www.google.com/url?sa=t&source=web&rct=j&url=https://ndpb.gov.ng/Files/NigeriaDataProtectionRegulation.pdf&ved=2ahUKEwiXyeCZ7rX-AhUH76QKHUkIChYQFnoECA8QAQ&usg=AOvVaw0oAe53wYsv7IlsBX8gzZGx> accessed 10 April 2023

[39] NDPR 2019, s 1.3 (d)

address, IME1 number, 1MS1 number, SIM and others";[40] and Sensitive Personal Data" as meaning "Data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information".[41]

From the definition of data as explored in the NDPR, and the preamble of NDPR, it is apparent that closely linked to data is "computer system or network". An overview of preceding discussion shows that what is also central to the Terrorism Act of 2022, the Cybercrimes Act 2015 and the Data Protection and Regulation Act is the use and place of the "computer system or network". The NDPR does not use the word 'computer system' but uses "system" and "computer" independently. It uses "system(s)" in relating to other operations and subjects like "information systems",[42] "digital systems",[43] "online Systems",[44] "data base management systems[45] "file' and 'filing' system"[46] "hackable"[47] "emailing",[48] "legal",[49] "multi-lateral or regional".[50] It however defines a "computer" to mean Information Technology systems and devices, whether networked or not:"[51]

The Terrorism Act uses the word "'computer" and "system" just once, and this time, combined as "computer system". It designates "computer system" and its uses as likely objects of terrorist acts, with a result of "endangering human life or causing major economic loss?'[52] On the other hand, Cybercrime Act 2015 sees a computer system or network as a means of perpetuating acts of terrorism.[53]

Interestingly, there is no provision of the Cybercrime Act that envisages that a computer system or network, can on its own, without a human effort perpetuate acts of terrorism. It defines "person" capable of using a computer or computer systems as "an individual, body corporate, organisation or group of persons;" but one really wonders if this definition of a person within a computer and computer systems or network is sustainable for a long time. The rapid development of Artificial Intelligence and Algorithms into computer systems, network, and technological devices, which are undergoing advanced Machine learning operations to function minimally with human assistance and make decisions on their own, has

[40] NDPR 2019, s 1.3 (q)
[41] NDPR 2019, s 1.3 (v)
[42] NDPR 2019, The Preamble
[43] NDPR 2019, The Preamble
[44] NDPR 2019, The Preamble
[45] NDPR 2019, s 1.3 (h)
[46] NDPR 2019, s 1.3 (e) (m)
[47] NDPR 2019, s 2.6
[48] NDPR 2019, s 2.6
[49] NDPR 2019, s 2.11 (b)
[50] NDPR 2019, s 2.11 (e)
[51] NDPR 2019, s 1.3 (b)
[52] Cybercrimes (Prevention and Prohibition) Act 2015, s 3 (g) (viii)
[53] Cybercrimes (Prevention and Prohibition) Act 2015, s 18 (1)

thrown up the subject of the legal personality or personhood of artificial intelligence in human form, also known as Robots or in other devices. And most recently, chatGPT by OPENAI and other AI services has ushered in a new level of disruption across human endeavours, with new vistas of knowledge and research.

The definitions of the concepts of computer by the Cybercrime Act are quite extensive. The Cybercrime Act defines a "computer" as different from a "computer system". Accordingly, a computer as stipulated in the Act means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility. All communication devices that can directly interface with a computer through communication protocols shall form part of this definition. This definition excludes the following; portal hand-held calculator typewriters and typesetters or other similar devices." On the other hand, Computer System "refers to any device or group of interconnected or related devices, one or more of which, pursuant to a programme, performs automated or interactive processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or media".[54]

The inter-relation of terms across the Nigerian Data Protection Regulation 2019, Cybercrime Act 2015 and Terrorism Act 2020 shows a complementariness of regulatory powers and authorities. Therefore, a revisit of Section 18 of the Cybercrime Act brings into focus, all the preceding discussion on "computer", "computer system" or "network", and "terrorism" in the three Acts, that " 1) Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment. (2) For the purpose of this section, "terrorism" shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended."[55] The Cybercrime Act titles this section as "Cyberterrorism", the first and only use of the word in any legislation, regulation or policy in operation in Nigeria as at the time of this writing.

The impact of acts of terrorism perpetuated through the use of computer networks or systems or technologies, is becoming more pronounced with the evolution of computer services in core areas of human existence and governance. An instance is the emergence of Supervisory Control and Data Acquisition (SCADA) Systems.[56] The SCADA Systems has been defined as "computer systems relied upon by most critical infrastructure organizations (such as companies that manage the power

[54] Cybercrimes (Prevention and Prohibition) Act 2015, s 58

[55] Cybercrimes (Prevention and Prohibition) Act 2015, s 18 (1) (2)

[56] SCADA systems are connected to the internet or internal networks which are connected to the internet for the purpose of ubiquitous access and remote control of the activities

grid) to automatically monitor and adjust switching, manufacturing, and other process control activities, based on digitized feedback data gathered by sensors. These control systems are frequently unmanned, operate in remote locations, and are accessed periodically by engineers or technical staff via telecommunications links."[57]

The impact of the SCADA Systems came into global news when in 2003, 21 power plants operated on the SCADA systems were brought down, and this affected "critically important institutions in the United States and Eastern Canada.[58] The ease and likelihood of a much impact and commission of a cyber-terrorist attack, on systems like SCADA has been linked to certain motivating factors. Brunst,[59] highlighted these factors as: Location Independence,[60] Speed?[61] Anonymity,[62] Internationality,[63] Cost Benefit.[64]

---

[57] Clay Wilson, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress" CRS Report (2005) <http://www.iwar.org.uk/cyberterror/resources/crs/45184.pdf> accessed 25 June 2017

[58] Wilson, *Ibid*

[59] Phillip W, Brunst, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet" in Wade, M. and Maljevic´, A. (eds.), 'A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications' (2010) *Springer Science and Business Media* LLC, 65. < https://www.google.com/url?sa=t&source=web&rct=j&url=https://citeseerx.ist.psu.edu/document%3Frepid%3Drep1%26type%3Dpdf%26doi%3D59291a84e786b7bab163383d4413135bb8d915dd&ved=2ahUKEwjEv8ag77f-AhU3T6QEHfzzBn8QFnoECAcQAQ&usg=AOvVaw06wBwobSj3FcgSYCv3ln4H> accessed 10 April 2023

[60] The attacks on the internet are not location bound which makes it possible for cyber-terrorists to carry out their attacks on a location without being physically present. This gives an advantage over the conventional terrorist attacks where the attackers must be physically at the site to plant a mine, throw a bomb, make sporadic shootings, abduct their victims and other heinous activities that physically impact on the location or victims. It is possible for a cyber-terrorist to launch an attack from a remote location at the victims which makes it possible for him to avoid the danger of being easily apprehended or facing a reprisal attack from the opposition.

[61] Another point of consideration is the speed at which attacks are launched on the internet. Malware such as computer viruses and worms can be launched and spread easily within a very short time without human interaction. The speed at which these malware programs spread is independent of the attacker but dependent on the connection speed of the victims which helps them to spread

[62] Cyber-criminals have the tendency of hiding their identity on the internet and covering their trails. This very advantage makes the internet more endearing for criminal purposes. Even though each computer attached to the internet has an Internet Protocol (IP) address which can be used to trace cyber-criminals it may be difficult where a cyber-café is used to launch an attack. The trail will only end at the café where such café does not keep records of the users. Moreover, there are some technical methods of hiding identity on the internet which include the use proxy servers and anonymity networks. Also, the cyber-attacks perpetrators may simply route their traffic over hacked computers of innocent users.

[63] The features of the internet as discussed above include the possibility of operating from distant location to launch attacks and the anonymity of the attackers. It has been observed that most nations are still operating at national sovereignty level in dealing with network issues which makes

It is apposite to state that the fact that the word "terrorism" is mentioned once in the Cybercrime Act, or that it merely mentions "cyberterrorism" as a title to a two sub-sectioned section 18, does not make it a less important legislation in the Cyber-terrorism legal framework. That emphasis is recurrent in this article, and still being made. This is also because, most of the activities or offences, consequent on the intent of the offender, which constitute steps or activities that may likely lead to Cyber-terrorism constitute the threshold of offences called cybercrime.

The first recorded case of conviction on cyberterrorism was in the US. Ardit Ferizi, had knowingly obtained data of 1,300 U.S Military personnel and federal employees by hacking into a protected computer. The stolen data was then given to ISIS, for target in Terrorist attacks. Two years after, a British Teenager, Kane Gamble targeted the CIA, FBI and Department of Justice database and obtained sensitive information on American military and intelligence operations in Iraq and Afghanistan. He was subsequently convicted of engaging in cyberterrorism. Christen, Denney, and Maniscalco argued that Kevin Mitnick, the world's most famous computer hacker, though unpopular, was labelled a "computer terrorist" by the US Department of Justice. Furthermore, cyber-terrorists have the tendency to crash computer networks, causing functional paralysis and even significant financial loss that could threaten lives or even kill for any reason.[65]

Apart from Cybercrime activities as being a core of cyber-terrorism. Information technology warfare activities have also been identified as most likely to lead to cyberterrorism depending on the intent of the offender. Information warfare has been said to include activities like "computer or network hacking, website defacing, malware programs (such as viruses and worms) infestations, denial-of-service attacks, etc." These activities are also covered by the Cybercrime Acts of 2015.
Cybercrime activities which are a core of cyberterrorism have been identified as one of the challenges of Health Infrastructure in the 21st century. The 2020 COVID-19 Pandemic has become a turning point in all areas of human endeavor. It has equally forced an unprecedented technology inclusion in the existence of man, including his health.

---

the network vulnerable to attack by cyber-criminal, especially by routing their attacks through unregulated or weakly regulated environment. At times, attacks can be routed through countries that do not have the technical wherewithal to trace or investigate cybercrime. This could create problem when investigating internationally operating terrorists.

[64] The cost of launching attacks on the internet is very low compared with cost of physical attacks on the victims which may contain certain overhead costs which could involve procurement of equipment, traveling, planning, training, networking, communicating, etc. Cyber-attacks only require minimal initial investments due to the cheapness of procuring computer gadgets which need not be too sophisticated for the purpose of the attacks. More so, computer network resources are strewed everywhere and easily accessible.

[65] Kevin J. Soo Hoo, Seymour E. Goodman & Lawrence T. Greenberg, *Old Law for a New World?* 'The Applicability of International Law to Information Warfare' The Center for International Security and Cooperation, *(*1997) 44 (3)

The definition of Health by the WHO makes health an inevitable part of human existence. The importance of health to the existence of mankind was more pronounced during the COVID-19 pandemic. However, the pandemic seems not to be over in the healthcare sector all over the world. One of the ways by which health care professionals adjusted and adopted to keep health service delivery on going in the midst of the technology was to adopt the new normal called "Telehealth".

3.0 Telehealth

The field of Telehealth studies presents a peculiarity, which borders on the use of terms to describe the umbrella field of ICT Health Care.[66] Studies that borders on deploying the use of information and communication technologies (ICT) in Health care has been described in many terms such as "e-health", "ICT for health", "medical infomatics", "telehealth", "telecare". [67]

The term most early used in the field of ICT Healthcare is *"Telemedicine"*. Its use was dated as far back as 1960, to describe the exchange of medical care between a doctor and patient(s), even when not in the same physical location. [68] About some years later, *"Telehealth"* was used, in 1978. Telehealth therefor became a term, used with the intent at ensuring an inclusiveness of broader activities in the heath sector, not limited to medical practices of medical personnel.[69]

Another term which has equally held much influence alongside *"telehealth*" is the *"e-health "* term.[70] It was coined during the 'e-terms[4] explosion, that followed the diversified use of the internet to render public services on a large scale. [71] Hence, we had the terms, 'e-commerce, e- mail, e-marketing, e-pay, etc. The *e-health* came to be a term that connotes the delivery of health and/or information services or its enhancement through the use of technologies related to the internet.[72] Today, e-

---

[66] Bashshur, R. L., Shannon, G., Krupinski, E., & Grigsby, J., 'The taxonomy of telemedicine' (2011) 17 (6) *Telemedicine and e-Health,* 484-494 <https://doi.org/10.1089/tmj.2011.0103> accessed 20 September 2022 2022; Nicola Jane Green, *Exploring The Impact of Telehealth VideoConferencing Services On Work Systems For Key Stakeholders In New Zealand: A SocioTechnical Systems Approach,* Ph.D Thesis, Massey University, 2020. < http://hdl.handle.net/10179/16468> accessed 20 September 2022

[67] Deede Gammon, Liv Karen Johannessen, Tove Sorensen, Rolf Wynn & P Whitten, 'An overview and analysis of theories employed in telemedicine studies. A field in search of an identity,' (2008) 47 (3) *Methods of Information in Medicine* 260-269 <https://pubmed.ncbi.nlm.nih.gov/18473093/> accessed 20 September 2022

[68] Green, *supra* n66

[69] Liezl van Dyk., 'A review of telehealth service implementation frameworks' (2014) 11 (2) *International Journal of Environmental Research and Public Health* 1279-1298 <https://doi.org/10.3390/ijerph110201279> accessed September 2022.

[70] Green, *supra* n66

[71] Oh Hans., Rizo C.arlos, Enkin Murray, & Jadad Alejandro, "What is eHealth (3): A systematic review of published definitions" (2005) 41 (1) *World Hospital Health Service* 32-40 <https://doi.org/10.2196/jmir.7.1.e1> accessed 20 September 20, 2022); Green, *supra* n66

[72] Green, *supra* n66

health has taken a new dimension due to the emergence of more intelligent integration of the internet with technology devices through the *Internet of Things (loT)* concepts. As technology became used in health care delivery, the term *"Telecare"* came into being. *Telecare* refers to the facilitation of ICT and monitoring technologies in delivering home-to- home health and social care to persons in their personal or desired locations.[73] The most recently used terminology in the ICT health care domain is the *m-health,* also, referred to as the *mobile health. M-Health* became a known phenomenon in 2003, and it connotes e-health applications popularly known as *Apps,* which are deployed through mobile technologies. [74]

In this paper, recourse is made to the term "telehealth" rather than "telemedicine". Firstly it is because the latter is a subset of the former. *Telemedicine* denotes some more specific medical practices, while *Telehealth* provides an over-arching concept that embraces other specified areas of medical practices not covered by telemedicine, especially in the case where the health care provider and recipient are not located in the same physical location.[75]

3.1 CYBER-CHALLENGES TO TELEHEALTH

The foremost challenges to Telehealth globally are related to cybercrime activities, which provide a ground for cyber-terrorism. Niger Cyber Hacktivists, a group of Nigerian hackers, attacked government sites including the National Poverty Eradication Programme website and the Niger Delta Development Commission, posting a letter protesting against misappropriation of funds by the government and the country's Freedom of Information Act. Later in January 2013, the Economic and Financial Crime Commission (EFCC) was attacked in response to reports of corruption. Cyberattacks, in the form of denial-of-service and computer bugs, cost the Nigerian government about $200 million annually. The exponential growth in mobile telecommunication users and the rise in social networking, potential sources of globalization, especially among the multitudes of unemployed youths in Nigeria are the twin factors that drive cybercrime and terrorist activities. According to a report issued by Center for Internet Security, [76] one of the key issues of the healthcare industry are largely cyber-security related, such as malware, [77] and the distributed denial of service (DDOS).[78] For instance, the highest number of data

---

[73] Solli Hilde., Bjørk Ida Torunn, Hvalvik Sigrun. & Hellesø Ragnhild., 'Principle-based analysis of the concept of telecare', (2012) 68 (12) *Journal of Advanced Nursing*, 2802-2815. < https://www.researchgate.net/profile/Hilde-Solli/publication/225046177_Principle-based_analysis_of_the_concept_of_telecare/links/60705904a6fdcc5f77912d91/Principle-based-analysis-of-the-concept-of-telecare.pdf> accessed 20 September 2022; Green, N.J, *supra* n1

[74] Green, *supra* n66

[75] Green, *supra* n66

[76] Centre for Internet Security, "Cyber-attacks in the Healthcare Sector" <https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/> accessed 10 December 2022.

[77] Malware compromises the integrity of systems and privacy of patients

[78] (DDoS) attacks that disrupt facilities' ability to provide patient care

breaches reported in any industry or sector in 2021 was recorded in the health sector.[79] The definition of critical infrastructure in the Cybercrimes Act 2015 includes systems and assets vital to the country and that a destruction of which would have an impact on the national public health and safety of the country.

The healthcare sector provides a unique field of opportunities for Cybercrime activities, as well as unique challenges. First, is that medical data, which is included in the definition of the NDPR as being sensitive data,[78] [80] is indeed, invaluable, and usually a target for any cyber-criminally minded individual. It must be said that the bridge between cyberterrorism and the healthcare system is cyber-attacks or cybercrime. The channel that makes cyber-attacks more prominent is the infusion of technology in health practice and care delivery.

A cyber-attack on a healthcare organisation is aimed at stealing large quantities of sensitive health information, which are usually protected. Hence, the year 2020 witnessed a surge in the rate of cyberattacks targeted at health care institution.[81] Cyberattack is usually carried out by hackers, who use different cyber methods to steal information and gain value from information. For instance, a cyber-attack using ransomware will steal health information for the sake of ransom. A ransomware allows a hacker to hold a healthcare system hostage until a ransom is made. Usually, such ransom is requested or paid for in millions of dollars. This usually is far more than a ransom demanded by a terrorist or kidnapper.

It is interesting to know that even advanced countries which boast of the best of technological advancements and cybersecurity, have not had their healthcare sector spared from the surge of cyber-attacks. For instance, the Kaspersky Security report highlighted some notable attacks in some international jurisdictions.[82] The HIPPA Journal, reported in July 2021, that about 70 data breaches of 500 or more records were recorded across health entities in the US. It even reported that between August 2020 to July 2021, there were over 700 reported data breaches of 500 or more healthcare records, which led to a compromise of over 44,369, 781 health data of individuals.[83] In Germany, also during the pandemic, it was reported that the "number of successful cyberattacks on health service provides operating critical infrastructure more than doubled." [84] In Dusseldorf University Hospital, Germany,

---

[79] The HIPAA Journal, "Healthcare Industry Has Highest Number of Reported Data Breaches in 2021" (August 5, 2021) <https://www.hipaajournal.com/healthcare-industry-has-highest-number-of-reported-data-breaches-in-2021/> accessed 20 December, 2022

[80] "Sensitive Personal Data" means Data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records, or any other sensitive personal information; NDPR 2019, s 1.3 Definitions.

[81] HIPAA Journal, *supra* n79

[82] AO Kaspersky, 'Kaspersky Security Bulletin 2021 Statistics' <https://securelist.com/ksb-2021/> accessed March 20, 2023

[83] HIPAA Journal, *supra* n79

[84] AO Kaspersky, "Kaspersky Security Bulletin 2021 Statistics" available at <https://securelist.com/ksb-2021/> accessed 20 March, 2023)

over 30 computer network servers were held to ransom, causing the cancellation of surgery, the closure of emergency room and the near death of a female patient whose ambulance had to be redirected from the Dusseldorf Hospital to another hospital. France has not been left out in the global healthcare epidemic.

As of 2020, the media reported over 20 massive cyberattacks against health institutions, and in 2021, the situation worsened with about one major ransomware attack per week. The same trend was recorded in Spain, where over 45,000 harmful attacks were identified by authorities, which were targeted against health sector organisations. Same in Ireland, where a ransomware attack in 2021 that "severely disabled a number of HSE systems" resulted in the shutdown of most of the HSE systems. The outcome of this was that several services in Ireland which relied on digital processes such as scans, referrals and diagnostic services had to be operated manually, causing serious delays.[83] [85] In all these cases, the huge disruption and financial losses incurred during each attack is enormous. For example, one of the largest healthcare providers in the US, which operated about 25 hospitals providing acute care, 330 behavioral health facilities and 41 outpatient facilities reported a loss of 67 million dollars following an experienced Ryuk ransomware attack. In addition, a California-based nonprofit health care provider with five hospitals and over 10 outpatient facilities, reported that when it experienced a ransomware attack in 2021, it could not access the information systems at two of its hospitals. This ransomware attack affected the access by staff to electronic medical records, shut-down of offsite back-up servers, and as such, the stroke and heart attack patient from about three of its main hospitals had to be rerouted to other hospitals while trauma patients brought to two of its hospitals had to be redirected to other hospitals. It lost about 91.6 million dollars in revenue and spent over 21.1 million dollars on response and recovery, though over 140,000 patients had their health information compromised.

The threat to healthcare is not expected to decrease in years to come. This had been attributed to the tech-rush fever that bit the healthcare system all over the world so hard, causing digital transformation, and remote healthcare delivery services. This digital transformation in the healthcare system, has been described as telehealth or telemedicine.

3.2 TELEHEALTH TRENDS AND VULNERABILITIES

In Nigeria, three likely trends of telehealth digital transformation may be experienced, forming core infrastructure of telehealth in Nigeria. They are:

a. Virtual Care and Remote Medicine:

The shift from physical and onsite appointments and consultation to remote and virtual ones has been the benchmark of telehealth or remote medicine. This was spurred by the burden on doctors and nurses, stretched to capacity, but were needed to keep the healthcare sector running, yet avoiding any form of physical contact during the pandemic. Even though there is usually the

[85] AO Kapersky, *supra* n84

need at time for some physical consultation in a normal health setting, the presence of technology to make such meetings less desirable and more evitable has come to stay.[86]

The side effect of remote consultations and appointment involves digitising offline records to be available as data and information available for both parties. Equally, new information will then be uploaded online for further deliberation. For instance, the electronic medical records have become the new form of data to support telehealth practice. The sensitivity and value of medical data consisting of various information from health care providers and recipients, which was earlier discussed has made healthcare data beach one of the costliest and can make a cyberterrorist attack one of the gravest.[87] This then leads to the second trend of Data Security and Cloud Adoption.

b. Data Security and Cloud Adoption

During the pandemic, over 60% of health care organisation moved into cloud. This is because of the enormous quality and quantity of data of patients being processed from time to time. Data including the online searches, mobile phone information and communication data and health information requested or processed, are all citizens data which help healthcare providers have a clearer understanding of *a* patient's treatment plan.[88]

The cloud adoption for data storage and seamless telehealth provision brings in other players into the telehealth care provision apart from the main hospital or health care providers. This collaboration times entails exchange of data collected on a patient or healthcare subscribers in one or more health facility. The availability of medical data in one place, through cloud adoption, allows an analysis of the data, and thus produce unique trends or information about a patient that will attract personalized healthcare services. For instance, McKinsey reports that "'broad consensus exists that the use of cloud technologies could unlock digital and analytics capabilities across the healthcare spectrum...' by 'enabling them to more effectively innovate (for example, new use cases in analytics, IoT, and automation), digitize (for example, stakeholder journey transformation), and realize their strategic objectives.'[87] [89] The risk of adopting an inevitable cloud infrastructure is that hospitals and clinics have become a data bank themselves.

c. Artificial Intelligence, Internet of Things (IoT) and Internet of Medical Things (IoMT).

The availability of data equally enables another trend of Telehealth in Nigeria, which is the Artificial Intelligence, Internet of Things (IoT) and Internet of Medical

[86] AO Kapersky, *supra* n84

[87]AO Kapersky, *supra* n84

[88] AO Kapersky, *supra* n84

[89] AO Kapersky, *supra* n84

Things (IoMT) .[88] [90]

While in remote medicine and cloud adoption, there is much presence of health and IT personnel, the Artificial Intelligence and Internet of things and Internet of Medical Things looks forward to having more devices be networked together, trained intelligently to work with little or no human interference, using the data fed into it. The data fed into it will include the medical data, that is data on a patient and also data gained from an electronic observation and analysis of physical medical practices. Hence, by the Al, IoT and IoMT, the telehealth care innovation is to see more tasks performed by less human efforts. The less human efforts is because there are technologies that are able to do same or more than a human effort can produce, yet at a lower cost. Again, according to McKinsey, 'Al has the potential to transform how healthcare is delivered, by supporting improvements in care outcomes, patient experience and access to healthcare services; increasing productivity and the efficiency of care delivery and allowing healthcare systems to provide more and better care to more people; and helping to improve the experience of healthcare practitioners, enabling them to spend more time in direct patient care and reducing burnout.'[89] [91]

The potential of Al, IoT and IoMT as a form of Telehealth practice is yet to be untapped, even globally, talk less of Nigeria. For Instance, it is estimation that about "85,000 medical devices can be connected to the network of a Hospital, including MRls, computed tomography, ultrasound, nuclear medicine and endoscopy systems, as well as systems communicating with clinical laboratory analyzers such as laboratory information systems."[90] [92]

d. Vulnerable Point for Telehealth

These three prominent structures of Telehealth care practice highlighted above are however vulnerable to cyber-attacks and even terrorism through two roles, which are that of: visible human actors and invisible human actors.

i. Visible Human Actors (VHA):

Visible Human actors refers to the inevitability of having human personnel presence and participation in telehealth care delivery. For example, Verizon in its Data Breach Investigations conducted in 2018 found out that, the only industry that has more internal actors responsible for its breach, that external actors is the health care industry. That means that in 2020 where 8.5 million medical records were exposed after a compromising incidents of data breaches, an insider was responsible for 1 in 5 of that data breaches that occurred. The insider breaches can either be intentional or non-intentional. The non-intentional insider breach involves error or wrongdoing, yet they equally account for the exposure and compromise of over 8 million records of individuals in 2020, with insider error contributing

[90] AO Kapersky, *supra* n84

[91] AO Kapersky, *supra* n84

[92] AO Kapersky, *supra* n84

7,673,363 and insider wrongdoing incidents causing a theft and exposure of about 241,128 records.[93]

The Nigerian principal legislation for regulating the healthcare is the National Health Act (NHA) 2014. It makes adequate provisions for the role of visible human actors in the health and telehealth industry. The NHA in its section 26 (1) states that "all information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment is confidential". The import of this section is to safeguard the confidentiality of health data record, which are susceptible to the activities of visible human actors. This obligation of confidentiality is not absolute. Hence, where there is an order by a court of competent jurisdiction or the consent of a person required by law is given for disclosure or such a disclosure will have no threat to the owner of the records and the public, then the role of a visible human actor as regards confidentiality of data is permitted. Equally, the National Health Insurance Scheme Act (NHIS Act) provides for a secrecy obligation that binds the officials and other employees to treat with secrecy and confidentiality all data and information obtained in the course of their duty or in the exercise of their powers. Also like the NHA Act, the NHIS Act allows a variation of this obligation of secrecy on the ground of disclosure to a court or an arbitration as contained in section 38.[94]

As touching consent, section 28 (1) of NHA states that a patient is permitted to consent to the access of its health record by a healthcare provider. It also provides that where the interest of the patient is paramount and there is need for research, the consent of the patient can be sought and given. However, where information that is personally identifiable is not included in a research data which is to be used the purposes of further research, teaching, and studying, then the authorisation and/or consent of the patient or any other prescribed authority can be dispensed with. Section 27of the NHA provides further on disclosure to a third party, as a visible human actor. It provides that if a disclosure is important to be provided to another healthcare service provider or personnel, it will be permitted on the grounds of legitimate purpose within the ordinary course and scope of his or her duties. Also the interest factor comes to play, where the interest or intention of the user is legitimate.

ii. Invisible Human Actors (IHA):

The invisible human actors (IHA) are the real threats to cyber-terrorism and likely perpetrators of cyberterrorism. These invisible human actors can be categorised as hackers. Hacker groups are in different levels, according to the level of technological expertise. Also, hackers can differ according to intent and purpose of association.

A distinguishing fact between hackers and terrorist is usually the organisation they belong to and the intent of their operations. It is also important that a cyber-

[93] AO Kapersky, *supra* n84

[94] It also prescribes a fine of not less than N20,000 or imprisonment for a term of two years or both.

terrorist usually engage in activities of a cybercrime nature, but with a goal, means and result that is of a terrorism nature. The hackers simpliciter are human actors whose hacking or cybercrime activities is for their enjoyment or struggle for more individual hacking exploits, either for financial or other reasons. But a cyber-terrorist is also a hacker whose activities are in furtherance of a terrorist organisation operations like the Al-Qaeda, or sympathetic to the goals of a terrorist organisation and helps, the cyberspace activities of the hackers contributes to the fulfilment of certain goals of the terrorist group.[95] [96]

Using it is obvious that a hacker so called, and a cyber-terrorist all have the same modus operandi. However, usually, a cyber-terrorist is usually linked with non-tech terrorist and communicates with traditional terrorism actors, as such, there are usually trails by which one can trace a cyber-terrorist, unlike a hacker, who association is merely online.[94] [97] In most cases, hackers either steal data or hold a system containing data hostage for some pecuniary benefits. But the frequency of hacking for data theft or ransom payment is more than that of cyber-terrorist.[95] [98] Like a tradition and physical terrorist attack, a cyber-terrorist usually makes his aim known or leaves a trail of messages that can be deciphered or carries out the cyber-terrorist attack at a sensitive and relevant time by which one can link the cyber-terrorist attack to a group or groups of terrorist.[96] [99] For example, an attack on an electrical plant that supplies electric power for citizens and business in a country will be deemed to be more of cyber-terrorism than hacking. Because the loss of electricity will bring no gain to a hacker but much more a terrorist group, who will see the black-out that results from the cyber-attack on the electric system as an achievement or promotion of an ideological goal or political statement.

In guiding against invisible human actors, the National Health Act (NHA) in its section 29 mandates that the management or authority of a healthcare facility puts in place "control measures to prevent unauthorized access to those records and to the storage facility in which, or system by which, records are kept". The implication of this is that there must be a corporate policy adopted by the management and staff of the healthcare organisation or facility ensure both offline and online security

---

[95] Ottis Rain, Lorentz, Peter, 'Cyberspace: Definition and Implications', *in Proceedings of the 5th International Conference on Information Warfare and Security, Dayton* (2010), Oklahoma, Reading: Academic Publishing Limited, pp 267-270.; < https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.researchgate.net/publication/236886275_Cyber_Terrorism_and_Cyber_Crime_-_Threats_for_Cyber_Security&ved=2ahUKEwjcvoXrgLb-AhWi8rsIHeqQCHwQFnoECBAQAQ&usg=AOvVaw01ej7BdW8TGScy6CzDWCWc> accessed 10 April 2023.

[96] Jugoslav Achkoski and Metodija Dojcinovski, "Cyber terrorism and cybercrime – threats for cyber security", *Global security and Challenges of the 21st century,* MIT University – Skopje (2012) < https://www.researchgate.net/publication/236886275_Cyber_Terrorism_and_Cyber_Crime_-_Threats_for_Cyber_Security> accessed 10 April 2023

[97] *ibid*

[98] Achkoski *et al supra* n*96*

[99] Achkoski *et al, supra* n96

of data. On the other hand, the Cybercrimes (Prevention and Prohibition) in its section 21 equally mandates that a cyber-attack or threat in this context of a health facility or health data records, must be reported to the Nigeria Computer Emergency Response Team (NgCERT).[97] [100]

4.0 CONCLUSION AND RECOMMENDATIONS

By way of conclusion, it is also noted that coupled with the National Health Act, Cybercrimes Act, and Terrorism Prevention Act, other legislations that will apply to containing cyberterrorist activities in the health & telehealth sector include but not limited to the Code of Medical Ethics 2008,[101] Freedom of Information Act 2011,[102] Guidelines for The Management of Personal Data By Public Institutions in Nigeria 2020,[103] Medical and Dental Practitioners Act,[104] National Agency for Food and Drug Administration and Control (NAFDAC) Act 2004,"[105] Federal Competition and Consumer Protection (FCCP) Act 2O18,[106] National Health Insurance Authority Act

---

[100] The Federal Government coordination centre responsible for managing cyber incidents in Nigeria. <https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.cert.gov.ng/&ved=2ahUKEwi5qZ72_7X-AhUNIMUKHacNApUQFnoECDMQAQ&usg=AOvVaw3u3zbesaJbMhZLD0Hr6aiM> accessed 10 April 2023

[101] Code of Medical Ethics < https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.mdcnigeria.org/downloads/code-of-conducts.pdf&ved=2ahUKEwiZ7byh77X-AhXWt6QKHbC9BDcQFnoECBIQAQ&usg=AOvVaw3IQpYoqdkvk0-o2DBf5JzG> accessed 10 April 2023

[102] Freedom of Information Act 2011 < https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.cbn.gov.ng/foi/freedom%2520of%2520information%2520act.pdf&ved=2ahUKEwjxyMmM77X-AhUO_qQKHT1PBt4QFnoECBUQAQ&usg=AOvVaw0cYIfllnMLXDoa6Mohu2Bs> accessed 10 April 2023

[103] Guidelines for The Management of Personal Data By Public Institutions in Nigeria 2020<https://www.google.com/url?sa=t&source=web&rct=j&url=https://ndpb.gov.ng/Files/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal11.pdf&ved=2ahUKEwjNvbX77rX-AhWC-6QKHeWgBIcQFnoECA8QAQ&usg=AOvVaw38cpII9oxHdQh2UY7oXjeP>

[104] Medical and Dental Practitioners Act <https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.mdcnigeria.org/downloads/cap-m8.pdf&ved=2ahUKEwj4k7bd7rX-AhWRq6QKHQJ_DagQFnoECBYQAQ&usg=AOvVaw3cl0ZFWHoa2tqFpqjofb0S> accessed 10 April 2023

[105] NAFDAC Act creates policies, regulates, and controls the importations and sale of drugs and health products < https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.nafdac.gov.ng/wp-content/uploads/Files/Resources/Regulations/NAFDAC_Acts/NAFDAC-ACT-Cap-N.-1-LFN-2004.pdf&ved=2ahUKEwiP3Mbi7bX-AhXB2qQKHQG3AmcQFnoECBoQAQ&usg=AOvVaw1133HeC69QZCGAUUImSRqf> accessed 10 April 2023

[106] FCCP Act promotes and protects the interest of consumers of products in Nigeria.< https://www.google.com/url?sa=t&source=web&rct=j&url=https://fccpc.gov.ng/wp-content/uploads/2022/07/FCCPA-2018.pdf&ved=2ahUKEwjAw52m5bX-AhUarKQKHe3yCZ8QFnoECBsQAQ&usg=AOvVaw3z2Y5PVIuNJVrI-pwbc_Vh> accessed 10 April 2023

2022,[107] National Information Technology Development Agency (N1TDA) Act 2007[108] and Guidelines, Nigeria Data Protection Regulation (NDPR),[109] Nigerian Communications Commission Act[110] and Guidelines, Patients Bill of Rights, Standards Organisation of Nigeria (SON) Act of 2015.[111]

This study finds that there is no single legislation for cyber-terrorism in Nigeria, hence the need to combine several legislations together. It also finds that the health-related legislations are insufficient for cyber-challenges such as cyber-terrorism. It equally finds that the mention of healthcare in cyber-related legislations as examined above are not enough in addressing cyber-challenges in healthcare as they do not specify on the modalities of their application to healthcare. They best serve as a statutory premonition of grave cyber-challenges to healthcare like cyber-terrorism. Hence, it is highly recommended that the hint provided by the cyber-related legislations be heeded urgently, through the statutory and policy formation of a cyber-health focused policies that harness legal and regulatory powers for cyber-terrorism and other health cyber-phenomenon. The urgency of such legal and policy formulations has been heightened by the release chatGPT by Open AI, which may endanger digital health sensitive information and infrastructure.

---

[107] National Health Insurance Authority 2022 < https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.nhis.gov.ng/download/nhia-act-2022/&ved=2ahUKEwji2L_K7rX-AhVSDewKHUuOAP4QFnoECAgQAQ&usg=AOvVaw37orhFzYQKsEN_boiyn17f> accessed 10 April 2023

[108]National Information Technology Development Agency (N1TDA) Act 2007 <https://www.google.com/url?sa=t&source=web&rct=j&url=https://nitda.gov.ng/nitda-act/&ved=2ahUKEwiQ0aS77rX-AhUGtqQKHXmBBscQFnoECBQQAQ&usg=AOvVaw2sDT2J30FGbHGDIfje6bfw> accessed 10 April 2023

[109] Nigerian Data Protection Regulation (NDPR) 2019 <https://www.google.com/url?sa=t&source=web&rct=j&url=https://ndpb.gov.ng/Files/NigeriaDataProtectionRegulation.pdf&ved=2ahUKEwiXyeCZ7rX-AhUH76QKHUkIChYQFnoECA8QAQ&usg=AOvVaw0oAe53wYsv7IlsBX8gzZGx> accessed 10 April 2023

[110] Nigerian Communications Commission Act <https://www.google.com/url?sa=t&source=web&rct=j&url=https://ncc.gov.ng/documents/128-nigerian-communications-act-2003/file&ved=2ahUKEwiNvpH_7bX-AhUFuKQKHfEwAWwQFnoECCAQAQ&usg=AOvVaw0gCvnCplfRgTLPcJ9-jxSR> accessed 10 April 2023

[111] SON Act 2015 sets the standards for medical device technologies produced and imported into the country <https://www.google.com/url?sa=t&source=web&rct=j&url=https://nigeriatradeportal.fmiti.gov.ng/media/SON-ACT-2015.pdf&ved=2ahUKEwitjZHK7bX-AhXSJ-wKHb4wDRoQFnoECBkQAQ&usg=AOvVaw2ytQ84ts5olutLPicrZ7Eu> accessed 10 April 2023