International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 30-09-2023, Accepted: 15-10-2023, Published: 31-10-2023
Volume 9, Issue 5, 2023, Page No. 257-262

Cyberspace, cybercrime and the emerging legal dimensions in Nigeria

Kelvin Bribena
Faculty of Law, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria

Abstract
Given greater connectivity and sophistication in the world, the goals of cyber attackers have been evolving from traditional criminality to disruption of economic activity and infrastructure. In some cases, instead of stealing information, technical designs, defence secrets, nuclear warheads, military secrets, university research labs, computer forensic investigation secrets etc. Computer criminals destroy computer applications and crash communication networks through computers. The research method employed here was the black letter otherwise known as the doctrinal method which involved the use of primary and secondary sources of law in analyzing the subject matter. The paper expatiated on national and international implications of growing cyber threats within our cyberspace, it assessed the existing national, regional and international instruments so as to assist in establishing a sound legal foundation. The paper interrogated whether we have the right cyber infrastructural balance in our cyberspace given the pace at which technology is growing and the need for privacy protection, cybersecurity and data protection. The work found the need for extensive campaign and awareness of cyber safety and so recommended a strong collaborative work at all private institutional levels/tiers of government in order to fortify our digital infrastructure and cyberspace borders. It suggested that Nigeria should bring its national laws up to international benchmarks to achieve global networking and compliance.

Keywords: Cyberspace, cybersecurity, cybercrime, computer, legal dimensions, information communication technology (ICT)

Introduction

The definition and scope of cybercrime vary by jurisdiction, mostly reflecting the sociocultural background of each nation [1]. However, any criminal activity that uses a computer as a tool, a target, or a medium to facilitate other illegal behaviors can be broadly classified as cybercrime. It also includes more conventional types of criminal activity where the computer is either the subject or the object of the crime [2].

Therefore, any electrical, magnetic, electrochemical, digital, optical, or other high-speed data-processing equipment that can carry out arithmetic, logical, or storage operations, as well as any related data storage facility, is considered a computer. The device allows people of all backgrounds to come together in banking arena, cafés, defence platforms, connection of civil societies, refugee camps, political groups, electoral processes, etc. It is a crucial device for national security, national elections, stock markets, land title verification, registration of tax, revenue issues, crime detection and prosecution [3], traffic, clean water and electricity supplies.

Cyberspace is a fact of daily life which includes the internet and the hundreds of millions of computers the internet connects, the institutions that enable it, and the experiences it enables. It has evolved into a crucial aspect of modern civilization, influencing people in both wealthy and developing nations to face a new reality. Therefore, network-supported computer systems that are accessible through interconnected platforms and that provide multidimensional worlds, whether artificial or "virtual," are referred to as cyberspace [4].

Users can engage in activities conducted through electronic environments whose operational domains transcend traditional territorial, governmental, social, and economic borders thanks to cyberspace. Due to the complexity and specialized nature of the operations involved, access was first restricted to a small and powerful group, which limited participation. But since then, the world's access to cyberspace has greatly increased. Around two billion people were using the internet as early as 2010, which opened up new avenues for rivalry, conflict, and the quest for influence and power. Additionally, it makes it easier for people to communicate with one another, which promotes idea generation, information sharing, increased access to knowledge, and other ways of thinking [5].

Cybercrime refers to illegal activities that are conducted via information and communication technology, including mobile devices and the internet [6]. A broad range of behaviors are usually included under cybercrime laws, including as hacking, infringement of intellectual property rights, and the distribution of illegal or harmful content, such as child pornography and racist or xenophobic materials. According to some academics, there are three main types of cybercrime: crimes against people, like online harassment or the dissemination of pornographic content; crimes against property, like software piracy and the unapproved sharing of copyrighted movies and music via peer-to-peer networks; and crimes against the state, like cyberterrorism. However, cybercrime laws in many jurisdictions frequently ignore cybercrimes against individuals in favor of corporate interests and state security risks.

ICT technology has become ubiquitous and has enhanced national and economic developments in aviation, shopping, national defence and intelligence, immigration, stock markets, terrorism, electoral processes, online activism, crime prevention, prosecution. However, this boundless promise has also been used negatively by criminals in many perilous ways. Cybercrime is indeed, a hydra-headed monster living with us now. Nations, who lose in the battlefields of land, sea and air now fight even in the cyber space.

International Jurisdiction

In 2014, the government of the United States of America budgeted $13 trillion on its cyber defence programs to protect government computers and networks and to share intelligence with private industry [7].

In the United States of America, numerous statutes have been enacted to safeguard users within cyberspace. These include the Comprehensive Crime Control Act of 1984; the Computer Fraud and Abuse Act of 1986 (CFAA); the Electronic Communications Privacy Act of 1986 (ECPA) [8]; and the National Information Infrastructure Act of 1996 (NIA) [9]. Also notable is the Economic Espionage Act of 1996, which was enacted to give effect to the World Intellectual Property Organization Copyright Treaty and the WIPO Performances and Phonograms Treaty, both of which were designed to modernize international copyright law in response to emerging technologies. Additional legislation includes the Identity Theft and Assumption Deterrence Act of 1998 (ITAD), the Identity Theft Penalty Enhancement Act of 2004 [10], and the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 [11].

Identity theft and financial fraud are only two examples of the many intricate and extensive kinds of cybercrime that have emerged on a global scale [12]. For example, in 2012, the largest oil business in the world, Saudi Aramco, was hit by a self-propagating malware that destroyed gigabytes of data and erased software and source code from up to 30,000 systems. A few months later, Bank of America, Wells Fargo, and a number of other significant US banks were the target of another undisclosed cyberattack that frequently interfered with their online operations. Similarly, more than 1,000 centrifuges at Natanz, which at the time was the center of Iran's nuclear program, were destroyed by the "Stuxnet" malware, causing significant physical harm [13].

These sophisticated cyberweapons have the ability to seriously damage vital national infrastructure, including water and electricity systems, air traffic control, financial institutions, and civilian and military communication networks, often with no traces of the attacker.

In a similar instance, malicious software was used by a combined US-Israeli operation called "Olympic Games" [14] to change the operating speeds of centrifuges at Iran's nuclear enrichment site in Natanz, causing the centrifuges to malfunction and ultimately destroy themselves.

Two major cyberattacks, one targeting a German steel mill in 2014 and the other interfering with Ukraine's electrical grid in 2015, caused severe physical destruction comparable to the catastrophic effects of atomic weapons. Numerous cybersecurity experts attribute both incidents to Russian agents. Despite these developments, even technologically advanced governments have shown little interest in restricting cyberwarfare or cyberweapons because both state-sponsored and individual cyber activities remain covert.

One typical justification of secrecy is the preservation of sources and procedures, and regulation is made considerably more challenging by the absence of comprehensive international rules controlling cyberspace. Because of this, the evolving global cybersecurity architecture is still far behind the strategic arms control framework, even in spite of two UN General Assembly resolutions urging state [15] s to adhere to the laws of armed conflict in cyberspace and bilateral cybersecurity agreements between the United States and China [16].

Furthermore, cybercrime frequently results in infringement of intellectual property rights. One such example is the Louis Vuitton v. Net-Promotion lawsuit [17]. In this case, the Louis Vuitton trademarks and the disputed domain name "luisvuitton.com" were examined in compliance with Article 16 of the TRIPS Agreement and Article 6 of the Paris Convention. The only distinction between the complainant's trademark, "Louis Vuitton," and the respondent's domain name was the letter "o." It was believed that this minor alteration would not be noticeable to the majority of people in either Spanish or English, and search engines would likely direct visitors to both "vuitton.com" and "luisvuitton.com." The adjudicating panel concluded that the complainant's domain name and trademarks were confusingly similar to those of the respondent.

Additionally, over a thousand domain names registered in eBay's name were successfully transferred to the online auction and e-commerce site. Over 1,153 domain name disputes involving eBay's claimed bad-faith registration were decided by the World Intellectual Property Organization's (WIPO) Arbitration and Mediation Center. The challenged domain names were in fact registered in bad faith in violation of the Uniform Domain Name Dispute Resolution Policy (UDRP), according to WIPO, which upheld eBay's claims. The term "eBay" was used in all of the challenged domain names, together with three numeral characters and either a ".com" or ".net" suffix.

Domestic Jurisdiction

As a developing nation, cybercrime in Nigeria consist mainly of a group of socio-economic offences against property, title documents (cloning) intellectual property infringements, financial crimes, hacking, phishing and registration of other persons' domain names. The enormity of intellectual property infringements is compounded by the huge population of over 180 million people which inhibits economic development and foreign investments.

Nigerian prosecutors have turned to the Economic and Financial Crimes Commission (EFCC), which is charged with looking into, prosecuting, and upholding laws pertaining to all economic and financial offenses, in the lack of a comprehensive cybercrime statute [18].

Undoubtedly, the major contributions of the Cybercrimes Act are found in the wide coverage of cybercrimes and penalties. The Act descends heavily on fines and terms of imprisonment on cyber criminals concerns on national especially theft or alteration of national, government, financial institutions networks.

a. **Computer Related Fraud:** It is illegal for someone to intentionally change, erase, enter, or suppress any computer data, whether for financial gain or not, in order to cause another person to lose property [19]. A person who knowingly enters data that produces false information with the intention that it be regarded or acted upon as authentic faces a minimum fine of N7,000,000.00, a minimum sentence of three years in jail, or both [20]. Whether or not the data is legible or understandable is irrelevant. In a same vein, anyone who transmits an electronic message with the aim to deceive and grossly misrepresents any fact upon which reliance causes damage or loss is guilty of an offense and faces a minimum five-year jail sentence, a fine of N10,000,000.00, or both.

b. **Theft of Electronic Device:** Any person who steals infrastructure terminal owned either by the government or a financial institution is liable to 3 years imprisonment or a N1,000,000.00 fine or both; Stealing an Automated Teller Machine (ATM) attracts either 7 years imprisonment or a fine of not more than N10,000,000.00 or both. Merely attempting to even steal an ATM Machine attracts a punishment of 1-year imprisonment or fine of not more than N1,000,000.00 or both upon conviction.

c. **Electronic Signatures:** The Act only allows electronic signatures for legally enforceable contracts pertaining to the purchase of goods and services. Wills, codicils, other testamentary documents, death and birth certificates, family law cases (such as marriage, divorce, and adoption), court orders, affidavits, pleadings, motions, notices, judicial documents, and directives from authorized authorities (such as withdrawal orders for hazardous or expired drugs or chemicals) cannot be signed electronically. It is illegal to use electronic signatures in these situations.

d. **Accessing, interfering with, or destroying any computer, system, or network for terrorist purposes is illegal:** This clause, which stipulates life in prison upon conviction, is especially pertinent to combating Boko Haram and other insurgencies in Nigeria [21].

e. **Identity Theft and Impersonation:** Also known as phishing, these crimes carry a maximum sentence of seven years in jail, a fine of N500,000.00, or both.

f. **Child pornography and related offenses:** These offenses are strongly condemned by society and attract sentences of one to fifteen years in jail or penalties of N250,000.00 to N25,000,000.00. Producing [22], distributing [23], making available [24], and possessing child pornography [25]; obtaining child pornography for oneself or others [26]; and usingcomputer systems to solicit a minor for sexual activity are all illegal [27]. Additionally, the Act forbids enlisting, forcing, or exposing a minor to exploitative or pornographic performances [28].

g. **Cyberstalking and Cybersquatting:** It is illegal to intimidate or threaten anyone online. Penalties include three to five years in prison, penalties ranging from N7,000,000.00 to N25,000,000.00, or both. Cybersquatting is punishable by a fine of N5,000,000.00, two years in jail, or both.

h. **Distributing racist or xenophobic literature [29]:** Threatening people on the basis of their race, ethnicity, or religion, or encouraging genocide or crimes against humanity are all offenses that carry a maximum sentence of five years in jail, a fine of N10,000,000.00, or both [30].

i. **Importation and Use of E-Tools [31]:** Using computers, devices, or passwords to conduct crimes is punishable by a fine of N5,000,000.00 to N10,000,000.00 or two to seven years in prison.

j. **ATM/POS Manipulation [32]:** Interfering with an ATM or POS terminal is illegal and can result in a fine of N5,000,000.00, five years in prison, or both. Employees of financial institutions who commit such fraud risk seven years in prison without the possibility of a fine.

k. **Computer viruses, phishing, and spam [33]:** Are crimes that carry a maximum sentence of three years in prison, a N1,000,000.00 fine, or both.

l. **Fraud Associated with Electronic Cards [35]:** Fraud using bank cards carries a maximum sentence of seven years in jail, a N5,000,000.00 fine, or both. Card theft is punishable by up to three years in prison, a fine of N1,000,000.00, and accountability for the cost of the stolen items or money. Additionally, the Act [35] eliminates the requirement for an actus reus by making it illegal to possess forged, expired, or counterfeit cards, invoices, vouchers, or card numbers with the purpose to conduct fraud, even if the fraud is not actually committed.

m. **Fraudulent Devices, Emails, and Websites:** It is illegal to use any device, email, or fraudulent website to get a cardholder's information with the intention of defrauding them. The penalty is N1,000,000.00, three years in prison, or both [36].

Initiatives on National Security, Financial & Economic Crimes

a. National Security, terrorism and Critical national Infrastructure

The Act addresses national security issues like terrorism. Grave penalties are stated for offences relating to critical national information infrastructure, which results in grievous bodily harm to any person. Critical national infrastructure can mean air space, national elections, state buildings, airports etc.

If found guilty, an offender faces a maximum sentence of fifteen (15) years in jail without the possibility of a fine. If an offender is found guilty, they could be sentenced to life in prison if their acts cause the death of one or more people. Additionally, anyone who wilfully gains unauthorized access to a computer system or network for fraudulent purposes, obtains information that is important to national security, or interferes with a computer system by entering, sending, destroying, erasing, deteriorating, changing, or suppressing computer data in a way that stops the system from functioning as intended will face consequences. These offenses include cyberwarfare, purposeful misdirection of electronic messages to fraudulently obtain financial gain or obstruct processes, which delays, accelerates, or defeats the messages' intended purpose, and unauthorized destruction or hacking of emails containing sensitive information, including financial information.

People who purposefully or unlawfully cause another person to lose property by erasing, changing, or suppressing computer data in order to obtain financial gain for themselves or another person are also subject to punishment.

b. Workers in the Public and Private Sectors

Anyone working in the public or private sectors who tampers with computer or electronic systems with the

intention of defrauding others—for example, by underpaying or overpaying workers—is subject to legal consequences. Unlawful withdrawals from public sector employees' salary and other benefits are a common occurrence in Nigeria.

c. Financial Institution Workers

Safeguarding Financial Institutions and the Stock Market Employees of financial institutions are also forbidden under the Act from rerouting emails with the intention of committing fraud. An employee who violates this rule faces a maximum sentence of seven (7) years in jail and must return any money that was stolen or forfeit any property that was acquired in this way to the financial institution or the impacted client. Any cooperation between the employee and outside parties that leads to fraud against the financial institution or its clients is subject to liability. This clause particularly addresses circumstances in which an employee gives cybercriminals information that permits fraudulent activity. In order to support this, the Act requires workers in both the public and commercial sectors to give up all access credentials and privileges to their employer as soon as they are let go.

Obligation to Report Cyberattacks Under the Law

Operators of computer systems or networks are required by law to notify the National Computer Emergency Response Team Coordination Center of any attack that compromises system or network functionality so that corrective action can be taken. If such assaults are not reported within seven (7) days, the operator may be denied access to the internet and face a punishment of N3,000,000 that must be paid into the National Cyber Security Fund. In addition to this reporting obligation, all communication service providers must cooperate with Act-related processes and supply information that law enforcement agencies request. According to Section 21 (1), neglecting to disclose cyber thefts, intrusions, or disturbances is a crime that carries a statutory N2,000,000 punishment that must be paid into the National Cyber Security Fund. According to Section 21(3), an individual or organization that does not notify the National Computer Emergency Response Team (CERT) of such incidents within seven (7) days is in violation of the law, faces denial of internet access, and must also pay a mandatory fine of N2,000,000 into the National Cyber Security Fund.

Problems with Jurisdiction

Section 50(1) gives the Federal High Court sole authority to decide cases involving violations of the Act that are committed inside Nigeria, on ships or airplanes registered in Nigeria, or even outside of Nigeria. This jurisdiction is in addition to other cases that are covered by other statutes and other cases that the Federal High Court is legally assigned to handle. A judge may, upon ex parte application, provide law enforcement authorities the authority to make arrests, conduct searches, and seize property in order to gather electronic evidence that is essential to an investigation. The Act acknowledges that many cyber services can obfuscate a user's IP address by routing traffic through various channels, sometimes for a fee, making criminal identification more difficult, and it offers complex procedures for arrest, seizure, and prosecution. Law enforcement frequently needs to identify the source of an electronic threat or robbery in order to track down cybercriminals. This process can be quite complicated and may require international cooperation because of the anonymity provided by the digital age, particularly when communications are routed through many nations. Delays like this raise the possibility that critical information would be lost or unavailable, enabling criminals to carry out their illegal actions.

Framework for Administration of the 2015 Cybercrime Act

1. The President: Protection of National Security

Computer systems, networks, programs, data, and traffic data may be designated as essential to national security by the President, based on the National Security Adviser's (NSA) recommendations. Nigeria's national and economic security, as well as the public's health and safety, might be severely impacted by any incapacitation, destruction, or tampering with these systems.

2. Council for Computer Professionals' Registration

According to the Act, all operators of cybercafés must register with the Corporate Affairs Commission and the Computer Professionals' Registration Council. In order to discourage illegal activity, operators must keep a user registry. Council members must have finished the National Youth Service Corps program, which suggests that they are postsecondary graduates. Cybercafés are subject to monitoring duties by the Council, which also has the authority to set operational rules for them.

3. The Office of the National Security Adviser's duties

The NSA's mission is to collect intelligence on the country's capabilities, the intentions of its enemies, and sensitive material. In accordance with the National Security Agencies Act, the office assists and organizes security and law enforcement organizations in their fight against cybercrime. Overseen by the NSA are two important:

1. The National Computer Emergency Response Team (CERT) Coordination Center is in charge of keeping an eye on and handling cyber occurrences across the country.
2. The National Computer Forensic Laboratory helps law enforcement and security organizations with their investigations.

A significant weakness in the Draft African Union Convention on Cybersecurity was the absence of a regional Computer Emergency Response Team, which is addressed by the creation of CERT. The NSA is designated as the coordinating organization for all security and enforcement agencies under the Act in Section 41(1) of the Act. Developing and implementing a comprehensive National Cyber Security Policy; establishing and maintaining CERT and the National Computer Forensic Laboratory; building capacity in pertinent security agencies; facilitating public-private partnerships in cybersecurity; and coordinating Nigeria's participation in international cybersecurity cooperation are some of the responsibilities. The NSA maintains a round-the-clock contact point for prompt international collaboration and makes sure law enforcement and intelligence agencies build institutional capacity, including national and international training programs. The Attorney General of the Federation must

approve the appropriate agencies' prosecutorial authority under Section 47, especially for offenses involving failure to notify cyberthreats to CERT, which could postpone prosecutions under Sections 19 and 21.

Advisory Council on Cybercrimes

The Act creates the Cybercrime Advisory Council, which is led by the NSA and consists of representatives from several departments and agencies. The council meets at least four times a year, and notice in the Federal Gazette may be used to increase the number of members. Facilitating cybersecurity knowledge and intelligence exchange; advising on the Act's implementation; encouraging graduate internships in cybersecurity; supporting computer and network security research and development; and awarding grants to higher education institutions to further ICT and cybersecurity research are some of the functions.

The Federation's Attorney General

By guaranteeing adherence to regional and international standards, upholding international cooperation, prosecuting offenses, and requesting mutual help from foreign authorities for investigations, the Attorney-General is entrusted with enhancing the Act's legal framework. In order to promote reciprocity in international collaboration, the AG may, even in the absence of formal agreements, order the return of forfeited property to foreign states.

Fund for National Cybersecurity

A 0.005% fee on all electronic transactions by organizations specified in the second schedule of the Act, such as GSM and telecom companies, ISPs, banks, financial institutions, insurance companies, and the Nigerian Stock Exchange, finances the Fund, which is based at the Central Bank of Nigeria.

Prosecutorial Difficulties

1. Acceptability of Electronic Proof

The admission of electronic evidence in cybercrime proceedings is not entirely covered under the Evidence Act of 2011. Direct oral testimony is required by Sections 126 and 127, which oblige witnesses or victims—including those who are overseas—to testify in Nigeria. Because cybercrime is transnational, this is expensive and demoralizing. This problem might be lessened via video conferencing.

2. Knowledge Gaps in Technology

To properly handle electronic evidence, investigators, prosecutors, and judges need sophisticated ICT abilities, computer forensic training, and technical infrastructure. Traditional ideas of possession and evidential appraisal are complicated by the novelty of email technology.

3. Cooperation Among Agencies

The EFCC's role in prosecution is impacted by bureaucracy, which frequently impedes collaboration between law enforcement, intelligence, and security organizations.

4. Inaccurately Obtained Proof

Judges have the authority to remove evidence that was obtained inappropriately under Section 15 of the Evidence Act of 2011. The Cybercrime Act ensures that investigations are not hampered by procedural formalities by requiring that such evidence be allowed unless its undesirableness outweighs its probative value, given the hazards associated with cybercrime.

Recommendations

1. To help people and organizations protect themselves, public awareness programs on self-defense, training, and identifying possible cyber exposures should be put into place.
2. To safeguard computer systems, government and business IT teams must constantly create and update thorough policies.
3. Nigeria ought to harmonize its domestic cyber regulations with global norms and best practices.
4. Mandatory information communication technology (ICT) training programs ought to be implemented by public secondary schools and local government councils.
5. To improve national cybersecurity, the offices of the Attorney-General of the Federation and the National Security Adviser, working with other stakeholders, should keep up with the latest developments in technology and security.
6. In order to solve the issues raised by e-commerce and the larger digital economy, Nigeria would benefit from using the strategy outlined in the American Anti-Cyber Squatting Consumer Protection Act (ACCPA), 1999.
7. To regulate domain name registration, a National Commission ought to be set up. The Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit organization founded in 1998 to oversee the worldwide domain name system (DNS), is currently in charge of this. Legitimate commercial interests will be verified and domain name availability would be properly monitored by a Nigerian commission.
8. Proactively acquiring technological, analytical, and legal skills in cybersecurity is imperative for the judiciary. It must uphold its independence, stop investigative abuses, enhance law enforcement education, and retrain staff members in information technology.
9. Children should get instruction on acceptable computer use and the repercussions of infractions. More secure authentication techniques, including biometric systems, should be used in place of or in addition to passwords.
10. To protect computer systems, people and organizations should use strong network security architectures, encryption, data protection techniques, and follow accepted information security guidelines.
11. To limit the use of offensive cyber technologies and create effective cyber arms-control frameworks, a global conversation is required.
12. Following the U.S. model, Nigeria should establish specialized investigation and prosecuting capabilities at the federal and state levels. Working closely with Assistant U.S. Attorneys through the "Computer and Telecommunication Coordination" program, the Department of Justice's Criminal Division Computer Crimes and Intellectual Property Section (CCIPS) is at the forefront of cybercrime prosecution in the United States. The FBI maintains almost 200 agents in field offices devoted to computer crimes, while the CCIPS employs about 100 investigative computer scientists

and analysts. In London, Ottawa, and Canberra, the FBI Cyber Division has also hired Cyber Assistant Legal Attaches.

Conclusion

Even if a computer isn't used directly to commit a crime, it might nevertheless yield important evidence since it might have records that are essential to an investigation. Cyberspace must be acknowledged as a realm where governments, businesses, and individuals can exercise influence and power, and networks must be protected. Governments, business boards, and other stakeholders must proactively identify and mitigate cyber threats in order to achieve effective cybersecurity.

Cyberspace is not just a place where governments operate. Since the majority of computer networks are privately held, cooperation with commercial organizations—such as technology corporations, defense contractors, financial institutions, and communication companies is necessary for their management and protection.

Every year, businesses and individuals throughout the world spend about $67 billion to safeguard their networks. Because cyberspace capabilities may be a source of both opportunity and vulnerability, decisions made by governments and corporate leaders have a big impact on the entire world. Cybersecurity flaws could endanger national security by compromising political influence, power structures, and the integrity of national boundaries.

References

1. Shane Harris, The rise of Cyber warfare, Publishing group 2014 P.3.
2. Shikha Singh: Cyber Laws, Global India Publications PVT Ltd, 2011. P.553S
3. The Rise of Law in Cyber Space (Standard law Review) (1996) 1367 1402 P.16.
4. Michael Benedikt. Cyber space First Step (1991) MIT-Press, P. 3.
5. Nazli Choucri, Cyber Politics in International Relations MIT Press, Cambridge, Massachusetts, London. England, 2012, 14.
6. Flavia Fascendini, "Small Thoughts Around Cybercrime and Legislation and gender" Gender centered thematic bulletin, 11. <http://www.genderit.org/newsletter/cybercrime-legislations-and-gender>accessed on 4 February 2023
7. Ibid
8. This Act amended the Wiretap Act and was intended by Congress to afford piracy protection to electronic communication
9. The Act was created to put a stop to trade secret misappropriation. Also, the Digital Millennium Copy Right Act, 1998
10. This law amended ITAD and added the offence of aggravated identity theft by additional two-year terms of imprisonment for identity theft in connection with particular federal violations
11. Cyber Security Enhancement Act (CSEA) 2002.This Act set the rules for commercial email. It establishes requirements for commercial messages, bans false or misleading email header information and prohibits deceptive subject lines, gives recipients the right to be removed from the mailing lists and provides tough penalties for violation.
12. Shane Harris, P. 213
13. Shane Harris, The Rise of Cyber warfare, Publishing Group 2014, P.47.
14. Confront and conceal, David Sanger of the New York Times, June 1, 2012
15. Financial losses due to cyber-crimes in Nigeria alone in 2016 were estimated at N 12bn (One hundred and twenty-seven billion naira) by Maj. Gen Babagana munguno (rtd) at the inauguration of the Cybercrime Advisory council, see This Day Newspapers of 13th January, 2017. Companies and Individuals spend about $67bn annually to protect their computers and networks. See Shane Harris, P. 24
16. EU's General Data Protection (GDPR) and, the EU-US Privacy Shield, and other national laws have been promulgated.
17. WIPO Arbitration & Mediation Centre, Administrative panel, France, under de ICAAN Uniform Domain Name Dispute Resolution Policy, Case no.: D 2000-0430. S. 25(I)
18. S.1 of the Advanced Fee Fraud and Other Related Offences Act, 2006.
19. S. 13.
20. Ibid
21. S.18(1).
22. S.23(1)(a).
23. S.23(1)(b).
24. S.23(1)(c).
25. S.23(1)(d).
26. S.23(1)(e).
27. S.23(3)(a).
28. S.23(3)(c).
29. S.26.
30. South Africans recently published xenophobic materials against Nigerians.
31. S.27.
32. S.28.
33. S.30.
34. S.32.
35. S.33(9).
36. S. 36