Al-Hikmat: A Journal of Philosophy
Volume 44 (2024) pp 1-19

Cybercrime as a Dehumanising Phenomenon in the Twenty-First Century in the Nigerian Context: A Philosophical Discourse

Olufunso Olubanjo-Olufowobi
Lecturer, Department of Philosophy and Religion,
Mountain Top University, Prayer City, Ogun State, Nigeria
E-mail: *ooolufowobi@mtu.edu.ng*

Babajide Olugbenga Dasaolu
Professor, Department of Philosophy
Olabisi Onabanjo University, Ogun State, Nigeria
E-mail: *dasaolu.babajide@oouagoiwoye.edu.ng*

Adebayo Ayokunle Aina
Professor, Department of Philosophy
Olabisi Onabanjo University, Ogun State, Nigeria
E-mail: *adebayoaina@oouagoiwoye.edu.ng*

Abstract

Dehumanisation means to disinherit human qualities of a person or group of persons, such as compassion, respect, individuality, and empathy. It is an aggressive behaviour which offends people's dignity. Dehumanisation is often considered a phenomenon associated with conflict and war. However, prominent twenty-first-century cases of robbery, rape, abduction, human trafficking, and particularly, the atrocities that take place in cyberspace through digital technologies have suggested otherwise. The inventions of digital technologies have brought remarkable progress in human society in numerous ways, ranging from education, entertainment, information, business and commerce. Along with these rewards, however, digital technologies bring a diverse range of risks and harms to individuals, institutions and states. In Nigeria, some unscrupulous people are using digital technologies for their sinister acts. A significant and growing threat of digital technologies to humanity is cybercrime. This research through critical analysis and expository methods investigates the dehumanising impact of cybercrime on individuals, businesses, and the country at large.

Keywords: cybercrime, dehumanisation, digital technologies, Nigeria.

Introduction

One eminent category people belong to, irrespective of their divergent differences in gender, race, colour, culture, nationality, religion, or social status, is ‘human’. To disregard the humanity of others is to dehumanise them. Dehumanisation is the abuse of human dignity, a cruelty against the worth and well-being of an individual. According to Immanuel Kant (1724-1804), dehumanisation is treating rational, autonomous agents as mere instruments for one’s ends. Kant holds that human nature demands respect since it allows individuals to determine their own goals in conformity with morality. Every human being should be treated as an end, not as just a tool (Manninen 2018). Human dignity is then the status that gives people the right to be treated with respect; a status that presupposes them for value because they are the only ones to whom value makes meaning. The concept of dehumanisation has often been associated with conflict (particularly, intergroup conflict) slavery, colonialism, genocide, massacre, racism and war. But prominent twenty-first-century cases of murder, rape, abduction, human trafficking, child molestation, hate speeches, discrimination-based on gender, religion, education, affluence-and especially, the enormities that take place in cyberspace facilitated by digital technologies have suggested otherwise.

Digital technologies provide innovative and sophisticated means by which conventional and novel crimes can be committed. Of significant and growing threat of digital technologies to humanity is cybercrime. Corroborating this, Ho and Luong (2022) state that the phrase cybercrime is generally accepted to include both conventional misconducts that are aided or intensified via the usage of Information and Communication Technologies (ICT) as well as new categories of crimes that have evolved with the introduction of ICT. Cybercrime creates a vicious state of affairs that allows for aggressive behaviours which offend people's dignity. With it, people are prone to hatred, cruelty, fraud and fraudulent acts, privacy violations, dubious relationships, psychological and mental abuses. It creates huge security, economic, psychological and mental health threats to individuals, organisations, and government, particularly in Nigeria.

Investigating critically into the challenge of cybercrime and its effects on individuals, businesses and the nation as the problem of dehumanisation constitute the crux of the work. It employs critical analysis – a qualitative data collection method which allows the researcher to provide a systematic clarity of the meaning of cybercrime thereby avoiding conceptual ambiguities. The expository method is used in bringing forth the dehumanising effects of cybercrime. To this end, the section after the introduction explores scrupulously the various definitions of cybercrime to provide a better understanding of the term. The section "Cybercrime as a dehumanising phenomenon and its effects" provides a detailed exploration of the dehumanising impact of cybercrime on individuals, businesses and the nation at large. Finally, the measures that could be taken to combat cybercrime at the individual, organisation and national levels are proffered.

Cybercrime: The Problem of Definitions

The term cybercrime originates in the advancements recorded in the Information and Communication (ICT) sector and the growing prevalence of digital technology usage in society. As people currently hinge on digital technologies for everything and every feasible human activity is made possible through the Internet and computers, crooks are also taking advantage of this to perpetrate their ominous acts making cybercrime a serious problem. Bolstering this, Phillips *et al.* (2022) aver that "digital technology and cybercrime are pervasive features of modern life. Approximately 60% of the world's population are internet users and the global adoption of digital technology is rapidly increasing; global internet penetration increased by approximately 7% over one year (from January 2020 to January 2021)". They opined further that the "increased adoption of digital technology has caused an evolution in criminal behaviour, resulting in the increased occurrence of 'cybercrime"'.

The theft of information, money, or other goods over the Internet mainly for financial gain and security harm is what is commonly referred to as cybercrime. However, there are divergent views on what cybercrime is or what constitutes cybercrime as there is no consensus on the meaning of cybercrime. In other words, there is no univocal definition of what is and what is not cybercrime. The diverse lexicon under which cybercrime is explained depicts its numerous conceptions. Such synonyms include but are not limited to technology-enable crime, virtual crime, e-crime, digital crime, computer-aided crime, electronic crime, technology-facilitated abuse, net crime, information technology crime, internet crime, internet fraud, crime by computer, computer-related crime, high-tech crime, information age crime, cyberspace crime, cyber-attack, and online fraud.

Cybercrime is from two distinctive terms: 'cyber' and 'crime'. The word "cyber" is derived from "cybernetics," a term used to describe the field of communication science that focuses on studying mechanicalelectrical communication systems and automated control systems (Olivia 2022). The term characterises interactions involving or relating to computers or networks. The term "crime" refers to particular negligent acts or inactions that are detrimental to the welfare or morality of the public and are thus illegal. The term “crime” in cybercrime primarily means a harmful or malicious act that should be considered unlawful; it should be considered unlawful because it is harmful with or without any specific law prohibiting it. Bolstering this view, Wall (2008) argues that the phrase denotes essentially the prevalence of hazardous computer-related behaviour, without any explicit reference in law. In most cases, these hazardous computer-related behaviours are called cybercrimes before the emergency of law prohibiting them.

Also known as computer fraud, cybercrime is the act of using a computer and the internet to take or alter electronic data, or to gain unlawful use of a computer or system. It is a distinct form of misconduct, in that, it is not limited to any geographical boundary and involves unknown perpetrators. It encompasses illegal activities facilitated by digital technologies, i.e. computers and network facilities. It involves the spread of illegal information, images, or other materials or malware against devices, computers or entire networks to either damage or disable them. Hence, Aghatise (2006) defines cybercrime as criminal activities carried out using electronic devices (computers), the communication network (internet), and data with the sole purpose of extorting valuables from victims, once a vulnerability is exploited. Jahankhani *et al.* (2014) buttress this view when they argue that “computer crime occurs as a result of criminals perceiving opportunities to infiltrate computer systems to achieve criminal ends or to use computers as instruments of crime, betting that the 'guardians' lack the means or knowledge to prevent or detect criminal acts”. It entails, among other things, actions targeted against the confidentiality, integrity, and availability of computer system networks and data.

Halder and Jaishankar (2011) consider cybercrime as an offence, with a criminal motive, committed against a person or group of persons to harm the reputation of the targets as well as cause irreparable damage to the hardware of sensitive infrastructure, including the internet and mobile phones. According to Theohary and Finklea (2015), cybercrime is any crime done with the aid of a network, computer, or hardware device. Tavani (2016) provides an unambiguous definition of cybercrime when he defines it as a crime in which the illegal act is carried out only through the usage of cyber technology within the cyber realms

The United States, one of the signatories to the Council of Europe Convention on Cybercrime, defines cybercrime as a wide variety of destructive acts, such as the unlawful interception of data, system interferences that jeopardise network integrity and availability, and copyright violations. According to the Department of Justice (DOJ) of the United States, cybercrime is categorised into three groups: 1) crimes where the computer is the target, such as when trying to enter a network; 2) crimes where the computer is a weapon, such as when launching a Denial-of-Service (DoS) assault, and 3) crimes in which the use of a computer serves as an accessory, such as the storage of illicitly obtained data (Brush *et al*., 2023).

According to Dennis (2023), cybercrime — also referred to as computer crime —is the use of a computer to advance illicit activities like fraud, the trafficking of child pornography and other intellectual property, identity theft, and privacy abuses. In the words of Neumann (2009), cybercrime is the unauthorised use, access, modification, or destruction of hardware, software, data, or network resources; the unauthorised disclosure of information; the unauthorised copying of software; the denial of an end user's access to his or her hardware, software, data, or network resources; and the use of or agreement to use computer resources to obtain information or physical property illegally.

Hacking, the dissemination of illegal electronic information, privacy violations, the use of false digital signatures, system interference, unauthorised access, illegal interception, and the unauthorised use of a device for fraudulent acts are all examples of cybercrime. It also includes breaking into computers to steal or destroy information, or to damage the computer source code.

Cybercrime is characterised as any unlawful act with the computer or internet as a subject (tool) or object (target) of the crime or both. The computer might be seen as the instrument rather than the target of cybercrime when a person is the main aim. In this case, the harm done manifests in the actual world. Human shortcomings are usually exploited as these crimes characteristically require less technological competence compared to when a computer is the target. Legal action against the crime when an individual is the target, is more challenging because the harm is primarily psychological which is intangible. When the computer is the main target of cybercrime, the crime is committed by a selected group of criminals. Contrary to crimes committed with a computer as a tool, these crimes call for technical expertise from the criminals. By and large, cybercrime can be defined as any misconduct or hazardous act where networked computers are either the sources, tools, or places of crime.

Cybercrime as a Dehumanising Phenomenon

Cybercrime of various forms known generally as yahoo-yahoo, yahoo-plus, or hustlers' kingdom in Nigerian's parlance are dehumanising phenomena through which victims are deceived about the real intent of the "other party". Their humanity is abused, degraded, demeaned, deprecated, and manipulated as mere things. Contrary to their will, they are employed by fraudsters as a way of achieving their (fraudsters) objectives causing harm in quantum. In other words, cybercrime allows for aggressive behaviour which offends people's dignity. With it, people, companies and Nigeria as a nation are used as mere tools or instruments for the attainment of crooks' inconsiderate goals.

Cybercrime affects every person and equally every sector of the nation. In light of this, it is accurate to state that everyone is vulnerable to cybercrime as long as they own a mobile phone, bank account, or important computer files, and are listed in any direct marketing database. Such effects range from psychological and emotional traumas to physical injury, privacy infringement, and financial loss for individuals. While for corporations, such can include financial loss, reputational harm, and legal implications. Cybercrime also has far-reaching disastrous effects on society, including adverse economic effects, national security challenges, reputational harm and a rise in cyberbullying and harassment.

On Individuals

Cyberspace criminals (as cybercriminals are also called) attack individuals ferociously through e-mail bombing/spoofing, pornography, identity theft, hacking, advanced fee scams, deepfake cyber harassment, spamming, Automated Teller Machine (ATM) fraud, piracy, and phishing, *etc*. A few of the effects of cybercrime as a dehumanising phenomenon on individuals include the following.

Psychological and Emotional Impact of Cybercrime

The psychological damages caused by cybercrime though different in the degree among victims, are typically severe and long-lasting. These emotional traumas experienced by victims of cybercrime often result from a sense of violation and include loss of trust, shell-shock, blaming oneself for not being vigilant enough, anxiety, secondary victimisation, reduced self-esteem and self-confidence, depressive symptoms, the feeling of helplessness, incompetence, and humiliation, fear and perceived risk, and loss of autonomy and control. The emotional stress that stems from stolen data or loss of money, for instance, leaves one to worry. Such worry does not only give rise to anger, depression, headaches, eating and sleep disorders but the victim can also experience Post Traumatic Stress Disorder (PTSD).

In many cybercrime incidents, victims might not report the incident but instead blame themselves for their weak cyber security. Such could result in shame, guilt, and, or suicide tendencies. The feeling of helplessness may creep in when a victim who expected the judicial system to bring cybercriminals to justice is disillusioned and is unable to obtain such justice. Such feelings may force the victim to retreat socially and become isolated to avoid becoming a victim of other digital crimes. The feeling of helplessness may also be a result of being previously a victim of cybercrime. Lack of social support may aggravate victims' distress when instead of receiving sympathy, they experience resentment and blame from family and friends organisations, or society in general for falling prey to the scam. The emotional traumas are further worsened by numerous psychosocial losses related to employment, family and, or relationships. For instance, loss of employment, as in the case of someone who accidentally typed the organisational banking details into a fake online form (thinking the instruction was from their boss) or in an e-mail to someone masquerading as a vendor.

Many sleep issues, including insomnia, are connected to stress. Being a victim of cybercrime might cause insomnia and nightmares owing to anxiety about the situation. This lack of sleep is caused by increased levels of the stress hormones cortisol and adrenaline (Suni & Dimitriu 2024).In a bid to manage the stress experienced from cybercrimes, victims tend to turn to negative coping strategies such as alcoholism, substance abuse, and social evading. Such victims could take to binge eating as a coping strategy for online fraud. People sometimes use "emotional eating" as a coping mechanism for unpleasant feelings including stress, rage, fear, grief, and loneliness caused by cybercrime. This circumstance frequently leads people to consume foods heavy in fat, sugar, or calories, which contributes to obesity.

Breaches of Privacy and Confidentiality

With the disclosure of private communications, photographs, videos, audio recordings, and other personal information without the knowledge or agreement of the target through hacking, malware, identity theft, financial fraud, medical fraud, and other means, cybercrime compromises people's privacy and data security. Violating someone's right to privacy and confidentiality can be harmful in addition to affecting their dignity. Medical fraud and the theft of private patient data can also have serious consequences on an individual's health, even leading to death.

Reputational Harm

The loss of credibility and trust can result from cybercriminals posting humiliating or harmful things online using stolen information. In career contexts, the impacts of reputational damage can be very harmful, resulting in job loss or difficulty in securing a profitable job.

Cyber Harassment

E-mail harassment, cyberstalking, the spread of pornographic content, defamation, indecent exposure, e-mail spoofing, and cyber fraud are common forms of harassment people experience through cybercrime. In addition to intellectual property theft, illicit access to their computer systems, viruses being introduced into their systems, and vandalism, they might also experience unauthorised control or access to their properties (Lamidi 2020).

Financial Loss/Economic Hardship

Financial Loss/Economic Hardship is one of the most significant consequences of cybercrime on individuals as they lose all their life savings in a jiffy. Individuals' bank information is a frequent target by cybercriminals, who employ a variety of ways, including phishing, hacking, and ATM fraud, to acquire access to an individual's financial information, such as credit card numbers, bank account data, and passwords. The stealing of intellectual property and sensitive data of an individual could also have adverse financial implications on such. Corroborating this, (Khatri 2023) avers that “victims often find themselves facing drained bank accounts, unauthorised purchases, or even complete identity theft, leading to prolonged financial distress and difficulties in reclaiming their financial stability.”

Technophobia

Technophobia, also known as cyberphobia, refers to the extreme or irrational fear of computers or technology. This phenomenon is exacerbated by the rising threat of cybercrime. As cyber-attacks become increasingly sophisticated, more people develop technophobia or cyberphobia, leading to a growing reluctance to adopt and utilise digital technologies

In Nigeria, this fear is particularly pronounced, with many individuals avoiding the use of Information and Communication Technologies (ICTs), such as online banking applications, due to concerns about falling victim to cybercrime. This lack of confidence not only hampers their ability to fully benefit from the digital world but also prevents them from leveraging new technologies and participating in online activities. Ultimately, this has a negative impact on the well-being of citizens.

Loss of Productivity and Opportunity

People may find themselves unable to access vital systems due to ransomware or denial-of-service attacks, which can cause disruptions to everyday routines and lower productivity. In both personal and professional endeavours, this may result in losing possible opportunities, monetary losses, and setbacks (Khatri 2023).

On Businesses

While larger businesses with a strong internet presence used to be the only ones targeted by cybercriminals, this has changed in recent years. Because they are aware that small as well as medium-scale companies typically have less robust security architecture stemming from ignorance, lack of funds, or nonchalance about digital safety. A lot of cybercriminals are now shifting their focus to target these kinds of companies. Nobody is protected as a result; although larger corporations continue to be the focus of intense attacks, smaller businesses, and even mid-size organisations are equally vulnerable.

This was validated when Akintaro (2022) reported that cybercriminals hit 71% of Nigerian businesses surveyed by Sophos, a Global cybersecurity firm with ransomware in 2021. Cyber-attacks against corporations and government agencies come in the form of hacking, online recruiting scams, identity theft, malicious software attacks, phishing, website cloning, cyber defamation, *etc*. Some of the effects of cybercrime as a dehumanising phenomenon on businesses include the following:

Financial Harm

The devastating financial effects of cybercrime are especially dangerous for small and medium-sized businesses. Successful cybercrime may result in financial loss, intellectual property theft, or the loss of customer data, and their recovery may be costly. Occasionally, businesses may be forced to close due to the financial toll that cybercrime takes.

Increased Costs

Businesses invest a lot of money in protecting their systems from online fraud. They spend money on a variety of things, such as public relations support, insurance premiums, cyber security technology, and expertise, and notifying affected parties of a breach. All these decrease profit margins while raising overhead costs.

Furthermore, to stay in compliance with cybersecurity requirements, firms might need to engage solicitors and other professionals. If they become the target of a crime act, they would have to pay much more for legal expenses and other costs associated with filing civil lawsuits against the criminal(s) and/or defending a lawsuit against the organisation if significant customer's or client's data is compromised as an individual has every right to suit a business organisation if their data is compromised. Every company that faces these legal challenges bears heavy costs. In the event of a security breach of any type, the corporation may suffer hitherto unparalleled and unrewarded damages in defending itself in court (Investopedia 2023) or as a penalty, if a customer loses their important information or suffers some financial loss because of the cyber-attack on the company.

Once more, malware may be extremely costly for an organisation. Malware and distributed denial-of-service (DDoS) may track an organisation's operations for a long period making the corporation inept to provide its services to customers at this time. The corporation suffers significant losses as a result of this denial of service, both directly and indirectly. To cause a denial of service, one can employ spam attacks, viruses, or flood the company's server with requests for services, which can slow down servers or force computer systems to shut down entirely. Malware can also be in the form of ransomware restricting employees from using IT systems until the hacker is paid off. The ransomware which usually sneaks into a system, installs itself on the system and encrypts all databases and files, demanding a ransom to unlock the contents. The ransom usually results in significant direct money losses for the company as well as a sense of anxiety and uncertainty for employees. Therefore, protecting against cybercrime is an extremely costly endeavour.

Loss of Data and Intellectual Property

Cybercrime may result in data theft by a competitor firm following espionage. This implies that the firm is no longer in possession of its crucial data. Yet an organisation invests a huge amount of money in gathering, scrutinising, and applying data. The firm suffers a direct financial loss as soon as the information is taken. Furthermore, valuable contacts are lost, resulting in a decline in revenue from merchants and customers. Importantly, the seamless operation of a corporation is very impossible in the absence of precise data (Girdhar & Popli 2017).

The loss of intellectual property could have a severe negative impact on businesses whose competitiveness depends on research and innovation. It might affect the company's long-term viability if the outcomes are declining revenues, opportunities lost, and market share. Validating this claim, Oliva (2022) affirms that “an organisation can lose its competitive advantage and suffer losses when a hacker steals its confidential information and plans and sells it to a competitor."

Damage to Reputation

The reputation of a company may suffer irreparable harm as a result of cybercrime. A company's reputation that is developed over years of sound business procedures can be destroyed in an instant by a single cyber-attack. When clients experience financial losses on a business's website, they may be sceptical to patronise the company. The company's reputation is damaged in the eyes of vendors and customers even if the main page is vandalised for just a few hours. Cyber-attacks on companies have the potential to expose confidential customer information, eroding public confidence in their ability to protect customer and client information. Revenue and market share can decrease drastically due to losing dependable customers.

Legal Repercussions

Cybercrime could have a very detrimental legal effect on businesses. Particularly in industries with strict regulations, like healthcare and banking, data breaches may result in legal action, fines, and penalties.

On Nation

Cybercrimes have emerged as a major issue facing many countries in the world today and Nigeria is not left out. They are not limited to any geographic or political boundaries and are aggressively targeting government, military, and even critical infrastructures. Cyberterrorism, hate speech, hacking, child pornography, cyber drug trafficking, sextortion, catfishing, online gambling, and cyber espionage are some kinds of cyber-attack against the nation. The effects of cybercrime as a dehumanising phenomenon on Nigeria as a nation-state include but are not limited to the following:

Economic Impact

The economy suffers greatly as a result of cybercrime as it causes financial losses for people, companies, government, and government agencies. Repairing harmed systems, finding lost data, business disruption, profit reduction/rising operating and averting further attacks, etc. are part of the expenses incurred due to cybercrime. Consumer trust in online transactions may also be impacted, resulting in a decline in business sales and revenue. Cybercrime also leads to the theft of intellectual property, which has a detrimental impact on market innovation and competitiveness. All these affect the national economy and GDP. *Hence,* Morgan (2020), *asserts that* if cybercrime were considered a country, it would have the world's third-largest economy, trailing only the United States (US) and China. It undermines the incentives for innovation and investment and represents the leading transfer of financial resources on record.

Threat to National Security

National security may be seriously threatened by cybercrime as attacks on military and governmental networks have the potential to compromise sensitive data and interfere with operations (Cavelty 2019). It undermines national security in Nigeria through the stealing of State secrets, exposing individuals and corporations to online manipulations like cyber espionage, cyberstalking, hacking, deepfake, *etc*. Like other nations, Nigeria is powered by a network of linked systems called critical infrastructure, which serves as the mainstay of the nation. It includes commercial facilities, energy, financial services, communication networks, emergency response systems, food and agriculture, and essential services. In the words of Young (2024), an attack on critical infrastructure that is successful might have disastrous results. This is because, if sensitive patients' data is compromised, medical services interrupted or healthcare system is completely shut down, the transportation network is immobilised by ransomware, or a power infrastructure is completely blacked out, there will be significant financial loss, disruptions to normal activities, and fatalities. Such disruptions have the potential to affect economic stability, national security, and public safety, with difficult-to-quantify knock-on effects. Cybercrime can also be used for ideological and political reasons, which can cause social and political unrest. The threat of cybercrime to national security is exacerbated by the country's existing security challenges, including Boko Haram's insurgency, kidnapping, and armed robbery.

Increase in Harassment

Cybercriminals can use technology to target specific people or groups, disseminating harmful information and harassing messages. This may lead to psychological and emotional harm as well as harm to groups' reputations and interpersonal relationships. Thereby, damaging mental health and causing depression and anxiety. Cybercrime can also disseminate false information, which has negative social and political repercussions.

Social Media Manipulation

The use of social media platforms to persuade, mislead, or manipulate people or groups for political, financial, or personal gain is known as social media manipulation. There are many ways to do this, such as disseminating false information, fabricating personas or profiles, or amplifying messages with deepfake, bots or automated accounts. Such effects may be profound because they have the potential to compromise the legitimacy of democratic processes, foster the spread of extremist ideologies, and reduce public confidence in authorities and information sources.

Dehumanising through Coerced Grooming

In situations where children are the target of cybercriminals child pornography is beget. This happens mostly through coerced grooming. One of the most horrific and devastating crimes is child pornography; victimisation is unending since the photographs are uploaded to the Internet and can never be completely removed. Such images keep getting passed from one person to another. The victim's present and future may be impacted by this. Other crimes like sexual violence and addiction, sexism, objectification, *etc*. are also caused by it. It results in physical wounds, agony, infections spread by sexual activity, *etc*. Children who experience it may experience psychological effects such as suicidal thoughts, low self-esteem, anxiety, depression, anger, and other emotional and mental breakdowns. Given that children are a country's greatest asset, child pornography casts doubt on a country's future.

Pollution through Indecent Exposure

Another negative effect of cybercrime on society is cybersex trafficking through which Nigerians especially youths and teenagers are exposed to indecent pictures and images that pollute their minds. Through cybersex trafficking, people, particularly women, children (girl-child), and the impoverished are used as tools to meet miscreants' inordinate desires.

Cybersex trafficking, also known as online sexual exploitation, or cyber form of forced prostitution involves the transportation of victims followed by a live streaming of rape or coercive sexual acts on a webcam. The victim is deceived, hauled away, or threatened before being sent to "cybersex dens".

Their dens are usually positioned everywhere the cybersex traffickers have access to a phone, tablet, or computer with a webcam program and an internet connection. The perpetrators take advantage of dark web sites, apps, video conferencing, dating websites, online chat rooms, and other platforms to exhibit the sexual acts they coerced victims to perform on themselves or other people.

International Reputation Tainted

A recent survey of cybercrime experts assessing the top cybercrime-producing nations reports Nigeria as number one in the Scams index but comes between 5th and 10th in banking crimes, ransomware, intellectual property theft, and financial crimes (Lemos 2024). Reports like this present every citizen as a potential scammer, making it difficult for Nigerians to engage in any meaningful socio-economic relation with the rest of the world. The global reputation of the country is tainted, discourages foreign investment, and erodes trust in the digital economy as Nigerians are treated with suspiciousness in business dealings (Maitanmi, *et al*. 2013). Consequently, the honest majority of Nigerians suffer as a result, and the country's development is retarded.

The overall effect of cybercrime on a nation was averred by Abubakari (2021) when he submitted that in West Africa (and by implication Nigeria), cybercrime has a micro, meso, and macroeconomic impact. At the micro level, citizens lose out on financial resources as well as chances to travel abroad. The meso level of e-businesses suffers financially and reputation-wise. At the macro level, nations with high rates of cybercrime see a decline in foreign investment, harm to their reputation abroad, and financial difficulties.

Ways Forward

It is essential to have a comprehensive policy to protect people, companies, and countries against cybercrime. Sequel to the aforementioned effects of cybercrime on individuals, corporations, and Nigerian society, the researcher recommends the following

Roles of Individuals

(a) Individuals should be aware that weak passwords, inadequate privacy settings, phishing e-mails, and out-of-date security software are often ways cybercriminals access people's online accounts. The use of strong passwords that are difficult for a person or program to guess is recommended. The longest passwords are, the most secure; consisting of a combination of upper and lower case letters, figures, and symbols, as well as the absence of any dictionary terms or connections to personal data. (b) Using unique passwords for every account safeguards individuals in the case of a breach and helps deter cyber thieves from accessing these accounts. (c) Mobile devices and applications must be regularly updated to protect oneself.

(d) It is important to be wary of suspicious links, it is best to delete them immediately and block them to prevent subsequent messages. (e) Do not share personal information. Individuals must ensure they are the only ones having access to their accounts e.g. e-mail, banking, social media, and any other service that requires logging in. Similarly, they are advised to double their login protection by enabling multi-factor authentication (MFA). (f) Nigerians are cautioned against using free Wi-Fi networks as public Wi-Fi might endanger sensitive information. Never send important data—such as credit card numbers or other personal information—over an unencrypted Wi-Fi network since these networks are accessible to everyone, including cybercriminals. (g) Importantly, Nigerians must learn to respect the dignity of each other; they must treat one another as human beings.

Roles of Organisations

(a) Respect for human dignity (online and offline) must be prioritised by every organisation in Nigeria to reduce the menaces of dehumanisation b) Stringent technical measures should be religiously adhered to. Such include the following: (i) Operating systems, browsers, and all other system software need to be updated regularly for all corporate enterprises. (ii) To combat malware of any type, firewalls, antivirus software, and other intrusion detection prevention systems must be installed and updated constantly. (iii) Important data must undergo all necessary encryptions to better safeguard it. Passwords, filters, and other measures must also be used accordingly and consistently. (iv) Employees' administration authority should be tightly regulated and specified to prevent software from being installed without permission.

(v) Pen drives, memory cards, USB drives, solid-state drives, and other external memory devices must be used under strict guidelines. Workers must be prohibited from taking them to or from the workplace. Since it is not uncommon for an employee to be an invader, it should also be in the corporation's policy to screen all employees for external memory devices as they enter and exit the building.vi) It is necessary to block some websites that are discovered to be dangerous to prevent malicious material from entering the network of the company.

Roles of the Nigerian Government

(a)The government and those in authority must place premium emphasis on respect for human dignity both in cyberspace (online) and physically in society. b) Public awareness about cyber menaces should also be prioritised by the Nigerian government. c) Adequate trained manpower and effective legislation are required to combat cybercrime. (d) Regular training of law enforcement officers to keep them abreast of the dynamism of cyberspace is also imperative. e) Government investment in cybersecurity for critical infrastructure is imperative. By investing in cybersecurity, governments can build a more resilient and secure future for all.

Conclusion

Cybercrime is a dehumanising phenomenon that disregards human dignity, stripping victims of their emotions, thoughts, and inherent human characteristics while perpetrators are indifferent to their victims' plight. To combat this, rehumanisation is essential. When one uses or treats others as a means or a tool to achieve their selfish interest, such abuses humanity, the class to which they belong. Rehumanisation thus becomes crucial, as it involves acknowledging and respecting human dignity, and treating others as ends in themselves rather than means to achieve selfish interests. By prioritising respect for human dignity at every level, we can mitigate the devastating effects of cybercrime and foster a more empathetic and humane society.

References

Abubakari, Yushawu. 2021. "The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: A review." *PrzestrzeńSpołeczna* 1, no. 1/2021 (21).

Aghatise, E. J. 2006. "Cybercrime definition." *Computer Crime Research Centre. June* 28.

Akintaro, S. “71% of Nigerian businesses were hit by cyber attacks in 2021.” *Nairametrics*. (2022) AccessedMay 12, 2024from: https://nairametrics.com/2022/05/02/71-of-nigerian-businesses-were-hit-by-cyber-attacks-in-2021/

Brush, K.; Cobb, M. and Rosencrance, L. 2024. "Definition cybercrime." *TechTarget Editorial* (2021). Accessed April 25, 2024, from https://www.techtarget.com/searchsecurity/definition/cybercrime

Cavelty, Myriam Dunn. 2019. *National Security in the Digital Age.* Oxford shire: Routledge.

Christoff, Kalina. 2014. "Dehumanisation in organisational settings: Some scientific and ethical considerations." *Frontiers in human neuroscience* 8 (2014): 748.

Dennis, Michael A. “Cybercrime.”*Britannica.com*. 2023, June 16. Accessed May 12, 2024 from https://www.britannica.com/topic/cybercrime.

Finklea, Kristin M., and Theohary, Catherine A. 2015. "Cybercrime: Conceptual issues for Congress and US law enforcement." Washington: Congressional Research Service, Library of Congress, 2015.

Gabel, Stewart. 2021. *The Role of Dehumanisation in the Nazi Era in Activating the Death Drive Resulting in Genocide*. University of Denver, 2021. (Doctoral dissertation, University of Denver).

Girdhar, Anup, and Navneet Kaur Popli. 2017. "Harmful effects of cybercrime in business and economic sustainability." *ABS International Journal of Management, 5* no.1 (2017): 74-76.

Halder, Debarati, and KaruppannanJaishankar, 2011. Eds. *Cybercrime and the victimisation of women: Laws, rights and regulations: Laws, rights and regulations*. IGI Global.

Ho, HuongThi Ngoc, and HaiThanh Luong. 2022. "Research trends in cybercrime victimisation during 2010–2020: a bibliometric analysis." *SN Social Sciences* 2, no. 1 (2022): 4.

Investopedia.“6 Ways Cybercrime Impacts Business.”*Dotdash Meredith.* 2023, July 13. Accessed on May 3, 2024, from: https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx

Jahankhani, Hamid, Ameer Al-Nemrat, and Amin Hosseinian-Far. 2014. "Cybercrime classification and characteristics." In *Cybercrime and cyber terrorism investigator's handbook*, pp. 149-164. Syngress.

Khatri, Mousam. "How Cyber Attacks Affect Individuals: Understanding the Personal Impact of Digital Threats.*" Linkedin.com*. 2023, August 7. Retrieved May 3, 2024 from https://www.linkedin.com/pulse/how-cyber-attacks-affect-individuals-understanding-personal-khatri/

Lamidi, MufutauTemitayo. 2020. "Investigating Cybercrime in Nigeria." In *Encyclopaedia of Criminal Activities and the Deep Web*, pp. 1018-1033. IGI Global.

Lemos, Robert."Nigeria & Romania Ranked Among Top Cybercrime Havens.*"Dark Reading Global.*2024, April 18.Retrieved May 17, 2024, from https://www.darkreading.com/cybersecurity-analytics/nigeria-romania-ranked-among-top-cybercrime-havens

Lebech, Mette. 2004. "What is human dignity?" *Maynooth philosophical papers* ed. by M. Lebech, Maynooth (2004): 59-69.

Maitanmi, O., S. Ogunlere, S. Ayinde, and Y. Adekunle. 2013. "Impact of cybercrimes on the Nigerian economy." *The International Journal of Engineering and Science* 2, no. 4 (2013): 45-51.

Manninen, Bertha A. 2018. "Dehumanisation." *The Society of Philosophers in America (SOPHIA)* 3, no 2 (2018).

Neumann, Peter G. "Computer-related risk futures." In *2009 Annual Computer Security Applications Conference*, pp. 35-40. IEEE, 2009.

Olivia, Onwugbenu Ezinne. 2022. "Examining the effect of the elevated rate of cybercrime on the growth and sustainable development of Nigeria's economy." *Journal of Commercial and Property Law* 9, no. 1 (2022): 32-43.

Phillips, Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. 2022. "Conceptualising cybercrime: Definitions, typologies and taxonomies." *Forensic Sciences* 2, no. 2 (2022): 379-398.

Suni, Eric, and Alex Dimitriu. 2024. "What causes insomnia?" *Sleep Foundation* (2022). Accessed on May 12, 2024, from Sleepfoundation.org: https://www.sleepfoundation.org/insomnia/what-causes-insomnia

Tavani, Herman T. 2016. *Ethics and technology: Controversies, questions, and strategies for ethical computing*. John Wiley & Sons.

Wall, David S. 2008. "Cybercrime and the culture of fear: Social science fiction (s) and the production of knowledge about cybercrime." *Information, Communication & Society* 11, no. 6 (2008): 861-884.

Young, Destiny. 2024. "Critical Infrastructure Protection: Why the Nigerian Government Must Invest in Cybersecurity."*LinkedIn.com* 2024, February 25. Retrieved from https://www.linkedin.com/pulse/critical-infrastructure-protection-why-nigerian-government-young-cxp6f/