Cyber Crimes as Emerging Global Threats: Nigerian Context

Mohammed A.N.A. Imam (Ph.D.)
Department of Sociology, Yobe State,
University Damaturu, Nigeria
abusakin55@gmail.com

Goni Ibrahim Usman
M.Sc. Candidate, Department of Sociology, Federal University Dutes,
Jigawa State, Nigeria
gibrahimusman@gmail.com

DOI: 10.56201/ijssmr.v10.no5.2024.pg196.209

Abstract

Cyber crimes as emerging global threats across the globe. The paper aimed to examine the factors that derive individual to engage into the phenomenon of cyber crime as a global threat which has negative effect on populace of the world from internet arena. The emerging trend of cybercrimes have made various people vulnerable especially the internet navies due to the lack of cybercrime knowledge in the society. These emerging cyber threats are committed in on daily basis irrespective of gender, ages, youths and adolescent who are usually perpetrate so-called cybercrime phenomenon. This research depends upon secondary source or desk review data that will be generated via printed materials such as textbooks, book chapters, newspapers, magazines, journal articles, and periodicals, among others. The findings of the study revealed that the advent of social media such as WhatsApp, Facebook and Tweeter among others have dramatically become an analogy for unique forms of crime in the cyber space which are committed in daily basic. Also the porous nature of the internet give room for criminal minded from open society to cyber world to perpetrate any such of criminal behaviour in the cyber space. The study recommended that, the internet services (ISPs) should monitor suspicious activities of individual's online and alert relevant law enforcement authorities. Furthermore, the Interpol and other agencies that are responsible for combating cybercrime should censor the use of the social media platform in the global village which will enable to curb criminal minded individuals across the globe.

Keywords: *Cyber Crime, Cyber Defamation, Cyber Stalking, Cyber Hate Speech Cyber Bullying, Sextrusion*

Introduction

The growing of internet has dramatical change and reshaping the pattern and nature of human society from physical space to cyber space. Moreover, the cyber space is the connection of the internet through the use of auxiliary devices such as computer laptop, smart phones and tablet which connect people all over the world without consuming time and financial constraint. However, the Internet, with its infinite size and previously unimaginable capabilities that has negative dark side that opened windows to new form of crimes unknown as cybercrimes. Cybercrimes is a new phenomenon that not only challenge but also transcend all physical boundaries and limitations to detect, punish, and diminish an increasing threat all over the globe. Moreover, cybercrime refers to the use of computer technology to commit crime or engage in any activity that threatens a society's order and stability (Brenner (2007). Whilst the computer and its contents are the primary targets in computer crime, cybercrime is associated with the use of a computer or/and the internet to commit traditional crime (Ibrahim, 2016).

Cybercrime is an illegal act perpetrated with computer or devices and the Internet. It involves breaking, damaging and stealing of sensitive data, sharing of unsolicited sexually suggestive materials, harassment, sexploitation, downloading pirated contents and undermining national economies. In line with the above, Adesina (2017) described cybercrime as a term that encompasses all illegal activities committed by an individual or group of individuals referred to as scammers, hackers, internet fraudsters, cybercitizens or *419ners*, using the internet through the medium of networked computers, telephones, and other Information and Communication Technology (ICT) equipment. In Nigeria, people commonly refer cybercrime to as *Yahoo-Yahoo* (Adeta, 2014; Edward & Charles, 2017; Jaishankar, 2011; Olumoye, 2013). This is owing the fact that the emergence of online advance fee fraud (a variant of cybercrime) is associated with advent of Yahoo App in Nigeria (Trend Micro and INTERPOL, 2017). The common tools used for cybercriminals consist of smart phones, tablets and computer laptops to carry out their defamatory activities in cyberspace the purpose of this research is to investigate the emerging threats that cybercrimes pose as a global threat by examine the factors that derive individual to engage into this phenomenon.

Methodology

A survey research design adopted for this research, to analyse the emerging cybercrime as a global threat. However, this research depend upon secondary source or desk review data that generated via printed materials such as textbooks, book chapters, newspapers, magazines, journal articles, and periodicals, among others. The study also used some search engines like Google-scholar, academia.edu, Research Gate, etc. Primarily, the data collected were related to those for evaluating and identifying the cyber threats as a global phenomenon, and text Analysis method was used.

Literature Review

Factors Responsible for Cyber Crime

There are several factors that predispose people to cyber defamation. For the purpose of this study, the following factors are vividly explained.

Organised Criminal Interest: The internet had led to organised crime group that carried out cybercrime's acts. Cybercrime activities have been utilised through the use of internet for criminal purposes (Lavorgna, 2015). The internet offers an opportunity structure for decentralised, flexible networks of loosely organised criminals' partners in the distribution of work based on knowledge and skills (Leukfeldt, 2015). There are enough motivations for organised criminal groups to employ the internet architecture for criminal gains. One of such reasons is that the Internet guarantees them anonymity and drastically reduces their risk of doing "business," as their chances of apprehension are relatively low (Ndubueze, 2020).

Revolution in Information and Communication Technologies (ICTs)

The revolution in information and communication technologies (ICTs) has brought a lot of changes that occur in the world, which are aimed at enhancing the flow of information and the exchange of ideas across the globe via the use of technological devices among information seekers. The revolution of ICT has given room to all forms of cyberspace-related crime, such as cyber deformation, cyber stalking, cyber bullying among others. This has no doubt led to an incredible increase in the number of people that get connected to and utilise the internet and associated devices. The threats of social networks are becoming major alarms for the technology of the internet and its applications (Michael et al., 2014). The consequences that are associated with the technology have widely spread to cyber deviance, cybercrime, and cyber terrorism.

The availability and accessibility of the internet within the cyber environment allow motivated cyber offenders to detect their targets and attack them from anywhere in the world (Shabnam et al., 2016). Betancourt (2016) opined that the recent explosion in the availability of electronic communication technologies had provided students with a new medium to bully their peers. Although social networking sites have opened a wide range of windows for socialising youths and children, they have also opened floodgates for various crimes against them and the public (Halder & Jaishankar, 2016). The advent of social media like WhatsApp, Twitter, and Facebook gives room for cybercriminals to target their victims in society through the use of these applications in cyberspace.

Lack of cybercrime awareness among Internet users

Many internet users are not aware of threats that are facilitated through the use of the internet, such as cyber terrorism, cyber deviance, and cybercrime, they do not have adequate knowledge on the phenomenon as a result of inadequate awareness among the internet users who engage in criminal behaviours in society. With the availability of the internet and other auxiliary devices expose to defamatory acts, only a few people are complaining about this crime, which demonstrates that they lack awareness of participating in cybercrime (Whittaker & Button, 2020). Matlhare et al. (2020) found that many internet users are unaware of or have very little knowledge of cybercrime. Given the lack of awareness about cyber threats, social networking site users may not pay attention to security or privacy settings or measures that protect them against victimisation.

Ineffective Cyber Policing in Nigeria

The ineffective cyber-policing is viewed as an inefficiency of the government of Nigeria to protect the cyberspace and its users from all forms of attack from cyberspace who have the intent of cybercrimes. The growing threat of cybercrimes poses serious challenges for police organisations. They do not have adequate policing that will deter people from cybercrimes (Harkin et al., 2018). Nevertheless, the Nigerian law enforcement agencies that are responsible for policing cyberspace criminals. Hence, there is a need to improve cyber-policing among the public in Nigeria as a whole. Ibekwe et al. (2021) defined cyber security as the body of rules, technological tools, and guidelines put in place for the protection of cyberspace. Cyber policing tends to have unique challenges due to a lack of cyber competency and expertise among the cyber policers (Abdullahi & Jahan, 2020). Despite the rapid growth of cybercrimes in Nigeria, there are few laws to prevent the phenomenon of cybercrime, and this will gives away to increase such crimes.

Porous nature of the internet:

The Internet is free and open to all, allowing anyone to contact anyone else with no identity or passport needed (Tade & Aliyu, 2011). This openness makes communication between individuals and devices more easily. Cybercriminal used fake or hidden identity on the internet due to the porosity of cyberspace. In fact, anonymity has made the internet porous and set the stage for lack of deterrence factors in cyberspace and provide the offenders with the means to commit cybercrimes.

Cyber Defamation

Cyber defamation is a false statement of fact that is harmful to individuals or someone's reputation and is published with fault, meaning as a result of negligence or malice through the use of the internet. Cyber defamation, also known as online defamation or internet defamation, is a type of behaviour that defames someone's image, character, and reputation in society and occurs all over the world. The common tools used for defamation consist of smart phones, iPads, tablets, and computer laptops to carry out their defamatory activities in cyberspace whereas cyber defamation may not only occur in written words, it may also be portrayed by images or symbols of false profiles that may be used to defame someone's reputation in cyberspace. In other words, defamation is generally considered to be an intentional infringement of someone's right to his good

name or, more fully, an erroneous, deliberate publication of words or conduct concerning another person whose status, good name, or reputation is likely to be undermined (Saeh, 2012). Cyber defamation is considered to be the act of defaming, abusing, offending, or otherwise harming a person in cyberspace through false statements. Defamation can take the form of libel (printed defamation) or slander (spoken defamation). A defamatory statement may be in the form of words, pictures, visual images, gestures, or any other method that signifies a meaning. Defamation is insulting behaviour, which means that it is the act of attacking a good name or person. The targets of defamation can be classified according to the individual person: against groups or groups, against a religion, against the deceased, and against the officials of the state (Carlton, 2020).

Cyberstalking

Cyber stalking is another form of internet assisted crimes such as cyber bullying, harassment, unwanted sending of text message, fraudulent phone calls etc, intentionally provoke an emotional response through online comments or post, all of these crimes are unwanted and may cause fear or distress to internet users or internet naïve (Imam & Usman, 2020). Stalking actually predates internet revolution. This means, people were stalked even before the advent of the internet. It only becomes easy and common with the use of internet because of anonymity and spatio temporal nature of the internet. However, the uninterrupted advances in information and communication technologies (ICTs), especially the introduction of internet broadband technology (IBT) to the public had given stalkers new platforms to attack their targets, across borders, which gives rise to a new form stalking known as cyberstalking (Loong, 2014).

Cybercrimes Act (2015) defined cyberstalking as the use of electronic communications network to persistently send a message or other matter that, (a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; (b) for the purpose of causing annoyance, inconvenience or needless anxiety to another. Therefore, the various forms of cyberstalking include sending harassing text messages, taking photos or videos of victims without their consent, harvesting and sending malicious malware or spyware to the victim's e-mail, sending false information or statements to people Facebook timelines, and monitoring the victim's activities on the platform or any other (Abu-Ulbeh et al., 2021). Moreover, great number of cyber stalking is taking place through the use of social networking site platforms.

Cyberbullying

Cyber bullying is the use of electronic devices to bully, threatening or intimidating individuals or instigate fear or to cause harm which is perpetuated through the use of internet in the cyber space. Matlhare et al. (2020) defined bullying as the aggressive, intimidation and the oppression of a vulnerable and defenceless person. Cyberbullying means experience of aggressive, intentional act carried out by a group or individual, using information and communication technologies (ICTs), over and over against a person who cannot easily defend him or herself (Wright & Wachs, 2019). This is perhaps why most victims of cyberbullying are young persons who may not resist being bullied. Peterson (2017) stated that cyberbullying and harassment, including threatening or sending unsolicited sexual messages are common among children and adolescents. Although cybercrimes are generally evolving in our cyberspace, cyberbullying is one of the prevalent patterns due to the

rising popularity of social media. Ngo (2020) stated how cyberbullying receives increased attention from researchers, teachers/schools, parents, children/adolescents, and the general public due to its rapid increase against social media users, especially Facebook users. The resent use of mobile application and the rise of smart phones have yielded to more accessible form of cyber bullying which expected that cyber bullying via platforms will be associated with bullying via mobile phones to a greater extent that exclusively through other more stationary internet platforms (DeMarco, Crowther, & Benard, 2018).

Online Bet9ja Gambling

Online Bet9ja has become widely recognised by the youths across the country due to it popularity of sport betting which enable them to get money through the various sports, games and casinos that take place in the cyber world today. Bet9ja (also known as betting) is a wagering money or something of value (referred to as "the stakes") or an events with an uncertain outcomes, with the primary intent of winning money or material goods using internet or any technology assisted tool. Online Bet9ja Gambling thus requires three elements to be present: consideration (an amount wagered), risk (chance) and a prize (the outcome). It is also a major international commercial activity, with the legal gambling market totaling an estimated $335 billion in 2009. The gambling can be conducted with materials, which have a value, but are not real money. For example, players of marble games might wager marbles (Nilsson, Ioannou, & Lester, 2018).

Sexting

Sexting is emerging trend in global technological world. Sexting is a knotty expression of sexual interest in the internet. The concept and term of sexting was recognized primarily in 2005 by the Daily Telegraph and became an official word in 2009 (Gasso et al., 2019a). It involves creating and sharing of nude or sexually suggestive images or materials, including plain text messages on the internet or social media platforms (Mitchell, et al., 2012). Similarly, Wolak and Finkelhor (2011) stated that the term “sexting” has been used in the media and by researchers to refer to sexual communications with content that includes both pictures and text messages, sent using cell phones and other electronic media. The phenomena such as non-consensual types of sexting such as forced webcam sex or sextortion of adolescents pose a great deal of negative impact on children’s sexual lives (Chatzinikolaou & Lievens, 2019). Increased use of internet and associated technologies had increased users’ chances of coming across unsolicited sexual materials. The motivation behind sexting is crucial to assess whether it aligns more with sexual expression or sexual exploitation. Several factors could be the reason such as peer pressure, desire for validation, curiosity and the influence of media and social media. All of these play a role in encouraging youth to engage in sexting (Olusola, & Yinka, 2013)

Sextortion

The increase number of social media platform has provided avenue for new and unique forms of crime in the cyber space like sextortion. Moreover, Nilsson, et al. (2018) see sextortion as an emerging threat that is facilitated by the use of online environments where perpetrators gain the trust of vulnerable individuals in order to obtain sexually explicit material and then use it to coerce, threaten or intimidate the victims for the purposes of sexual, personal or financial gain. Sextortion

is defined as threats to expose a sexual image in order to make a person do something or for other reasons, such as revenge or humiliation (Wolak & Finkelhor, 2011). Carlton (2020) opined that, sextortion is not well-defined by laws or understood by people. Sextortion is essentially the threat to expose a sexual image to coerce the victim into doing something, even if exposure of the image never actually occurs. The intention is to instigate fear, intimidation, restlessness, and discomfort by showing or threatening to publish nude images or videos of someone viral on social media platforms.

Cyber Hate (Speech)

Cyber Hate Speech is emerging trend in global technological world internet is considered as more power full channel for disseminating the news and information. Internet have become more accessible through the use of technological devices like smart phones, iPad, laptop and tablet computer. However, the presence of proximity, anonymity and worldwide services of the internet has made it an appropriate tool for spreading hate and extremism. Hate speeches were spread in emails and chat rooms in the olden days. But, due to availability of social networking sites today, spread of hate speech becomes easy and speedy (Jaishankar, 2008). Moreover, Ben-David and Fernández (2016) believed that the rise in the popularity of social media such as Facebook and Twitter have introduced new avenues for circulation of hate speeches. Cyber hate are online speeches that are regarded as derogatory, inciting, insulting, or defamatory said against a individual or group of individual. Social networking sites are platforms that allows people to express their views to others, either on their timeline or in groups. This serves as opportunity, example, for political actors, to blackmail their opponents, which constitutes cyber hate (Apuke & Apollos, 2017). This development influences the exponential growth of political extremism, hate, and discriminatory practices on social media platform despite the platforms' policies and functions to prevent them.

Spread of Fake News

Spread of fake News and cyber hate speech are moving hand in hand. Usually, the latter involves the former. For David et al. (2018), fake news overlaps with other information disorders, such as misinformation (false or misleading information) and disinformation (false information that is purposely spread to deceive people). This implies that fake news deals with spread of misleading or false information for selfish gains. Social media companies are making efforts to dislodge fake news (or misinformation) from their platforms (Henry et al., 2017).

moreover, Geeng et al. (2020) argued that the speed, ease, and degree at which information spread on social media denote that content moderation by the companies may be herculean or sometimes impossible. For example, languages other not configured in the social media platforms may be used to spread fake news without them detecting. Also, large contents are created and shared on social media platforms by users. So, it is difficult to account for all bytes of the contents that make up big data. Ghosh (1999) is of the view that cyberspace is porous market of information, which permits the creation of unauthorized channels for distribution of information.

Identity Theft

This is the fastest growing types of fraud across the globe. Identity theft is the act of obtaining sensitive information about another person without his or her concerned or knowledge, and using this information to commit theft or fraud (Quayle & Loof, 2014). The Internet has given cyber criminals the opportunity to obtain such information from vulnerable organization, companies' database. It has also enabled them to lead the victims to believe that they are disclosing sensitive personal information to a legitimate business; sometimes as a response to an e-mail asking to update billing or membership information; sometimes it takes the form of an application to a (fraudulent) Internet job posting. According to the All Party Parliamentary Group 2012, the available research, both in the UK and globally, indicates that identity fraud is a major and growing problem because of the escalating and evolving methods of gaining and utilizing personal information. Subsequently, it is expected to increase further over the coming years. This is an issue which is recognized in the highest levels of Government. In 2012 alone CIFAS, the UK's Fraud Prevention Service, identified and protected over 150,000 victims of these identity crimes (CIFAS, 2012).

Theoretical Frame Work

Space Transition Theory (STT) was used to explain the emerging threats of cybercrime as global issues. As a cyber-specific theory explains the changing nature of people's behaviours as they move from physical space to cyberspace and vice versa.

The space transition theory of cybercrime was developed by Jaishankar (2008). The theory posits that the behaviour of people in cyberspace tends to bring out their compliance and noncompliance behaviours both in the physical and in cyberspace. This theory does not explain physical space crime but cybercrime and how people move and behave from one space to the another. This entails persons with repressed criminal behaviour (in physical space) having a propensity to commit crime in cyberspace, which they would not otherwise commit in physical space due to their status and position. It also implies that the status of people in physical space does not transfer to cyberspace. For instance, he argues that the individual behaviour repressed in physical space is not repressed in cyberspace. The space transition theory argues that people behave differently when they move from one space to another, in this context, Jaishankar (2008). Postulates the theory as follows:

1. Persons with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise, they would not commit in physical space due to their status and position.
2. Identity flexibility, dissociative anonymity, and a lack of deterrence factors in cyberspace provide the offender with the choice to commit cybercrime.
3. Criminal behaviour of offenders in cyberspace is likely to be imported into physical space, which in physical space may be exported to cyberspace as well.
4. Intermittent ventures of offenders into cyberspace and the dynamic spatio-temporal, the nature of cyberspace provides the chance to escape.
5. Strangers are likely to unite in cyberspace to commit crimes in physical space. Associates of physical space are likely to unite to commit crime in cyberspace.

6. People from a closed society are more likely to commit crimes in cyberspace than people from an open society.
7. The conflict between the norms and values of physical space and the norms and values of cyberspace may lead to cybercrimes.

The application of Space Transaction Theory (STT) can be traced to the revolution of information and communication technology (ICTs), especially digital devices such as smartphones, iPhones, and iPads, internet technology, and social networking sites (SNS), which provide the opportunity for real-time communication in cyberspace. The first assumption of the theory of STT is that people who are internet active users and cyber criminals will use the cyber space to carry out their heinous activities through the internet to victimize individuals in society, which will not be done in the physical space due to their reputation. The alarming phenomenon of Cybercrimes in society is associated with identity, flexibility, and dissociative anonymity that encourage criminal minded to migrate to cyberspace to identify and target their victims. Before the advancement of the internet, most of these crimes are usually face-to-face (in physical space).

Moreover, the lack of deterrence in cyberspace and control by the government give criminals the opportunity to perpetrate various form of crime in cyberspace. Due to the lack of control by the law enforcement agencies in cyberspace and especially the censorship that will monitor the activities of people on social networking sites, this gives the perpetrator the chance to target their victims without fear of being detected by the law enforcement agencies in charge of controlling crime in cyberspace. However, intermittent ventures in cyberspace and the dynamic spatiotemporal nature of cyberspace give the offenders the chance to escape in cyberspace without being tracked by the law enforcement.

Discussion of Findings

The study revealed that the advent of social media such as WhatsApp, Facebook and Tweeter among others has dramatically become an analogy for unique forms of crime in the cyber space which are committed in daily basic, moreover, crimes like cyber stalking, cyber bullying cyber defamation are committed due to the evolution of information communication technology in the world. The threats of social networks are becoming major alarms for the technology of the internet and its applications (Michael et al., 2014). The availability and accessibility of the internet within the cyber environment allow motivated cyber offenders to detect their targets and attack them from anywhere in the world (Shabnam et al., 2016). The porous nature of the internet give room for criminal minded from open society to cyber world to perpetrate any such of criminal behaviour in the cyber space. The Internet is free and open to all, allowing anyone to contact anyone else with no identity or passport needed (Tade & Aliyu, 2011). Despite the fact that most of internet users are not aware of crime in cyber space and its implication against them, these give the offenders the chance to victimize internet naives about cyber threats, social networking site users may not pay attention to security or privacy settings or measures that protect them against victimisation in the cyber space.

Moreover, the phenomenon of cybercrimes is encompassing all illegal activities which are committed by individuals, groups and genders. There are enough motivations for organised criminal groups to employ the internet architecture for criminal gains. One of such reasons is that the Internet guarantees them anonymity and drastically reduces their risk of doing "business," as their chances of apprehension are relatively low (Ndubueze, 2020). Cyber policing has become subject of discussion across the globe due to the international boundaries and the differences of cyber laws of one country to another. Cyber policing tends to have unique challenges due to a lack of cyber competency and expertise among the cyber policers (Abdullahi & Jahan, 2020).

Conclusion

Cybercrime is an emerging global threat which is evolving across the world is considered as a trending social problem which has negative and physical consequences on individuals and the society at large. Moreover, these emerging cyber threats are committed in daily basis irrespective genders and ages, youths and adolescent are usually those that perpetrate this so-called phenomenon through the use of social networking sites application. The accessibility of the internet within the cyber environment allow motivated cyber offenders to detect their targets victims and attack them from anywhere in the world. Due to lack of cyber policing and censorship that will monitor the activities of criminal minded in the cyber space these give propensity of crime to take place in the cyber space. Moreover, these agencies are in charged with the responsibility to combat crime in cyberspace in Nigeria. The crimes include the Economic and Financial Crimes Commission (EFCC), the Nigeria Police Force (NPF), the Department of State Services (DSS), the National Information Technology and Development Agency (NITDA), and the National Communication Commission (NCC), among others Cybercrimes Prohibition, Prevention etc. Act (2015). Moreover, punishment should reflect the amount of offence been committed by the cyber criminals across the geographical entity of globe.

Recommendations

1- Government should provide public lectures campaign and awareness/prevention about the menace of cybercrime across the glove
2- The internet services (ISPs) should monitor suspicious activities of individuals online and alert relevant law enforcement authorities.
3- The Interpol and other agencies that are responsible in combating cybercrime should censor the use of the social media platform in the global village this will enable to curb criminal minded individuals across the globe.
4- To effectively fight cyber security threats at the national level, the cyber laws should not be restricted to only those operating within a country; there should be inter-regional and international cyber laws;
5- To ensure deterrence against cyber threats, sanctions on cybercrimes should be as severe as the gravity of the offence committed;

References

Abdullah, A.M. & Jahan, I. (2020). Challenges of Cyber Policing in Response of Cybercrime to Reduce Victimization. *International Journal of Research and Innovation In Social Science (IJRISS)*, IV(V), 219-226.

Abu-Ulbeh,W., Altalhi, M., Abualigah, L., Almazroi, A.A., Sumari, P., Gandomi, A.H. (2021).Cyberstalking Victimization Model Using Criminological Theory: A Systematic Literature Review, Taxonomies, Applications, Tools, and Validations. *Electronics*, 10, 1670.

Adesina, O.S. (2017). Cybercrime and Poverty in Nigeria: *Canadian Journal of Social Sciences*, 13(4), 19-29.

Adeta, K.A. (2014). Patterns and Consequences of Cyber-Crime in Tertiary Institutions in Zaria: A thesis Submitted to the School of Postgraduate Studies, Ahmadu Bello University, Zaria, in Partial Fulfillment of the Requirements for the Award of Master Degree in Sociology.

Apuke, O.D. & Apollos, I.N. (2017). Public Perception of the Role of Facebook usage in Political Campaigns in Nigeria. *International Journal of Community Development & Management Studies*, 1, 85-102

Ben-David, A.B., & Fernandez, A.M. (2016). Hate Speech and Covert Discrimination on Social Media: Monitoring the Facebook Pages of Extreme-Right Political Parties in Spain. *International Journal of Communication*, 10, 1167–1193

Betancourt, A. (2016). Do Cyber Victimization and Traditional Victimization Form Separate Factors? Evidence from a Preliminary Study. *International Journal of Information and Education Technology, 6(4), 296-300.*

Brenner, S.W. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare: *Journal of Criminal Law and Criminology*, 97(2), 379-476.

Carlton, A. (2020). Sextortion: The Hybrid "Cyber-Sex" Crime. North Carolina Journal of Law and Technology, 177. https://scholarship.law.unc.edu/ncjolt/vol21/iss3/5

Chatzinikolaou, A. & Lievens, E. (2019). Towards a Legal Qualifcaton of Online Sexual Acts in which Children are Involved: Constructng a Typology. European Journal of Law and Technology, 10(1), 1-25.

CIFAS (2012). The UK's Fraud Prevention Service. *Availableat: http://www.cifas.org.uk/ Council of Europe (CoE).*

Cyber Crime Prohibition and Prevention Act, (2015). By Nigerian Government.

David, M. J. L., Matthew A. B., Yochai Benkler, A.J., Berinsky, K. M., Greenhill, F. M., Miriam J. M., Brendan, N., Gordon P., David R., Michael, S., Steven A. S., Cass, R. S., Emily, A. T., Duncan J. W. & Jonathan, L. Z. (2018). The science of fake news: Addressing fake news requires a multidisciplinary effort. *Science* 359 (6380), 1094-1096.

DeMarco, J., Sharrock, S., Crowther, T. & Benard, M. (2018). Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation: A Rapid Evidence Assessment. NatCen Social Research.

Edwards, M., Peersman, C., & Rashid, A. (2017). Scamming the Scammers: Towards Automatic Detection of Persuasion in Advance Fee Frauds. International World Wide Web Conference Committee (IW3C2). http://dx.doi.org/10.1145/3041021.3053889

Geeng, C., Yee, S. & Roesner, F. (2020). Fake News on Facebook and Twitter: Investigating How People (Don't) Investigate. CHI Paper 655, 1-14

Ghosh, G. (1999). Gray Markets in Cyberspace. *J. Intell. Prop. L* 7 (1), 1-55. https://digitalcommons.law.uga.edu/jipl/vol7/iss1/2

Halder, D. & Jaishankar, K. (2016). Celebrities and Cyber Crimes: An Analysis of the Victimization of Female Film Stars on the Internet. *Temida, 19(3-4), 355-372.*

Harkin, D., Whelan, C. & Chang, L. (2018). The challenges facing specialist cyber-crime units: an empirical analysis. *Police Practice and Research*, 19(6), 519-536.

Henry, N., Powell, A. & Flynn, A. (2017). Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse. A Summary Report. RMIT University.

Ibekwe, C.C., Onyima, B.N. & Onyilofor, T.U. (2021). COVID-19 Pandemic and Proliferation of Ponzi Schemes in Nigeria Cyberspace. *Pakistan Social Sciences Review*, 5(2), 414-430.

Ibrahim, S. (2016).Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice, 47*, 44-57.

Jaishankar (2011). Expanding Cyber Criminology with an Avant-Garde Anthology. In Jaishankar (Ed.), *Cyber Criminology: Exploring Internet crimes and criminal behavior* (pp. xxvii–xxxv): CRC Press.

Jaishankar K (2008). Space Transition Theory of Cyber Crimes. In Schmallager F, Pittaro M (Eds.), *Crimes of the Internet* (pp. 283-301):Prentice Hall

Jaishankar, K. (2008). *Space transition theory of cybercrimes, crimes of the internet.* Pearson Publishers. ISBN-13:978-0-13-231886-0 pp.283-299

Leukfeldt, ER, Yar, M (2016) Applying Routine Activity Theoryto Cybercrime: A Theoretical and Empirical Analysis, *Deviant Behavior*, 37(3), 263-280.

Loong, A.C.J. (2014). Cyberstalking on Facebook: Examining the Relationship between Facebook Usage Characteristics and Cyberstalking Victimization among Young Malaysian Facebook Users. A dissertation submitted to the Department of Internet Engineering and Computer Science, Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, in partial fulfillment of the requirements for the degree of Master of Information Systems.

Matlhare, B., Faimau, G. & Sechele, L. (2020). Risk Perception and Knowledge of Cybercrime and its Preventive Strategies among Youth at the University of Botswana. *Mosenodi Journa*l, *23*(1) 99-113.

Michael, A.K, Boniface, A.K. & Olamide, A.S. (2014). Mitigating Cybercrime and Online Social Networks Threats in Nigeria: *Proceedings of the World Congress on Engineering and Computer Science*, 1, n.p.

Mitchell, K.J., Finkelhor, D., Jones, L.M. & Wolak, J. (2012). Prevalence and Characteristics of Youth Sexting: A National Study. *PEDIATRICS*, 129 (1), 13-20.

Mohamed Ali Saeh, (2012). Online Defamation and Intermediaries 'Liability: *International' (Social Science Research Network 20 December 2012)*SSRN Scholarly Paper 14

Mohammed A.N.A., Imam, & Goni .I. Usman., (2020). Cyber Stalking Victimization among Undergraduate Students in Yobe State University, Damaturu-*Nigeria Jalingo Journal of Social and Management Sciences* Volume 2, Number 4 September, 2020 ISSN 2659-0131

Ndubueze, P.N. (2020). Cybercrime and Legislation in an African Context. In Holt, TJ, Bossler, AM (Eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, https://doi.org/10.1007/978-3-319-78440-3_74

Ndubueze, P.N. (2020). Cybercrime and Legislation in an African Context. In Holt, TJ, Bossler, AM (Eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, https://doi.org/10.1007/978-3-319-78440-3-74

Ngo. F. (2020). Social Media: The Unseen Risks of Cybercrimes. A Thesis Presented to the Faculty of Anna Maria College Anna Maria College in Partial Fulfillment of the Requirements of the Degree of Bachelor of Science in Criminal Justice.

Nilsson, M.G., Tzani-Pepelasis, C., Ioannou, M. & Lester, D. (2018). Understanding the Link between Sextortion and Suicide.

Olusola, M., Samson, O., Semiu, A. & Yinka, A. (2013). Cyber Crimes and Cyber Laws in Nigeria. The International Journal of Engineering and Science (IJES), 2(4), 19-25.

Olayemi, O.J. (2014). Combating the Menace of Cybercrime: *International Journal of Computer Science and Mobile Computing*, 3 (6), 980-982.

Quayle, E., Allegro, S., Hutton, L., Sheath, M., & Loof, L. (2014). Rapid skill acquisition and online sexual grooming of children: Computers in Human Behavior, 39, 368–375.

Peterson, J. K. & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? *College of Liberal Arts All Faculty Scholarship*. 5. http://digitalcommons.hamline.edu/cla_faculty/5

Shabnam, N., Faruk, O. & Kamruzzaman, M.D. (2016). Underlying Causes of Cyber-Criminality and Victimization: An Empirical Study on Students. *Social Sciences*, 5(1), 2016, 1-6.

Tade, O. & Aliyu, I. (2011). Social organization of internet fraud among University Undergraduates in Nigeria. *International Journal of Cybercrime* 6 (3): 420-448.

Trend Micro & INTERPOL. (2017). *Cybercrime in West Africa: Poised for an Underground Market*: A joint Study Paper, 7-8. http://www.trendmicro.com/vinfo/us/ security/ news/cybercrime-and-digital-threats.

Whittaker, J.M. & Button, M. (2020). Understanding pet scams: A case study of advance fee and non-delivery fraud using victims' accounts. *Australian & New Zealand Journal of Criminology, 53(4), 497–514.*

Wolak, J. & Finkelhor, D. (2011). *Sexting: A typology*. Crimes against Children Research Center.

Wright, M.F & Wachs, S. (2019). Adolescents' Psychological Consequences and Cyber Victimization: The Moderation of School-Belongingness and Ethnicity. *International Journal of Environmental Research and Public Health, 16, 2493. 1-11.*