American Journal of Engineering Research (AJER) **2021**

American Journal of Engineering Research (AJER)

e-ISSN: 2320-0847 p-ISSN : 2320-0936

Volume-10, Issue-10, pp: 119-121

www.ajer.org

Research Paper Open Access

Cybercrime, Anonymity, and Link to Cryptocurrency

Samira Ibrahim[1], Daniel Ikechukwu Nnamani[2], Abidemi Temitope Omoloja[3]

[1]*Texas Southern University, Barbara Jordan- Mickey Leland School of Public Affairs, Department of Administration of Justice*

3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 346-401-7062

mirakaf@gmail.com

[2]*Texas Southern University, Barbara Jordan- Mickey Leland School of Public Affairs, Department of Administration of Justice*

3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 832-946-1426

dnamani13@gmail.com

[3]*Texas Southern University, , Department of computer sciences, 3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 (281) 745-6647*

abidemiomoloja@gmail,com

Abstract:*Since the dawn of the cyberspace age, cybercrime has evolved such that its scope and the number of its forms now belie the original aims at the heart of the invention of the computer and the internet.Today, cybercriminals can commit identity theft, hacking, privacy invasion, internet fraud, child pornography, file sharing and piracy, forgery and counterfeiting, denial of service attacks, computer viruses, cyber terrorism, spamming and mail fraud, and cyberbullying; while operationalizing technologies that are designed to conceal their identity. This study defines cybercrime, explores its origins and evolution, defines online anonymity, and illustrates how cybercrime has been facilitated by more sophisticated techniques of anonymity. Finally it link cybercrime to the groundbreaking cryptocurrency technology and offers an informed prediction of its outlook going forward.*

Keywords: Cryptocurrency, Cybercrime, Online Anonymity.

Date of Submission: 18-10-2021 Date of acceptance: 02-11-2021

I. INTRODUCTION

Cybercrimes can be defined as indictable deeds which involve computers, networks or networked devices as weapons, accessories or targets (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014). This implies, with the exception of novel forms, that cybercrimes types are generally similar to traditional and historically established types of crime, only demarcated by the operationalization of computer and internet technology (Marcum and Higgins, 2019). The discovery, identification and study of cybercrime in the history of academia have been closely followed by legislative efforts to control it and its forms; in the wake of the invention and rapid development of computer and internet technologies (Marsili, 2019). Nonetheless, such efforts have continued to come up against a dearth of credible statistical data on, and general ambiguity in the categorization of, cybercrime forms today. Importantly, for a contextual grasp of cybercrime, a short history of its origins and evolution are delineated in the following paragraph.

Origins and Evolution of Cybercrime

As is alluded to in the paragraph above, the general ambiguity discoverable in the literary scholarship on cybercrime today and the lack of a handle on its true extents and hotspots are down to the wild evolution of modern computers and internet technology discoverable today; a little over four decades after they arrived. While some other major forms of crime have existed for centuries now, the advent and evolution of cybercrime in its clearest form tightly follows the invention and evolution of the mobile computer around the late 1970s, and the internet in the early 1980s (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014).

Prior to the internet, cybercrime was in its most rudimentary of forms and largely entailed the theft of records and information from local networks (Scheau and Pop, 2018). After the internet had arrived and proliferated, the first clear form of cybercrime arrived in the form of email scams. Across the '80s, the major form of cybercrime other than information theft was inbox fraud; a clear example of which was the advance-fee scam heavily linked to West Africa today (Marcum and Higgins, 2019). By the 90s, the scene around cybercrime had taken a new appearance. Then was the age of web browsers; information technologies that had only begun to be explored and faced little restraints (Armstrong and Forde, 2003). In this climate, users and computers were susceptible to network compromise from viruses spread via unsecured web connections.

By the time the new century rolled around, the cyberspace was getting accustomed to social media; technologies where users could own accounts, post personal information, communicate, and share digital data (Marcum and Higgins, 2019). However, the very nature of these platforms meant that there was soon an embarrassment of private information online, providing cybercriminals with the tools to perpetrate acts ranging from identity theft to financial fraud (McQuade, 2006). In the second decade of the 2000s, cybercrime had grown so sophisticated that it virtually seemed boundless. Now blessed with skills honed over several years, cybercriminals had not only improved upon the illicit cyber acts pertinent to the decades prior, but they could compromise national, corporate and personal networks, illegally obtain information from them, steal and transfer illicit financial gains beyond the reaches of regional law enforcement, sponsor terrorist acts offshore, blackmail individuals or organizations for financial or political gain, infringe on copyrights, wage war, perpetrate sex trafficking, spy on states and organizations, stalk, and bully individuals and commit cryptocurrency fraud; while operationalizing software that are designed to conceal their identity (Chawki, 2010; Department of Justice, 2020.This latest node in the cybercrime base is what is referred to as anonymity. It is this feature of the current, sophisticated cyberspace that has enabled cybercrime to thrive seemingly beyond the check of formal law enforcement systems.

Online Anonymity

On a very basic level, anonymity can be defined as the feature of computer technology and the internet that enables users to conduct activities on the internet and digital networks without giving up their identity or revealing their actions to others (Armstrong and Forde, 2003). In the cyberspace, this status can be achieved through a number of techniques, including but not limited to the use of proxy servers and anonymity networks.

Techniques

Proxy servers are servers which operate in an intermediary capacity and which can be used to link a user's device with another device which the user intends to obtain information or resources from (Sarda et al, 2019). Anonymous proxy servers work by concealing the identity of the user by substituting their Internet Protocol (IP) address with a different one.

An anonymity network is another technique similar to proxy servers. It serves to conceal the IP Address of a user, and therefore their true location and activities. However, it is different in that it also stems access traffic from the service provider (Sarda et al, 2019). Anonymity networks, often in the form of software applications, shield the identity of users while also possessing the capability to host sites through concealed networks (Chawki, 2010). This is what enables users to access illicit parts of the internet such as the Dark Web.

Anonymity and Cybercrime

There is a subtle but perceptible debate in the domain of cybercrime research on the evolutionary direction of online anonymity since the invention of the internet. This is borne out of the need to determine whether online anonymity has grown stronger or weaker since the early days of the Web. On the one side, one group of researchers argue that there was much more anonymity in the first decade of the internet than is obtainable now, as users could very easily create web accounts with any identity they deemed fit, while many platforms today require users to create accounts with their real identity (Armstrong and Forde, 2003; Bray, 2016). On the other hand, the opposing batch of scholars argue that while the above may have been the case, the degree of sophistication of computer technologies obtainable today means that these requirements are not only overridden easily, far more daring heists can be pulled off in the cyberspace today without the perpetrator revealing their identity (Sarda et al, 2019).

The relationship between crime and anonymity in the cyberspace has flourished since the '80s (Chawki, 2010). Regardless of arguments that online anonymity is necessary to create a healthy cyberspace where user privacy rights are protected, furious efforts continue to be made to reduce the bar of anonymity in the cyberspace on the grounds that it has enabled the various forms of cybercrime obtainable today to thrive (Marcum and Higgins, 2019; Marsili, 2019). Online anonymity, regardless of what its true evolutionary course is, has for the best part enabled cybercrime to thrive by equipping users with the capability to conceal their identity and their actions during and after the execution of cybercrimes (Sarda et al, 2019).

Often, powerful web anonymizers used in crimes enable cybercriminals to operate outside the purview of the polity where communications originate. In the execution of cybercrimes such as BEC scams, email fraud, spamming and file sharing;anonymizers, including remailers, conceal the email address of a perpetrator and encrypt their messages to appear harmless and enable them get through spam detection walls and into the inbox of unsuspecting victims (Chawki, 2010; Jahankhani, Al-Nemrat and Hosseinian-Far, 2014; Sarda et al, 2019). In the execution of crimes like cyberbullying, child pornography, data sharing and cyber terrorism, these resources conceal the originating server information, assigned IP address, and identity of a perpetrator, and enable them to sneak in encrypted information through threat detection systems; create sites with misleading information for the dissemination of propaganda and recruitment information; access dark websites where they can trade stolen digital data; and transfer funds gained through or intended for illicit activities (McQuade, 2006; Bray, 2016). The transfer of finances in recent years has been made far easier through cryptocurrency technology (Foley, Karlsen and Putnins, 2019).

Cybercrime and Cryptocurrency

Defined simply as digital currency, cryptocurrency and cryprocurrency technology has enabled the perpetuation of financial cybercrime at a level of ease not formerly obtainable in traditional systems of financial transfer (Reddy and Minnaar, 2018). By virtue of its anonymity, open-source facility, availability, peer-to-peer transfer capacity and decentralization, cryptocurrency technology sits handsomely as the perfect means for the embezzlement of illicitly-obtained funds and financing of terrorist activity. Alone, the most popular cryptocurrency; Bitcoin, was reported in 2019 as being involved in roughly $80 billion of illegal activity annually (Foley, Karlsen and Putnins, 2019).

II. CONCLUSION

Cybercrime has, since the ‘60s, evolved to include dozens of unique forms. Today, cybercriminals can commit identity theft, hacking, privacy invasion, internet fraud, child pornography, file sharing and piracy, forgery and counterfeiting, denial of service attacks, computer viruses, cyber terrorism, spamming and mail fraud, and cyberbullying; while operationalizing technologies that are designed to conceal their identity. This feature, termed online anonymity, has matched the sophistication of the cyberspace across its four-decade lifespan and has enabled cybercrime to thrive seemingly beyond the check of formal law enforcement systems. With the arrival of the novel cryptocurrency technology in the late 2010s, cybercrime (particularly its financial forms) have become even more difficult to monitor and control. The outlook on this form of crime remains bleaker than ever; certainly from the perspective of traditional law enforcement.

REFERENCES

[1]. Armstrong, H. L., & Forde, P. J. (2003). Internet anonymity practices in computer crime. *Information management & computer security*.

[2]. Bray, J. (2016). *Anonymity, Cybercrime and the Connection to Cryptocurrency* (Doctoral dissertation, Eastern Kentucky University).

[3]. Chawki, M. (2010). Anonymity in cyberspace: Finding the balance between privacy and security. *International Journal of Technology Transfer and Commercialisation*, *9*(3), 183-199.

[4]. Foley, S., Karlsen, J. R., &Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?. *The Review of Financial Studies*, *32*(5), 1798-1853.

[5]. Jahankhani, H., Al-Nemrat, A., &Hosseinian-Far, A. (2014).Cybercrime classification and characteristics. In *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 149-164). Syngress.

[6]. Marcum, C. D., & Higgins, G. E. (2019).Cybercrime.In *Handbook on crime and deviance* (pp. 459-475).Springer, Cham.

[7]. Marsili, M. (2019).The war on cyberterrorism. *Democracy and security*, *15*(2), 172-199.

[8]. McQuade, S. C. (2006). *Understanding and managing cybercrime*. Boston: Pearson/Allyn and Bacon.

[9]. Reddy, E., &Minnaar, A. (2018).Cryptocurrency: A tool and target for cybercrime. *ActaCriminologica: African Journal of Criminology &Victimology*, *31*(3), 71-92.

[10]. Sardá, T., Natale, S., Sotirakopoulos, N., & Monaghan, M. (2019).Understanding online anonymity. *Media, Culture & Society*, *41*(4), 557-564.

[11]. Şcheau, M. C., & Pop, Ş. Z. (2018). Cybercrime evolution. *ISSN 1843-682X*, *24*(1), 225.

[12]. U.S. Department of Justice.(2020). A national strategy to combat identity theft.https://cops.usdoj.gov/RIC/Publications/cops-p107-pub.pdf

Samira Ibrahim, et. al. "Cybercrime, Anonymity, and Link to Cryptocurrency.”*American Journal of Engineering Research (AJER)*, vol. 10(10), 2021, pp. 119-121.