IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 5, Ser. II (Sep. −Oct. 2021), PP 24-26
www.iosrjournals.org

Types of Cybercrime and Approaches to Detection

Samira Ibrahim [1], Daniel Ikechukwu Nnamani [2], Ojeifoh Okosun [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

[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

[3]*Texas Southern University, Barbara Jordan- Mickey Leland School of Public Affairs, Department of Administration of Justice*
3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 346-777-0765

Abstract*: Since the dawn of the cyberspace age, cybercrime has evolved such that its scope and number of its forms now belie the original aims at the heart of the invention of the computer and the internet. Today, there are dozens of different forms of cybercrime, all with severe impacts for the finances, mental health, and physical safety of people, and consequently negative impacts for the economy and political orderliness of whole nations. These forms; privacy invasion and identity theft, cyber terrorism, child pornography and cyberbullying, are defined and their unique attributes are described. Finally, approaches to detection pertinent to each form of the cybercrime are delineated. The intent of the study is the identification of different forms of cybercrime to assist computer and internet users so that they do not fall victim to them.*

Keywords: Computer, Cyber Terrorism, Cyberbullying, Cybercrime, Identity Theft, Internet.

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

I. Introduction

A rough universalistic definition of the concept of cybercrime has arisen in academia across the 4-5 decades since its introduction (Marcum and Higgins, 2013). Today, cybercrime is defined as an activity that involves the use of a computer, network, or networked device; the target of a computer or network, or the employment of a computer as an accessory for the furtherance of illicit goals (Ali, Mohd and Fauzi, 2018; Vyawahare and Chatterjee, 2020). While the definition above may seem too simplistic, it certainly meets the criteria for the concept, as cybercrime is quite simply the extension of crime, but involving a computer or digital network, and encompassing new illicit activities by virtue of these novelties (Al-Khater et al, 2020). It is, therefore, the case that cybercrime has several forms to it. Four of these forms, or types, are briefly explored in the paper. These forms; privacy invasion and identity theft, cyber terrorism, child pornography and cyberbullying, are defined and their unique attributes are described. Finally, approaches to detection pertinent to each form of the cybercrime are delineated.

Types of Cybercrime and Approaches to Detection

Privacy Invasion and Identity Theft

By virtue of the highly digitized nature of citizen data collection and storage, the personal information of individuals in a given state or nationality are more at risk now than ever. Using the United States as a case in point, citizens and some United States residents who are documented in the national database are given a Social Security number instead of an identity number. This system of individual identification is employed in taxation, healthcare, education and employee documentation in some private organizations (Sharma and Gaherwal, 2017). Identity theft is, as such, very feasible, as access to a person's Social Security number can yield a wealth of information regarding the person's citizenship and facilitate the theft of their identity. This form of cybercrime is, however, not exclusive to the Social Security identification system, as it also applies to access and theft of an individual's digitized credit card details (Al-Khater et al, 2020). The acquisition of credit card details or Social Security information can serve many deleterious purposes, ranging from running up huge bills in the name of unsuspecting victims to selling the information for financial gain.

The multinational pertinence of identity theft makes it one of the commonest forms of cybercrime. However, there is a dearth of accurate global statistics on it. In the United States though, as much as 1.1 million Americans are victims of identity theft annually (Department of Justice, 2015), while another 15 million suffered from the theft of their financial account information and unauthorized access to their finances (Department of Justice, 2020). The cost of identity theft in the United States is estimated at more than $15 billion. The fallout from this, as such, has necessitated research on possible techniques of identity theft detection. When successful, identity theft can intersect with, or directly cause other independently defined forms of cybercrime. Some of these are hacking, ATM fraud, wire fraud, file sharing and piracy (Marcum and Higgins, 2019).

The risk of identity theft on computer or digital networks can be determined if a user receives requests for sensitive information—Social Security number, credit card details, mobile financial application username, password and PIN, savings account details—via email or social media platforms. It is important to note that the organizations that legitimately need such information—an employer, medical provider, school, bank or tax agency—rarely, if ever, use these channels to solicit for them (Al-Khater et al, 2020). Other methods of detection include the tracking of bills to know if and when a billing address has been changed; the frequent review of bills and bank accounts to know if or when there are charges for purchases not made (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014); the review of credit reports to detect accounts in a foreign name; and the acquisition of sophisticated software programs for strong password protection and detection of unauthorized network infiltration (Marcum and Higgins, 2019).

Cyber Terrorism

Cyber terrorism simply refers to the employment, operationalization, or target of computers and networks for the aims of spreading information or inciting fear, anxiety and violence (Marsili, 2019). Much like traditional forms of terrorism, cyber terrorism is not only commonplace, but its impacts can be severe. The careful dissemination of carefully formulated propaganda through internet technologies and across social media platforms can adversely impact the credibility and availability of information in a target location, facilitate political sabotage, negatively change public opinion, disrupt law and order, the damage of infrastructure and death (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014; Marsili, 2019).

The detection of cyber terrorism is a rather tricky endeavor, as the intent behind it usually comes to fruition before it is detected. In fact, cyber terrorism often goes undetected by its victims (Zhang, 2008). The classification of this form of cybercrime is often then left to professionals, usually working for the government, who possess the psychological and analytical resources suitable for the identification of phony information making the rounds on the cyberspace (Marcum and Higgins, 2019). On the surface, one can equip oneself to detect and prevent the effects of cyber terrorism by spotting information online that has been taken out of context by the creator or that irrationally incites the audience to take drastic actions.

Child Pornography

Child pornography as a form of cybercrime entails the spread of digital recordings (videos, images and audio files) of children and minors dressed inappropriately, scantily or appearing in no clothes at all; taking positions of or speaking in a sexually provocative manner (Sae-Bae et al, 2014). Sociological differences notwithstanding; the dissemination of child pornography is a serious crime globally (Vyawahare and Chatterjee, 2020). The impacts of child pornography on a minor include lifelong damages to self-image, the development of psychological disorders, problems with socialization, and disruptions in sexual development (Bada and Nurse, 2020).

The detection of child pornography is not a straightforward process, as spotting digital content portraying persons who appear underage in sexual positions may not be a completely reliable method. This is because the age of minority in certain polities can be as low as 18; an age where legal adults can easily appear underage (Sae-Bae et al, 2014). Nonetheless, this remains the best means of detecting child pornography in digital content. On a higher level of legislative enforcement, producers of adult digital content are required to show certification that the actors, actresses and models in their productions are, in fact, of a legal age (Dragan, 2018).

Cyberbullying

Cyberbullying entails the utilization of coercion, force, threats, and/or teasing to intimidate, abuse and/or dominate another individual, via computer networks, the internet or social media platforms (Ali, Mohd and Fauzi, 2018; Perera and Fernando, 2021). The rise of social media technologies in particular has been integral to the advent and evolution of cyberbullying, as the perpetual growth in the number of users from different social groups has served up a hotbed of unwanted social behaviors on these platforms. Teenagers and women are overrepresented in the victim population of cyberbullying (Vyawahare and Chatterjee, 2020). The various forms cyberbullying can take include but are not limited to cyber abuse (the perpetuation of verbal attack on social media); morphing (the unauthorized acquisition and spread of a victim's digital information online, for pornographic ends) (Bada and Nurse, 2020); cyber libel (the dissemination of false or incredible information about an individual or their interests online); and cyber blackmail (the illegal use of an individual's personal information to coerce and intimidate them into granting favors) (Dragan, 2018).

The detection of cyberbullying comprises of processes quite similar to those for the detection of cyber terrorism. Here, a user (or importantly, a parent) can detect cyberbullying by seeking to spot instances of verbal attack on social media, the unauthorized acquisition and spread of their (child's) digital information online, for pornographic aims, the dissemination of false or incredible information about them or their child online, and the illegal use of their personal information to coerce and intimidate them into granting political, sexual or financial favors (Bauman, 2015; Dragan, 2018). It is also important to understand that cyberbullying is often repetitive in nature, and mainly affects teenagers and females. These variables are invaluable in the detection of potential cases of this form of cybercrime.

Technical Cybercrime Detection Techniques

At the level of lawmaking and law enforcement, more technical and analytical resources are being operationalized in the detection of various forms of cybercrime, globally. These are cybercrime detection using statistical methods, neutral networking, machine learning, deep learning, data mining, and image and pattern detection systems (Al-Khater et al, 2020; Ali, Mohd and Fauzi, 2018; Sae-Bae et al, 2014). Generally speaking, these techniques go beyond the scope of the common civilian—with respect to both skill and accessibility—and, as such, the scope of this paper. Simply put, these technological techniques are often only employed by governments in the war against cybercrime (Al-Khater et al, 2020; Vyawahare and Chatterjee, 2020).

II. Conclusion

Since the dawn of the cyberspace age, cybercrime has evolved such that its scope and number of its forms now belie the original aims at the heart of the invention of the computer and the internet. Today, there are dozens of different forms of cybercrime, all with severe impacts for the finances, mental health, and physical safety of people, and consequently negative impacts for the economy and political orderliness of whole nations. Through the exploration of four selected cybercrime forms; identity fraud, cyber terrorism, child pornography and cyberbullying, it is determined that the detection of these crimes generally entails awareness of their commonness, an understanding of their definitive characteristics, and the possession of pertinent technical and analytical resources.

References

[1]. Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8*, 137293-137311.

[2]. Ali, W. N. H. W., Mohd, M., & Fauzi, F. (2018, November). Cyberbullying detection: an overview. In *2018 Cyber Resilience Conference (CRC)* (pp. 1-3). IEEE.

[3]. Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73-92). Academic Press.

[4]. Bauman, S. (2015). Types of cyberbullying. *Cyberbullying: What Counselors Need to Know*, 53-58.

[5]. Dragan, A. T. (2018). Child pornography and child abuse in cyberspace. *Journal of Legal Studies "Vasile Goldiş"*, *21*(35), 52-60.

[6]. 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.

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

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

[9]. Perera, A., & Fernando, P. (2021). Accurate Cyberbullying Detection and Prevention on Social Media. *Procedia Computer Science*, *181*, 605-611.

[10]. Sae-Bae, N., Sun, X., Sencar, H. T., & Memon, N. D. (2014, October). Towards automatic detection of child pornography. In *2014 IEEE International Conference on Image Processing (ICIP)* (pp. 5332-5336). IEEE.

[11]. Sharma, S., & Gaherwal, R. (2017). Comparative Study and Analysis of Unique Identification Number and Social Security Number. *Int. Journal of Scientific Research in Computer Science and Engineering*, *27*.

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

[13]. U.S. Department of Justice. (2015). NIJ Identity Theft - A Research Review. https://www.ncjrs.gov/pdffiles1/nij/218778.pdf

[14]. Vyawahare, M., & Chatterjee, M. (2020). Taxonomy of cyberbullying detection and prediction techniques in online social networks. In *Data communication and networks* (pp. 21-37). Springer, Singapore.

[15]. Zhang, L. (2008). *Effective techniques for detecting and attributing cyber criminals*. Iowa State University.

Samira Ibrahim, et. al. "Types of Cybercrime and Approaches to Detection." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 23(5), 2021, pp. 24-26.