Why Criminals Conduct Crimes in Cyberspace

John R. Wilson

Old Dominion University

IDS 300W Introduction to Interdisciplinary Theory and Concepts

Dr. Virginia Tucker Steffen

16 April 2022

Abstract

This research paper attempts to discover the understanding of motivations behind criminal behavior in cyberspace through interdisciplinary research. The document will utilize a holistic approach to better understand the motivations behind cybercrime through focusing on human factors, economic, and political aspects that will advance the understanding of the nature of the cyber environment. For instance, some cybercriminals are motivated by a desire to test their hacking skills to showcase their technical abilities because it is exciting. While others might be motivated through financial gain because that is how they measure success, or some might steal and share government secrets because they strongly feel their actions are morally centered and benefit the common people. Having insight of human motivations through a multidisciplinary methodology helps broaden awareness of cybercrimes through linking the technical and human aspects of the cyber environment.

Keywords: Motivations, cybercriminals, cybercrime, cyberspace, interdisciplinary

Why Criminals Conduct Crimes in Cyberspace

Introduction

The modern-day world operates in a technologically enhanced environment with interconnected computer communication networks. Cyberspace is the term used to describe the increased spread of cyberspace with a virtual word created by the links between computers, servers, internet-based devices, and servers, among other interdependent information system infrastructures. As technology advances, cyber criminals develop new strategies to attack and infiltrate systems through the introduction of malicious programs or other nefarious activity. Cyber criminals have different motivations of using cyber technology for purposes of self-interest. The fundamental reasons for crafting digital attacks in cyberspace is to commit a terrorist attack or some of the cyberspace attackers are motivated by the need to gain fame. In this context, the curiosity about technological advancement motivates the attackers to test their abilities relative to other developers. However, some groups are inclined to attack government systems in revenge for matters related to political conflicts, personal or national conflicts. Then, all businesses should acknowledge the presence of financially motivated cyber criminals to reinforce their operations. Individuals, businesses, governments, and other organizations must understand the motivations of cyberspace criminals, which are primarily financial, political, and technological, to combat cyber-attacks.

The Problem of Research

Over the past decades there has been an increased report on cybercrime. After careful examination, cybercrimes differ significantly in terms of types and patterns, and as a result, they have dynamics in terms of risk factors and consequences. The consequences of cybercrime are different in the way of perpetuation, victims, and the level of victimization. Therefore, the scope

of attack on the cyberspace varies on the type of crime, pattern of implementation, cause, and effects. Then, cyber criminologists need to improve their research on the causation of crimes on the cyberspace and their effects on the physical space (Payne & Hadzhidimova, 2020). At this digital stage, cybercriminals are becoming more independent, and the use of interdisciplinary approach is the best way to understand their behaviors and victimization in the cyberspace.

The nature of cybercrime indicates that the cyberworld has a crime problem, a business problem, a technological problem, and a hotbed of ethical problems. Importantly, the dynamics of these crimes create a need for the development of a multi-professional approach to understand human behavior related to cybercrime. It is important to acknowledge that the aspect of computer science has a limited scope of understanding the human element in cybercrime, and as a result, they require the help of social scientists (Jacob et al., 2019). Computer science is an analytical discipline that examines computers and the networks they are connected to, taking a technical based approach. It includes the study of data tools, computer science algorithms, software engineering and programming languages. Therefore, the field does not delve into the political, social studies, or the psychological aspects of cybercrime motivations, which fall under sociology, psychology, or political science. The legal aspects of cybercrime are also another consideration as it is also limited in scope. “It is one thing to enact laws that regulate conduct, it is quite another to assert jurisdiction over conduct that may be located or originate anywhere in the world. Cyberspace is a distinct phenomenon, beyond traditional rules based on geographical location” (Appazov, 2014, p. 10). It is important to remember that computer crimes are prosecuted by law rather than being controlled by it.

Indeed, most of the organizations are controlled by traditional cyber criminologists who have limited exposure to technology. Interdisciplinary approach in addressing cybercrime is considered as a premier organization that links technical and social sciences which promotes addressing of cybercrime through empirical research based on knowledge from a wide range of academic disciplines (Payne & Hadzhidimova, 2020). Then, using a multidisciplinary approach in addressing cybercrime would be the most appropriate way to understand the motivation of criminals in all characteristics of human behavior.

The Importance of Interdisciplinary

Organizations and security experts need to understand the attack, the attacker, and the dynamics around them. “All hackers do not think the same way as defenders or in a linear manner. Consequently, defenders need to be interdisciplinary in order to take in account various techniques and combat” (Maalem Lahcen et al., 2020, p. 5). In this sense, understanding changes in the human attitude and behavior is critical. A holistic approach to understanding motivations to cybercrime and creating effective cyber security measures is the one that considers integration of different disciplines. This process creates expert technicians and non-technician professionals who understand how their tasks relate to different subfields. Computer scientists, security engineers, and cybersecurity professionals address technical issues like developing security algorithms, plan and develop secure network systems, and securing devices. In some cases, the human factor is utilized to allow hackers to steal personal data or financial information. Though many businesses are working on installing and instituting state-of-the-art technology to make it more problematic for criminals, humans are still needed at each step of the process for hackers to succeed. As a result, focus on human factors, economic and political aspects would advance

understanding of the nature of the cyber environment. Then, security would be understood because of the attacker dynamics rather than a technological limitation.

Review of Literature

Chng et al. (2022) argues that predicting cybercrime is a challenge since the expansion of cyberspace is associated with the evolution of criminal behaviors. Besides, access to the internet is increasing across the globe, which exposes cyberspace to more criminal minds. According to Chng et al. (2022), most countries are not well equipped with the legal infrastructure to handle cybercrimes. The reason cybercrimes persist is due to their wide distribution of related computer activities, including travel scams, terrorist activities, extortion, health care fraud, and fake escrow scams. Chng et al., (2022) identify people who attack cyberspace as cybercriminals who can be classified as Type I Cyber Criminals, Type II Cyber Criminals, or Type III Cyber Criminals. Type I cyber criminals are politically motivated hobby hackers whose interest is recognition. Type II cyber criminals are hungry for recognition and financially motivated criminals who are, in most cases, associated with organized crime. Type III cyber criminals are former employees and motivated by revenge. They have been disgruntled and, as a result, manipulate organizational systems to disorient their operations.

Technology

Brar & Kumar (2018) argue that cybercriminals are motivated by the desire to test their hacking abilities. Technological advancement continues and creates new opportunities for development. Cybercriminals are knowledgeable about cyber technology, and among them are professionals who lack a chance to showcase their skills due to limited resources or legal restrictions against their activities. These groups interact with different technologies at work, in their social environment, and in their personal lives. Indeed, these criminals are studying cyber

technology in the process of creating advanced systems. In the process, they test the existing technologies for a measure of their capabilities. Then, attacking the information systems is intentional and, as a result, a crime.

Brar and Kumar (2018) reason that the satisfaction and joy of technologically motivated criminals is the fame they receive for their endeavors. For example, a successful attack on something that has never been performed by another attack makes the attacker feel proud. These attackers target many organizations, especially the well-established ones. Krishnan (2020) explains that human curiosity drives them to test and engage with new technological features. As a result, they share malicious messages and malware-laden attachments that are sourced from criminals. The offenders understand how the malware may affect the existing systems, but they are curious to see how they might affect the public. Their influence on the normalcy of computer and internet systems motivates them to create uncertainties in cyberspace. The happiness of such groups is when the community acknowledges the existence of dangerous systems and companies suffer for their underdeveloped programs.

Social media is one of the most widely used cyberspace infrastructures for human and robotic interactions by corporations. People have a high reliance on internet-shared information. Criminals identify the human and technological factors in social media and test them through the introduction of malware. Krishnan (2020) notes that people are ignorant on the social media accounts, for example the ones that suggest, "Keep Me Logged In", which are the main source of Malware if accepted. Criminals understand human behavior and ignorance as they interact with different features. Then, malware is used to test systems and human capabilities, and successful attacks become a source of joy for the criminal.

Finance

Financially motivated criminals act in retaliation for perceived or experienced injustices or conflicts with another party. They have information about the other party and manipulate data to access unauthorized information. At a low level of attack, financially motivated cybercriminals lack information technology knowledge and thus share information with others. These criminals are curious about how they can manipulate an organization's information to have financial gains. Some of them are students or junior employees. Such individuals are hard to identify in the organization since they develop their hacking techniques within the organization. Their promotions and higher rankings in jobs come along with access to more sensitive company information like passwords and code sources.

Kumar et al., (2022) argue that insiders are also financially motivated criminals who abuse access to information to serve their personal interests. They are ex-employees at influential organizations, including managers and senior employees, but are motivated by financial gain and revenge (Atkinson, 2015). Their use of information revolves around testing the malcontents and associating with fraud ideologies, including becoming followers of people with associated crimes. Since they might lack the technological knowhow to use the accessed corporate information, they share the secret with crime facilitators (Richardson et al., 2020). Cybercriminals use the shared information to launch sophisticated attacks that would not be possible otherwise. After a close assessment, cybercriminals and insiders share the psychology of financial motivation, which increases their possibilities of success and causes financial loss to corporations.

There are an increasing number of petty thieves in the social media using nefarious activities to perpetuate crime. These individuals lack deep technical knowledge, but they understand social media psychology (Bruijne et al., 2017). Then, they use simple tools to

increase traffic to their website where they have fake news and motivational stories. In the end, internet users end sharing private information including credit card numbers, which lead them to unbearable financial losses (Conger & Popper, 2020). They have become extreme in the digital age by targeting people with low knowledge and concern on their cyber activities like sharing personal information.

Politics

Politically motivated criminals assume the role of activists who strive to protest against perceived actions and processes taken by the government and corporations. “Although they all use the Internet to break the laws or rules, their internal motivations are not always utterly sinister; actually, some of them firmly believe that their actions are for the greater good” (Pawlicka et al., 2021, p. 843). Edward Snowden used his government systems access to steal information and share it with the public. Snowden believed the U.S. Government surveillance programs were violating the American peoples fundamental right of privacy (Benton, 2015).

According to Shad (2019), attacks on critical infrastructure are the new threat to national security through cybercrime. Terrorist groups motivate the criminals in most cases against the government. The United States has encountered several cases of counterintelligence where entrusted people with critical information use it against the government and its operations (Riikonen, 2019). This problem has created a new perception of foreigners working in influential positions in American organizations. For example, Chinese employees are discriminated against as spies due to the high number of American Chinese employees sharing secret federal information.

Cybercriminals enhance the expansion of international terrorism and organized crime. In the same context, terrorists have diverted their activities to the use of the internet to expand their

decentralized groups. The internet provides an opportunity to share information and transfer credit to the members to perpetuate crime (Casino et al., 2019). These groups create chaos and social unrest in the target country at a low cost and with little time. Cybercriminals use anonymous websites to communicate with other terrorists. These websites are hard to trace and have enhanced the randomization of some terror groups like Jihad in Africa and America. Cybercrime is evolving with technological advancement, so it is imperative to modernize law enforcement system along with it. The cybercrime has become a global threat, and the federal government must arm itself with cutting-edge investigative tools that are flexible enough to catch offenders at a global scale. Gaining more insight into cybercrime will allow prosecutors not only to prosecute offenders in ways that were not previously possible, but also inflict maximum punishment for their crimes by seizing all the assets available.

Conclusion

Cybercriminals have a motivation that is satisfied upon the achievement of their goals that are political, financial, and technological. The problem with developing effective cyber security measures is the limited consideration of human factors in technical operations. Security Engineers, cybersecurity professionals, and computer specialists need social sciences to understand human behavior and how it influences cybercrime. The multidisciplinary approach broadens the understanding of cybercrime by linking technical and human aspects of the cyber environment.

References

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*, 6. https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

Appazov, A. (2014). *Legal Aspects of Cybersecurity*. https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf

Atkinson, S. (2015). Psychology and the hacker–Psychological Incident Handling. *White Paper, SANS Institute*. https://www.semanticscholar.org/paper/Psychology-and-the-hacker-Psychological-Incident-Atkinson/ed03f45d9bf6475ab99123574dd225bbb68c92bf

Benton, B. (2015). The Misinformers: Edward Snowden, Aaron Swartz and The Troubled Relationship Between Hacktivists, Mass Media, and American Government. Www.academia.edu. Retrieved February 27, 2022, from https://www.academia.edu/26547917/The_Misinformers_Edward_Snowden_Aaron_Swartz_and_The_Troubled_Relationship_Between_Hacktivists_Mass_Media_and_American_Government

Brar, H. S., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, *2018*. https://www.hindawi.com/journals/jcnc/2018/1798659/

Bruijne, M. D., Eeten, M. V., Ganan, C. H., & Pieters, W. (2017). Towards a New Cyber Threat Actor Typology. A Hybrid Method for the NCSC Cyber Security Assessment. *Delft University of Technology*. https://repository.wodc.nl/handle/20.500.12832/2299

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, *36*, 55-81. https://www.sciencedirect.com/science/article/pii/S0736585318306324

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Conger, K., & Popper, N. (2020). Florida teenager is charged as 'mastermind'of twitter hack. *The New York Times. https://www. nytimes. com/2020/07/31/technology/twitter-hack-arrest. html*.

Jacob, J., Peters, M., & Yang, T. A. (2019). Interdisciplinary Cybersecurity: Rethinking the Approach and the Process. In *National Cyber Summit* (pp. 61-74). Springer, Cham. https://www.researchgate.net/publication/336033638_Interdisciplinary_Cybersecurity_Rethinking_the_Approach_and_the_Process

Krishnan, S. (2020). Exploitation of Human Trust, Curiosity and Ignorance by Malware. *arXiv preprint arXiv:2002.11805*. https://arxiv.org/pdf/2002.11805.pdf

Kumar, A., Chng, S., Lu, H. Y., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://www.sciencedirect.com/science/article/pii/S245195882200001X

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3(1), 1-18. https://doi.org/10.1186/s42400-020-00050-w

Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology*, *14*(1). doi: 10.5281/zenodo.3741131

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, *27*(2), 23-39. https://files.eric.ed.gov/fulltext/EJ1252710.pdf

Riikonen, A. (2019). Decide, Disrupt, Destroy. *Strategic Studies Quarterly*, *13*(4), 122-145. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-4/Riikonen.pdf

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies*, *39*(1), 1-19. https://www.issi.org.pk/wp-content/uploads/2019/04/1-SS_Muhammad_Riaz_Shad_No-1_2019.pdf

Vernacchia, S. (2018). A practical method of identifying cyberattacks. *PWC Middle East*. https://www.pwc.com/m1/en/publications/documents/wgs-cybersecurity-paper-new-updates.pdf