Criminal Profiling: A Cybercrime Perspective

Name

Institution

Research Paper Outline

The proliferation and growing complexity of online crime is an issue of global significance that has prompted exploration of different counter strategies. This paper seeks to demonstrate the role of criminal profiling as an effective strategy that combines electronic and digital content with psychological aspect of humans to improve efficiency of digital profiling of online offenders. The paper is structured as follows.

1. **Introduction**

Highlight the pertinent issues about cybercrime and criminal profiling in the context of current practices to justify the need for exploration of innovative profiling techniques. The introduction sets the tone of the paper by drawing on relevant literature on the topic to support the thesis statement.

2. **The Complex Concept of Cybercrime**

This sub-section of the paper presents different concepts about cybercrime, including the categories and behaviors of offenders associated to each sub-type of cybercrime. Understanding of cybercrime is crucial to inform knowledge of the characteristic's investigators should look out for during profiling of online offenders.

3. **Important Aspects of Criminal Profiling**

In this section, important factors about criminal profiling are discussed. The strategies that the section emphasizes on are inductive and deductive because they are based on ideological concepts that cover the working mechanisms employed in all other profiling techniques.

4. **Integration of Criminal Profiling and Cybercrime**

This section tries to highlight the areas in which cybercrime and criminal profiling marry. It is intended to develop understanding on how profiling strategies are applied to cybercrime and their effectiveness and efficiency.

5. Conclusion

In this section, important concepts advanced in the paper are revisited.

Criminal Profiling: A Cybercrime Perspective

Introduction

Criminal profiling is a concept whose increasing popularity is attributed to the rise in sophisticated crimes committed in cyberspace. These crimes have rendered the traditional investigative methods ineffective. The current society is increasingly dependent on technology and its offshoots. Smartphones and computers have become mainstays in daily lives of many individuals. There are users who are oblivious to the negative effects of such technologies. One area in which the effects of technology appear subtle is criminology. Griffin (2012) captured the true picture of the current changes in the society in the review of the developments in cybercrime. Griffin (2012) showed that people are striving to make weird accommodations, privacy is violated, and anxiety and fear elevated courtesy of cyber space. The developments are linked to increased vulnerability caused by the dependence on technology. Poonia (2014) observed that there is a category of the society intent on exploiting the power of technology systems to advance criminal objectives. A dramatic rise in instances of offending over the last decade materialized, due to the widespread adoption of electronic media (Griffin, 2012; Nykodym *et al.*, 2005; Kigerl, 2018). The most evident outcome is that criminal investigators face difficulties identifying perpetrators of this new and evolving type of crime. Criminal profiling is a useful technique employed by crime investigators to determine the identity of suspected offenders. However, review of literature on the phenomenon reveals that associated computer forensics, are not well defined to fulfill the role due to reliance on digital or electronic information. Criminal profiling process differs in computer-related investigations, but there are strategies and techniques that investigators can use to profile based on electronic or digital evidence.

The Complex Concept of Cybercrime

The benefits of advancements in technology and the internet remain undisputed. On the other hand, their detriments cannot be ignored because of the adverse social, economic, and political implications. Cyberspace is a platform for limitless opportunities, and criminal have turned it into a lucrative business venture. Online crime is costing individuals and corporations around the world hundreds of billions in dollars every year. Kao and Wang (2009) opined that cyber technology is a highly complicated platform that is preferred by criminals to commit crime. The phenomenon of committing crime online is referred to as cybercrime. Cyber criminals use personal computers and network-linked computers to perpetrate crime. Cyber investigation, which is supposed to combat cybercrime, is in its infancy. However, the proliferated adoption of technology necessitates fast tracking of efforts to improve efficiency of cybercrime investigations. Investigators require comprehensive knowledge of the dynamics of online offending. While details on the type of crime are available, little empirical evidence can be found on the mechanisms used by criminals to perpetrate them. The situation is complicated by the fact that cyber criminals are talented in covering their tracks. The anonymity of the perpetrators of crime in cyberspace reduces the effectiveness of digital and electronic media used as evidence and data to investigate related cases.

Cybercrime is a consequence of the unheralded possibilities and opportunities of cyberspace. Griffin (2012) contended that cyberspace is immune to the antics of man. Business and corporations strive to collect and store data on people, governments use spying software to track and trap offenders, and criminal are taking advantage of the available platforms to inflict suffering on the people. Griffin (2012) compared cyberspace to a parallel universe. The hardware and software involved in cyberspace create a whirl-round context in which webs, clouds, and

superhighways transport volumes of digital information everywhere. The lawless aspect of cyberspace, for instance, its indifference to stealing of data from others, is a major security and privacy issue. For these reasons, cybercrime generates global concerns because it has no spatial limitations. Jahankhani and Al-Nemrat (2012) noted that online offenders use far-reaching techniques, are cunning, and technologically advanced in a way that renders most investigative strategies by authorities unreliable. The challenge lies with all government and private stakeholders to ensure innovative approaches are developed that would enhance the effectiveness of techniques used to profile cyber criminals. Identification of perpetrators of online crime would mark significant progress in fighting this type of growing and highly sophisticated criminal venture.

Cyber criminals tend to share some online characteristics; hence, different criminal profiling strategies are recommended. The strategies, such geographic profiling (Butkovic *et al.*, 2019) and topic clustering (Kigerl, 2018) remain ambiguous because they involve deductions, which may prove difficult in pinning down the crime to a specific offender. Stephenson and Walter (2012) advanced that while the strategies for investigating ordinary crime are well defined, the profiling in those cases is oriented to psychological analysis, whereas the focus should be on criminology. Stephenson and Walter (2012) emphasized on the need to assess cybercrime to determine the different sub-types with the intent of improving investigative efficiency. In some instances, criminal profiling requires the investigating officer to think like the criminal. The assessment of cybercrime conducted by Stephenson and Walter (2012) revealed four distinct sub-types of the offense. The first is the power assertive, which is the most prevalent and is driven by the desire for power and control. The growth in power assertiveness increases the offender’s confidence and aggression, and in some instance, they take credit for

actions that are not theirs. The second sub-type of cybercrime is power reassurance where the offender seeks for power and control through fantasy. The offender projects their fantasy, most often sexual, on the victim and attempts to engage the victim in the illusion. The anger retaliatory sub-type of cybercrime is associated with behaviors that suggest rage. The rage may be directed to a person or organization that has power over the offender or a real symbolic target. The anger excitation type of cybercrime comprises of the smallest group of offenders who draw pleasure from inflicting harm on others. According to Stephenson and Walter (2012), anger excitation is less prevalent in cybercrime because it is difficult to perpetrate sadism online compared to the physical world. The sub-types of cybercrime present a foundational step for digital criminal investigators to base assumptions when creating online profiles for criminals. Understanding the crime intrinsically provides a better chance of successfully profiling the offender.

Important Aspects of Criminal Profiling

Recent evidence suggests that traditional methods used by investigative agencies are growing outdated in combating the complexity of modern crimes, particularly those committed online (Butkovic *et al.*, 2019; Irons & Lallie, 2014). Cybercrimes present significant detection and prosecution challenges than traditional crimes. The difficulties stem from the fact that accepted and sometimes controversial criminal profiling strategies integrated into mainstream investigative theories by authorities have no effectiveness when applied to cybercrime (Stephenson & Walter, 2012). The consensus among researchers in the field is that a paradigm shift to more intelligent methods that can be applied proactively, is timely. Criminal profiling is suggested as the most suitable approach. Criminal profiling is a major field in criminal investigation that seeks to integrate psychology and criminology. In the current dispensation where criminal investigations are reliant on forensics, basing crime on digital or

electronic data appears obscure. Profiling requires investigators to think like criminals and improve their investigative efficiency because computer forensics cannot define the concept of profiling appropriately. Criminal profiling integrates psychology and digital and electronic content to assist in building reliable profiles of suspected offenders. The strategy is crucial in the war against cybercrime where criminals show exceptional levels of evolution in complexity.

Reiterating that computer forensics appear to lack the rigor because its digital and electronic forms lack the dynamism needed to articulate human behavior is necessary. Collection of forensic evidence from the crime scene is a plausible strategy, but investigators risk presenting weak cases for prosecution by relying on such evidence that may be inadmissible in a court of law. The main aim of any criminal investigation is successful prosecution of the suspected offender by relying on concrete evidence that links them to the crime and establishes the motive for the actions committed. Such parameters cannot be generated through physical forensic evidence or computer forensics without integrating the human aspect – the psychological paradigm. According to Warikoo (2014), criminal profiling eliminates loopholes because it does not rely on making educated guesses. Instead, criminal profiling depends on scientific-based methodologies. Similar to investigations of traditional crimes, cybercrime requires profiling using computer based forensics. Some of the strategies used in criminal profiling today are inductive and deductive. In inductive profiling, investigators are exposed to sets of special scenarios from which they are required to conclude a general truth. From the scenarios, investigators are able to recognize a pattern in criminal incidents or behavior of perpetrators and develop a conclusion. In deductive profiling, investigators begin from a general case and work towards a set of supporting evidence. For instance, general characteristics of cyber criminals are identified, then, investigators work to establish examples that support those attributes. Kigerl

(2018) offered an example of topic modeling where suspects are clustered based on textual comments left on digital forums. The evidence is then used to narrow down to a specific case and link the offender to the crime. However, scholars in the field of criminal profiling contend that owing to the complex nature of cybercrime, a single strategy may proof ineffective. White *et al.* (2014) advocated for a hybrid profiling model that integrates inductive and deductive frameworks to achieve efficiency and reliability.

The argument advanced by observers in the field of criminology is that the evolution in crime requires a similar development in counter measures. The early principles of community policing and monitoring of criminals' communication networks are no longer viable in the modern context predominated by technology. In cyberspace, criminal create virtual identities that gives their criminal activities heightened anonymity (Kigerl, 2018; Jahankhani & Al-Nemrat, 201). The need for new criminal profiling strategies is evident in Hildebrandt (2008) where the primary functions of thee process are highlighted. In simpler terms, profiling is a pattern recognition process that is crucial in discrimination of noise from information based on constructed knowledge. Criminal profiling in cybercrime is necessary to facilitate dealing with copious sophisticated data from the shift to technology. Nevertheless, reliance solely on computer forensic data makes automated profiling inefficient when applied on its own. Machine profiling needs to be complimented by human profiling to integrate the psychological aspect of criminology for reliable results. Through profiling, law enforcement agencies acquire the knowledge they need to categorize and deal with criminal, aiding preemption of crime, arrests, and successful prosecution.

Integration of Criminal Profiling and Cybercrime

Films and television shows tend to depict regimes in forensic science and criminal investigation analysis as highly efficient (White *et al.*, 2011). Investigators use these profiling strategies to track and arrest serial criminals and perpetrators of different crimes. A significant proportion of the films and shows tend to be fictitious and disputed. They are a reflection of the major breakthroughs made in the fields of psychology and criminal over the past several decades. The law enforcement agencies utilized the strategies to capture many serial criminals by focusing attention on specific suspects (White *et al.*, 2011). Through criminal profiling, it is possible to create a bio-profile of a suspect by using forensic and digital evidence from the crime scene and other related cases. Criminal profilers use the evidences to try to piece together the psychological profile of the suspect through identification of their habits, behavior, motives, interests, and background. These factors are then used to link the suspected offender to the crime by integrating supportive physical or digital forensic evidence. However, White *et al.* (2011) observed that most of the forensic science strategies used in profiling focus of conviction of the perpetrator rather than their identification. Arrests are aided by information contributed by the public and victims of the crime incidents used to piece together important characteristics of the crime and the offender.

Cyberspace is the fastest developing platform worldwide, and with it, cybercrime has become the leading global business industry costing an estimated US$200 billion annually to individuals and organizations (Hildebrandt, 2008). The costs grew substantially over the years, prompting increase in calls for new strategies of combatting online crime. Consequently, cybercrime and computer forensics have become two inseparable discourses. Criminal profiling is being introduced into the foray to aid investigative agencies' efforts to prevent cybercrime and

prosecute perpetrators. Ineffectiveness of traditional techniques used by investigators is not a secret. Colombini and Colella (2011) noted that the disconnect between the current techniques used by investigative agencies is a cause for concern. Cracking cybercrime is dependent on timely results, which is made difficult by the existence of time and resource limitations. Digital investigators face computational and human challenges in resolving cybercrime. Through criminal profiling, they can adopt a proactive approach with the potential to improve the efficiency of the process.

A computer forensics approach is an indispensable element of the fight against cybercrime. Digital criminal profiling is taking the center stage in addressing cybercrime because it aids bot inductive and deductive processes. According to Colombini and Colella (2011), computer forensics allows digital profilers to make use of the abundant forms of electronic and digital evidence, a phenomenon associated with cybercrime. The objective is to establish indicators and evidence that are integral in identification of perpetrator of crime. Investigators must conduct correct analyses of log files and data in the computer system to understand criminal behavior and actions. The goal is to solve the puzzle of identifying the perpetrator, particularly in cybercrime where criminals' identities remain anonymous. Unlike in traditional criminal profiling where the profile of the suspect is created using physical evidence such as DNA, blood sample, or personal objects, digital profiling assumes a more sophisticated approach. Cyber criminals are adept at hiding their tracks, which makes it difficult for investigative officers. However, with the availability of substantial intelligence data from past crimes, it is possible to draw on analytical methodologies to generate compatible user digital profiles by integrating evidence left on the system – commonly referred to as digital footprint (Colombini & Colella, 2011). The nature of cybercrime may vary depending on the perpetrator

and the target victim, but the difficulty in profiling stems from the ability to exploit technology to mask the identity and actions of criminals.

Digital criminal profiling relies on the assumption that perpetrators of crime in cyberspace can have a specific outline. Nykodym *et al.* (2005) noted that the assumption draws controversy for lack of authenticity, but highlight some truthful aspects about cybercriminals haring certain distinguishing characteristics. The observation is important in that the common attributes can be used to create an outline for a suspect even in cases where the crime is different. Evidence related to the crime in question can be fed into the computer system to obtain a comprehensive outlook of the suspect. However, a new paradigm of criminal profiling relies more on intuition than past approaches of available records of crime.

Investigators can build a profile for a suspected criminal by relying on Brent Turvey's behavioral evidence analysis. According to Nykodym *et al.* (2005), Turvey developed four steps within two phases for conduction of behavioral evidence analysis. The first step is the equivocal forensic analysis where the evidence is evaluated despite its ambiguous significance. The investigator relies on the diverse computer systems and databases to collect data and use it to interpret its most probable meaning. The second step, victimology, assesses the victim. Profiling the victim of crime can yield useful insight for pinning down the perpetrator. There is a tendency of criminal to target victims with certain attributes, hence, a profiler can use victim characteristics to determine offender characteristics. The third step of Turvey's model is the crime scene characteristics, which refers to the outstanding features that can be drawn from the perpetrator's behavioral decisions in relation to the victim and the location of the crime. In cybercrime, the IP address plays an important role in profiling for time and location (Kao & Wang, 2009). These factors have a meaning to the offender, and profilers seek to establish such.

Overall, the third step of behavioral evidence analysis uses characteristics of the crime scene to establish the offender's profile. The fourth and last step of the model is offender characteristics. In this step, the profiler makes assumptions about the perpetrator's personality and behavioral characteristics.

Collected information provides useful insights in building the offender's profile. Nykodym *et al.* (2005) noted that employing Turvey's behavioral evidence analysis model can increase or reduce the number of suspects. This means it may be ineffective in narrowing down on the likely offender in contexts such as cyberspace where criminals share a number of characteristics. However, the profile built using the steps can be instrumental during the investigative and trials phase of the criminal justice process. Turvey's framework depicts the wide scope covered by investigators when collecting data for criminal profiling. The model proves to be reliable for investigating cybercrime where criminal have anonymous identities and proximity to the victim may not be a determinant factor.

Conclusion

The global society's adoption of technology proliferated over the last two decades. Today, many aspects of an average person's life revolve around daily use of technology, with the internet playing an integral part. Cyberspace generates substantial benefits for individuals and organizations, but some people have found it to be a niche suitable for advancing criminal acts. The dependence on technology increases vulnerability to cybercrime acts. The consensus among scholars in the field of criminology is that due to the complexity of cybercrime, traditional investigative methods prove to be inefficient. Consequently, they advance the need for an integrated approach that would yield the required efficiency.

Criminal profiling is the most promising approach to combatting cybercrime because it integrates electronic and digital data with psychological analysis to determine the propensity and the motive of offending. This is a critical process because of the complexity of cybercrimes and the tendency of online offenders to be anonymous. The process entails analysis of the different types of cybercrime, with the objective to establish specific stereotypes associated with cyber criminals. Therefore, criminal profiling represents a field with the potential to contribute arrest and prosecution of cyber criminals, a development that would have immense social and economic benefits given the current high prevalence of cybercrime. Criminologists face the challenge of researching on the suitability of different criminal profiling strategies to establish applicability to different sub-types of cybercrime. In addition, investigative personnel in law enforcement agencies must receive training on integration of computer forensics and psychology in criminal profiling. Substantial gaps in criminal profiling exist because of the ever-evolving nature of cybercrime. These gaps need to be addressed using, proven, efficient, and proactive criminal profiling strategies.

References

Butkovic, A., Mrdovic, S., Uludag, S., & Tanovic, A. (2019). Geographic profiling for serial cybercrime investigation. *Digital Investigation*, *28*, 176-182.

Colombini, C., & Colella, A. (2011, August). Digital profiling: A computer forensics approach. In *International Conference on Availability, Reliability, and Security* (pp. 330-343). Springer, Berlin, Heidelberg.

Griffin, R. C. (2012). Cybercrime. *J. Int'l Com. L. & Tech.*, *7*, 136.

Hildebrandt, M. (2008). Defining profiling: a new type of knowledge? In *Profiling the European citizen* (pp. 17-45). Springer, Dordrecht.

Irons, A., & Lallie, H. (2014). Digital forensics to intelligent forensics. *Future Internet*, *6*(3), 584-596.

Jahankhani, H., & Al-Nemrat, A. (2012). Examination of cyber-criminal behaviour. *International Journal of Information Science and Management (IJISM)*, 41-48.

Kao, D. Y., & Wang, S. J. (2009). The IP address and time in cyber-crime investigation. *Policing: an international Journal of Police strategies & Management*, *32*(2), 194-208.

Kigerl, A. (2018). Profiling cybercriminals: Topic model clustering of carding forum member comment histories. *Social Science Computer Review*, *36*(5), 591-609.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cybercrime. *Computer Law & Security Review*, *21*(5), 408-414.

Poonia, A. S. (2014). Managing digital evidences for cyber-crime investigation. *International Journal of Advanced Studies in Computers, Science and Engineering*, *3*(11), 22.

Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers & Security*, *22*(4), 292-298.

Stephenson, P., & Walter, R. (2012, January). Cyber-crime assessment. In *2012 45th Hawaii International Conference on System Sciences* (pp. 5404-5413). IEEE.

Warikoo, A. (2014). Proposed methodology for cyber-criminal profiling. *Information Security Journal: A Global Perspective*, *23*(4-6), 172-178.

White, J. H., Lester, D., Gentile, M., & Rosenbleeth, J. (2011). The utilization of forensic science and criminal profiling for capturing serial killers. *Forensic science international*, *209*(1-3), 160-165.