IMPEDIMENTS AGAINST CYBERCRIME INVESTIGATION IN YENAGOA: THE DETECTIVE PERSPECTIVE

Godslight Thomas SESE
Department of Cybersecurity, Faculty of Science
Federal University Otuoke, Bayelsa State Nigeria
https://orchid.org/0009-0004-3497-063
sesegodslight@yahoo.com
+2348069659313

Zibokifi Racheal Ghandi OLUMANI
Department of Sociology and Anthropology (Criminology and Security Studies)
Federal University Otuoke, Bayelsa State Nigeria
olumanizr@fuotuoke.edu.ng
+2348069404979

Abstract

The integration of technology in human daily endeavours has kept the word cybercrime on the lips of practically everyone. As the level of technological dependency increases due to unsatisfiable human needs, cybercrime has also gained global popularity. Thus, it has become a topic for discuss amongst individuals, corporate groups, nation states and international organizations and agencies. With continuous dependence on technological advancement, cybercriminals adopt advanced methods of exploiting system vulnerabilities, increasing the landscape of cyber threat in a sophisticated manner. Therefore, making it cumbersome and cost effective for law enforcement agencies to identify, trace, apprehend, convict and prosecute cybercriminals. The intent of this paper is to explore the various methods and patterns of cybercrime investigation and the impediments against successive convictions and prosecutions of cybercriminals by detectives in Yenagoa. Qualitative research method is employed while thematic analysis is utilized for data analysis. The study delves the two general categories of cybercrime investigation as digital forensics and open-source intelligence while both internal and external challenges were spotted as impediments. Internal issues highlighted a lack of logistics support, limited access to advanced technological resources, inadequate specialized training etc. External hurdles encompass victim non-cooperation, the anonymous nature of criminals, insignificant collaboration with other sister agencies, and the

complex nature of collecting and preserving digital evidence admissible in court, among other factors. The paper concludes with recommendations to tackle the challenges that impede apprehension, conviction and prosecution of cybercriminals in the cause of cybercrime investigation.

Keywords: *Cybercrime, Cybercrime Investigation, Open-source Intelligence, Detective*

Introduction

The growth of technology has both facilitated and impeded the investigation of crime, especially those crimes involving the use of computers and telecommunications. Sheer quantity of information creates considerable problems for investigators who sometimes have to examine gigabytes of data and break encryption codes before the material they are interested in can be discovered.

Nowadays, cybercrime is fast growing. The rate at which criminals are exploiting the speed, ease and most importantly the anonymity of the internet to perpetrate a diverse range of criminal activities is alarming. These criminal activities are virtual. It has no border restrictions. The network of cybercriminals consists of criminal organizations working with criminally minded technology professionals. Highly sophisticated, these cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale. (Grigor, 2022).

Criminal organizations are turning increasingly to the Internet to facilitate their activities and maximize their takings in the shortest time. The crimes such as ATM theft, SIM swap, Phishing, DOS attack social engineering among others, are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging. (Carr Ritz, 2023). As the internet offers near-total anonymity, it is difficult to discern the identity, the motives, and the location of a cybercriminal. The global connectivity of the internet makes it much easier for the criminals to act beyond national boundaries to conduct their illegal affairs. It also makes it possible for existing criminal organization to use more sophisticated techniques to support and develop networks for their activities. Thus, creating challenges for cybercrime detectives. (Grigor, 2022).

The growth of electronic commerce offers rich picking for criminals who are prepared to undertake fraudulent activities such as identity theft, misrepresented business opportunities and franchises, work at home schemes and credit card swindles. A cybercriminal is therefore, any person who knowingly or intentionally and without permission access or caused to be accessed any computer,

computer system or network. The Nigeria Cybercrime Act listed cyber offences as follows: offences against critical infrastructures; unlawful access to a computer; system interference; intercepting electronic messages; mails and money transfers; computer related forgery; computer related fraud; theft of electronic devices; unauthorized modification of computer system, network and data; cyber terrorism; identity theft and impersonation; child pornography and related offences, cyber stalking, cyber squatting, racist and xenophobic offences, manipulation of ATMs/POS terminal, phishing and spamming, spreading of computer virus and electronic cards related frauds among other. (Nigeria Cybercrime Act of 2024 as amended)

Cybercrime is often transnational in character; offenders take advantage of gaps in existing law to avoid conviction and prosecution. It is, therefore, important that every legal system take measures to ensure that its procedural law is adequate to meet the challenges posed by cybercrimes.In order to examine the prospects and the challenges in the investigation and prosecution of cybercrimes in Yenagoa, this article will focus on the challenges detectives encountered during cybercrime investigation. (Abu & Israt, 2020).

As computing science advances, its' technology has revolutionized the way crimes are committed. Detectives, who are trained traditionally to investigate physical crimes, now face the daunting task of navigating the complex and dynamic world of cybercrime. This paper aims to highlight the main impediments faced by detectives during cybercrime investigations. Detectives, who are typically trained to handle traditional crimes, face multiple impediments when investigating cybercrimes. The digital environment presents unique challenges that require specialized technical expertise, access to advanced investigative tools, and cross-border collaboration. In Nigeria, these challenges are compounded by limited resources and infrastructural deficits. Furthermore, the rapidly evolving tactics of cybercriminals, combined with a lack of cooperation from the private sector and underreporting by victims, significantly impair investigative efforts. (Dattatray, 2019)

This paper examines the primary impediments that hinder cybercrime investigation from the perspective of detectives operating in Yenagoa, Bayelsa State. It highlights the systemic, institutional, legal, and technological barriers they face and provides recommendations for addressing these challenges to enhance national cybersecurity and improve law enforcement outcomes.

Cybercrime Investigation

The process of identifying, analyzing, and responding to illegal activities conducted within the ambit of the cyberspace with the aid of digital devices and networks. (Makeri, 2017). It aims to expose the

anonymity of cybercriminals, collect and preserve evidence, and ensure perpetrators are prosecuted in accordance to the law.

Typologies of Cybercrime Investigation

Below are the different types of cybercrime investigation

19. **Digital Forensics:** This has to do with the recovering, analyzing, and preserving of evidence from computers, servers, networks, and storage devices to support legal proceedings.
20. **Cyber Threat Intelligence:** Is the act of carrying out cyber threat survey, understand the nature of the threats identified, attack, and the attacker's behaviour. This can be done through open-source intelligence analysis.
21. **Network Forensics:** Involves monitoring packets, and analyzing network traffic to detect intrusion, data breaches, or malicious activities.
22. **Cyber Fraud Investigation:** Refers to the sleuthing of crimes such as Point of Sale (POS) fraud, phishing, identity theft, credit card fraud, and other financial crimes executed by cybercriminals within and outside social media platforms. (Rukhsana, 2024)
23. **Malware and Virus Analysis:** Investigates malicious software, such as viruses, worms, ransom ware, and spyware, to understand their origin, behaviors, and impacts on individuals and organizations.
24. **Cyber Espionage and State-Sponsored Attacks:** It involves nation-state cyber activities, cyber hacktivism, cyber terrorism, espionage, and hacking, targeting governments' critical infrastructure.
25. **Online Sextortion:** Identify and apprehend offenders involved in producing, distributing, or possessing exploitative sexual contents (still or motion images) for financial gains, deformation, revenge and gratifications.
26. **Intellectual Property Crime:** Investigates plagiarism, piracy, counterfeiting, and illegal possession and distribution of copyright content.
27. **Online Harassment and Bullying:** Deals with the investigation of online threats, harassment, and bullying cases. This process identifies perpetrators and provides support for the victimized.
28. **Social Engineering Investigation:** Focuses on scams that trick individuals or organizations into revealing sensitive information.
29. **Incident Response and Threat Hunting:** Involves managing cybersecurity incidents, preventing future attacks, and proactively searching for threats within systems.

Theoretical Framework

Routine Activity Theory (RAT) is an environmental place-based explanation of crime which emphases on its relation to space and time. Cohen and Felson, (1979) in a bid to provide explanation for why crime occurs propounded this theory with its main assumption that crime occurs when three elements converge in time and space, the presence of all three elements increases the likelihood of criminality while the absence of these elements might reduce the chances of criminality. For Cohen and Felson (1979), these three elements are a suitable target, lack of a capable guardianship, and a likely motivated offender. A Suitable Target: Without the presence of a suitable target, the commission of crime is almost impossible. In this sense, a target can be anything; it could be a person, an object or a property, which can be attractive and fruitful for criminals. In other words, a suitable target is something, which provides instant profit to offenders. This might be a poorly secured cyber space, online data where a possible offender can see suitable targets (monetary gain, social class etc.). Motivated Offender: The potential offender gets motivated by the presence of suitable target(s) in this case a motivated offender is the cybercriminal (motivated offender encountering a suitable target increases the likelihood of cybercrime). Absence of Capable Guardian: The third element is the absence of guardianship (security agents, properly secured cyber data). Cybercrime victimization reduces with the presence of capable guardianship. In examining the routine activity theory in the parameters of cybercrime occurrence it aligns with the struggles and impediments faced by the detectives, as week guardianship in this case inadequate cybersecurity protocols, detectives lack of specialized technical knowledge required to investigate cybercrimes effectively creates a thriving environment for cybercrimes.

Result

In the course of this research, the following was uncovered.

1) **Anonymity:** Cybercriminals exploit various tools to maintain anonymity, including Virtual Private Networks (VPNs), proxies, and the dark web. These technologies make it difficult to attribute crimes to specific individuals. Detectives often face challenges in distinguishing between true perpetrators and compromised systems being used as proxies. These technologies make it difficult to attribute crimes to specific individuals. The lack of sophisticated tracking tools within Nigerian law enforcement makes this issue particularly pressing.
2) **Lacks in Technological Expertise and Training:** Most detectives lack the specialized technical knowledge required to investigate cybercrimes effectively. The rapid pace of technological change further exacerbates this issue, creating a continuous need for updated

training and education. Limited access to digital forensic tools and insufficient training budgets contribute to this impediment. In Nigeria, limited funding for police training and the absence of dedicated cyber units in some regions leave officers ill-equipped to handle digital investigations. Additionally, the scarcity of trained forensic analysts and cybersecurity professionals within the police force hampers progress.

3) **Evidence Collection and Preservation Procedures:** Digital evidence is inherently volatile and can be easily altered or destroyed. Detectives must ensure proper handling to maintain the chain of custody and admissibility in court. However, encryption, cloud storage, and data fragmentation complicate evidence collection. Additionally, suspects may use anti-forensic tools to hinder investigations. Nigerian law enforcement agencies often lack the technical resources and standardized procedures required to manage digital evidence effectively. The absence of specialized forensic labs in some regions further limits investigative capacity.
4) **Inadequate Resource Allocations:** Cybercrime units are often under-resourced, lacking both personnel and technological infrastructure. Investigations require expensive software, hardware, and skilled analysts. Time constraints further hinder the ability to thoroughly investigate complex cyber incidents. In Nigeria, economic constraints and competing national priorities often result in limited budget allocations for cybercrime enforcement. This leaves detectives with outdated equipment, limited internet access, and inadequate support services, all of which hinder the ability to investigate cybercrimes thoroughly.
5) **Evolving Nature of Cyber Threats:** Cybercriminals constantly adapt their tactics to evade detection. The use of artificial intelligence, zero-day exploits, and Advanced Persistent Threats (APTs) makes it difficult for detectives to stay ahead. Traditional investigative methods are often inadequate against these sophisticated attacks. Cybercriminals constantly adapt their tactics to evade detection. The use of artificial intelligence, zero-day exploits, social engineering, and advanced persistent threats (APTs) makes it difficult for detectives to stay ahead. Traditional investigative methods are often inadequate against these sophisticated attacks. Nigerian detectives are particularly vulnerable due to a lack of continuous professional development opportunities and insufficient intelligence-sharing mechanisms.
6) **Gap in Cooperation with the Private Sector:** Detectives often rely on data held by private companies, such as internet service providers and social media platforms. However, concerns about customer privacy, reputational risk, and lack of clear protocols can result in delays or refusals to share critical information. This lack of collaboration can stall investigations and limit the available evidence. In Nigeria, weak public-private partnerships and unclear legal obligations often lead to minimal cooperation, this in turn limits access to key evidence.

7) **Victim Reluctance in Reporting:** Many victims of cybercrime do not report incidents due to fear of reputational harm, financial repercussions, or lack of faith in law enforcement. These underreporting limits the scope of investigations and hinders the ability to identify broader cybercrime trends. In Nigeria, cultural attitudes, stigma, and mistrust in the criminal justice system contribute to significant underreporting. This reduces the pool of data available for analysis and pattern detection and hinders broader prevention and enforcement strategies.
8) **Jurisdictional Challenges:** One of the most significant obstacles in cybercrime investigation is jurisdiction. Cybercriminals often operate across national borders, using international networks to obscure their identities and locations. This makes it difficult for detectives to collect evidence, track suspects, and secure prosecutions. Mutual Legal Assistance Treaties (MLATs) and international collaboration are often slow and cumbersome, impeding the timely progress of investigations. In Nigeria, where bureaucratic delays and weak interagency coordination are common, these issues are further exacerbated.
9) **Inadequate Legal Frameworks:** Many legal systems have not kept pace with technological advancements. In Nigeria, while laws such as the Cybercrimes (Prohibition, Prevention, etc.) Act 2024 as amended exist, they are often not comprehensive or detailed enough to address the nuances of emerging cyber threats. Additionally, poor implementation, lack of prosecutorial expertise, and delays in judicial processes undermine the enforcement of cyber laws. Detectives may encounter difficulties in obtaining warrants or accessing digital evidence due to these legal constraints.

Conclusion

Cybercrime investigation poses numerous challenges for detectives in Nigeria, stemming from the complex and transnational nature of digital crimes. Addressing these impediments requires a multifaceted approach, including enhanced international cooperation, improved training and resources for law enforcement, updates to legal frameworks, and stronger partnerships with the private sector. Institutional reforms, investment in technology, and public awareness campaigns are also essential. By acknowledging and addressing these challenges, Nigeria can strengthen its cybercrime response mechanisms and better protect its digital economy and citizens.

Cybercrime investigation poses numerous challenges for detectives, stemming from the inherently complex and global nature of digital crime. Addressing these impediments requires a multifaceted approach, including enhanced international cooperation, improved training and resources for law enforcement, updates to legal frameworks, and stronger partnerships with the private sector. By

acknowledging and mitigating these obstacles, society can better equip detectives to combat the growing threat of cybercrime.

Cybercrime investigation is a complex, multidisciplinary field requiring technical expertise, legal knowledge, and analytical skills. It is vital in mitigating the impact of cyber threats and ensuring the security of digital environments.

Recommendations

Security and law enforcement agents should be regularly trained on cybercrime and digital forensics to keep them updated on cybercrime investigations. Properly equip law enforcement agents and their offices with modern devices necessary for tracking and investigating cybercriminals. Create awareness on cybercrime and cybersecurity among the general public. Encourage collaboration between law enforcement agents, corporate organizations, ICT companies/Internet Service Providers and Cybercrime/Cybersecurity Experts to effectively tackle cybercrime offenses.

References

Abu T. M. A. & Israt J. (2020). Challenges of Cyber Policing in Response of Cybercrime to Reduce Victimization. *International Journal of Research and Innovation in Social Science. 4(5), May 2020. ISSN 2454-6186*. www.rsisinternational.org.

Cohen, L. E. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review 44: 588–608.*

Cybercrimes (Prohibition, Prevention etc) Act 2015 with Amendment Act of 2024. www.cert.gov.ng.

Dattatray Bhagwan Dhainje (2019). Cyber-crime Investigations Issues and Challenges. *International Journal of Law. 5(6), November 2019, Page No. 129-134.*www.lawjournals.org

Grigor Khachatryan (2022). Analysis of Cybercrime Investigation Problems in the Cloud Environment. IJCSNS. *International Journal of Computer Science and Network Security, VOL.22 No.7, July 2022*. https://doi.org/10.22937/IJCSNS.2022.22.7.38

Carr Ritz (2023). "Some Legal and Practical Challenges in the Investigation of Cybercrime". *Cybersecurity Undergraduate Research1*. https://digitalcommons.odu.edu/covacciundergraduateresearch/2023spring/projects/1

Makeri, Y. A. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering, 7(4), 315 – 321.*https://doi.org/10.23956/ijarcsse/v6i12/01204.

Rukhsana Siddiqua, (2024) "Challenges Faced by Police Officers in Investigating Cyber Crime: An Exploratory Study in Bangladesh" *International Journal of Humanities Social Sciences and Education (IJHSSE), volume 11, no. 7, 2024, pp. 150-160.* DOI: https://doi.org/10.20431/2349- 0381.1107014.www.arcjournals.org.