



**LEVERAGING ROUTINE ACTIVITY THEORY FOR CYBERCRIME PREVENTION
IN NIGERIA: STRENGTHENING CYBER SECURITY ENFORCEMENT THROUGH
DIGITAL SURVEILLANCE TECHNOLOGIES**

By

ADEOYE, K.T, AKINDE, O.A & OLUWANIYI, J.I

Department of Crime management, The Federal Polytechnic, Ilaro

kowiat.ayanwale@federalpolyilaro.edu.ng; gbolaazadus1234@gmail.com;

john.oluwaniyi@federalpolyilaro.edu.ng

Abstract

Cybercrime has also become a serious concern in Nigeria, fueled by increased online transactions, weak cybersecurity enforcement, and evolving cyber threats. Even with the enactment of the Cybercrime (Prohibition, Prevention, etc.) Act of 2015, cybercriminals exploit technology vulnerabilities, outdated digital forensics, and underdeveloped law enforcement activities. This study investigates the prospects of digital surveillance technologies in strengthening cybersecurity enforcement and reducing cybercrime incidents in Nigeria. The study uses Routine Activity Theory (RAT) to test how threat detection using AI, real-time monitoring, and predictive analytics prevent cybercrime. Findings show that improved cybersecurity policy, in tandem with other agencies, and investments in advanced digital surveillance tools have the potential to curb cyber threats significantly. To further lower threats from financial fraud, identity theft, and ransomware attacks, greater public awareness and more stringent cybersecurity regulations are necessary. By utilizing digital surveillance technologies, Nigeria is able to create a stronger cybersecurity system and make digital interactions more secure for citizens, enterprises, and government agencies.

Keywords: Cybercrime, cybersecurity enforcement, digital surveillance, Routine Activity Theory, Nigeria.

Introduction

Cybercrime is a significant security challenge in Nigeria. The problem is compounded by rising digital transactions and new threats. In spite of the Cybercrime Act of 2015, cybercriminals take advantage of lax enforcement, outdated forensics, and gaps in regulations (Makanjuola & Ayantunji, 2024). Nigeria's cybersecurity is beset with tardy response to threats, poor infrastructure, and poor skilled manpower (Chinedu et al., 2021). Even though the National Cybersecurity Policy was updated in 2021, cybercrime perpetrators are still exploiting weak monitoring and enforcement systems (Ishiguo, 2024).

Literature supports that we need AI-powered surveillance, biometric authentication, and machine learning for improved cyber security (Phillips et al., 2023). Surveillance systems like CCTV and digital forensic can avert cyber threats but fail to do so because of poor investment in digital infrastructure (Olayemi, 2014; Sule et al., 2023). Inadequate law enforcement, poor regulation, and low awareness about cybersecurity worsen the situation (Obidimma & Ishiguzo, 2023).

The Nigerian government is conscious of the role of digital surveillance but is beset by budget constraints, policy lacunae, and privacy concerns (Ezeji, 2024). Law enforcement agencies rely on outdated investigation techniques, making cybercrime tracing futile (Phillips et al., 2023). Cross-border cybercrime complicates matters, demanding international collaboration (Nwafor, 2024). Disjointed cybersecurity enforcement among agencies like the EFCC, NCC, and ONSA also restricts intelligence sharing and proactive cyber defense activities (Chinedu et al., 2021).

Surmounting these issues entails fusing AI-powered cybersecurity solutions, real-time monitoring, and increased regulatory compliance between the financial sector and telecoms (Bello & Griffiths, 2021). The expansion of inter-agency collaboration, cybersecurity awareness, and law enforcement capabilities in digital forensics is essential to repelling cyber threats and safeguarding Nigeria's digital economy (Bulama & Shrivastava, 2023).

Routine Activity Theory (RAT) provides us with insights into cybercrime patterns in Nigeria by examining the connection between those who desire to commit crimes, vulnerable targets, and poor protection. Cybercrime perpetrators exploit technology issues and poor law enforcement to carry out fraud, identity theft, and cyberattacks (Akindipe & Akilla, 2024). Enhancing cybersecurity enforcement using AI-based surveillance, blockchain protection, and live threat detection can build robust protection to counteract cybercrime. Law enforcement agencies are challenged because they lack adequate tools and skills in digital forensics and data policing (Amali, 2024). Strengthening cyber security through predictive analytics, inter-agency coordination, and legislative amendments will close avenues for crime and protect businesses and national infrastructure. Harmonizing cybersecurity policies with RAT principles will strengthen Nigeria's ability to fight digital crimes and secure cyberspace.

Research Objectives

1. To assess the applicability of Routine Activity Theory (RAT) in analyzing trends of cybercrime in Nigeria and its usefulness in framing cyber security enforcement policies.
2. To evaluate the efficacy of online surveillance technologies in strengthening cyber security enforcement and reducing instances of cybercrime in Nigeria.

Theoretical Review

Routine Activity Theory

Proponent: Routine Activity Theory (RAT), developed by Lawrence Cohen and Marcus Felson in 1979, describes crime as situational and environmental and not just individual motivation. The theory holds that crime occurs when motivated offender, suitable target, and absence of effective guardian coincide in space and time. In accentuating the prospects for criminalization rather than depth of criminal motive, RAT presents a valuable paradigm to explain how cybercrime can develop in areas like Nigeria's largest cities Lagos, Abuja, and Port Harcourt where electronic payments are common and web-based criminal action is on the rise.

Assumption: The premise of the theory is that crime is opportunity-based and fueled by routine activities that place people and organizations at risk of victimization. As technology continues to transform society, novel opportunities for crime arise and contribute to crime waves. In Nigeria, the country's rapid growth of the digital economy, which has seen greater internet penetration, online banking, cryptocurrency trading, and social media interaction, has provided a fertile ground for cybercrime to flourish. The implication that crime rates are created by the routine activities can be observed in the manner cybercriminals target financial users online with no proper security.

Application: Use of RAT for cybercrime prevention in Nigeria involves using internet monitoring and artificial intelligence-driven cybersecurity to enhance enforcement. Machine learning can be used for real-time tracking of money transactions for the prevention of threats and fraud, especially in Lagos. Financial organizations can stop suspect transactions before execution, securing customer details using predictive analytics. Public sensitization is required because social engineering attacks individuals' weaknesses. Cybersecurity awareness campaigns on secure internet use, multi-factor authentication, and phishing identification can minimize threats. Lagos, Ogun, and Abuja organizations must incorporate cybersecurity training during onboarding to avoid

breaches. Regulatory agencies such as the CBN and NCC must impose stringent compliance on financial institutions and telecoms, requiring encryption, biometric verification, and fraud detection. Government-private sector partnerships and international cybersecurity alliances can enhance Nigeria's cybercrime fight.

Methodology

Research Design

This study adopts a qualitative research design based on secondary data sources to examine the role of digital surveillance technologies in supporting cybersecurity enforcement and suppressing cybercrime cases in Nigeria. The study is exploratory and draws upon academic literature, government reports, cybersecurity policy reports, and empirical studies to critique trends in cybercrime and establish the effectiveness of digital surveillance technologies in Nigeria.

The Effects of Digital Surveillance Technologies on Prevention of Cybercrime

Digital surveillance technologies actively monitor, prevent, and reduce cyber attacks. Artificial intelligence (AI) tools optimize the capability of law enforcement agencies to observe digital activity and pinpoint cybercrime patterns (Nsude et al., 2023). These platforms process massive amounts of data in order to find discrepancies, thereby enabling authorities to implement preventive measures. Organizations such as the EFCC employ digital surveillance to trace fictitious transactions and cyber crime operations.

Machine learning and artificial intelligence-driven surveillance foresees cyberattacks by analyzing behavior. Predictive analytics in banks is also highlighted by Adedoyin (2023) as a tool to detect illegal transactions and fight fraud. Many Nigerian banks currently use AI-driven fraud protection software that scans accounts in real-time, automatically blocking suspicious transactions.

Digital surveillance also supports cybersecurity law enforcement. While the Cybercrime Act of 2015 provides a legal framework, it is hindered by inefficient monitoring systems (Okoru & Oluku, 2024). Real-time surveillance supports efficient enforcement by tracking cybercriminal activities,

gathering evidence, and aiding prosecutions. Blockchain integration also supports secure financial transactions, increasing transparency and eradicating cyber fraud (Osazuwa et al., 2024).

Enhancing Cybersecurity Enforcement with Digital Surveillance

Surveillance technologies support national cybersecurity via real-time observation, threat detection, and rapid response. With cybercrime syndicates becoming more advanced, security agencies must use sophisticated surveillance to track networks and dismantle scam networks. Manasseh and Ede (2024) observe that the inclusion of surveillance in cybersecurity systems enhances the effectiveness of law enforcement. Facial recognition, biometric authentication, and forensic analysis of data increase verification of identities, inhibiting fraud and unauthorized access (Obidimma & Ishiguzo, 2023). Nigeria's financial sector has adopted biometric authentication, reducing identity theft and unauthorized withdrawals. Surveillance also assists in prosecuting cybercrime by providing electronic evidence. Adisa (2023) stresses the digital forensics aspect of enforcing cybersecurity, keeping extensive data trails that strengthen court cases against the offenders.

Challenges and Recommendations for Improving Cybersecurity Through Digital Surveillance

Though digital surveillance has advantages, poor infrastructure and a gap in cybersecurity skills, as well as poor enforcement of policies, is what holds Nigeria back. Okibe (2024) points out that even with cybersecurity policies, their enforcement is poor due to limited government investment in digital surveillance. Limited finances push most organizations to resort to using outdated security measures, which means more cyber threats. Privacy concerns also present challenges, with increased surveillance raising ethical concerns regarding protection and misuse of data. Clearly established regulations need to be established in order to balance enforcement with the right to privacy (Vitkus, 2023). Strengthening data protection law will prevent unauthorized surveillance and place Nigeria within global cybersecurity standards. To improve enforcement, Nigeria must invest in sophisticated surveillance, arm the police with digital forensic capacity, and construct public-private partnerships. Prevention of cybercrime is a matter of government, financial institutions, and technology firms collaborating to develop real-time detection. AI threat detection, blockchain security, and biometric authentication can significantly limit cybercrime (Ezeji, 2020).

Conclusion and Recommendation

The growing menace of cybercrime in Nigeria necessitates the immediate deployment of digital surveillance technologies to facilitate cybersecurity enforcement. This study investigates how AI, machine learning, and predictive analytics enable the identification and prevention of cyber threats and applies Routine Activity Theory (RAT) to determine the capable guardianship role. There is still room for improvement despite the progress, via weak law enforcement, archaic forensics, and poor public awareness. Enhancing cybersecurity requires AI-driven monitoring, blockchain protection, interagency cooperation, and tighter controls for banks and telecommunication companies. There is a need for public awareness of cybersecurity, forensic training for law enforcers, privacy-focused policies. A digital surveillance-based proactive cybersecurity model will enhance Nigeria's cyber resilience.

References

- Adedoyin, A. D. (2023). *A study of the impact of technology on cybercrime in the public and private sectors in Nigeria*. University of Portsmouth. Retrieved from port.ac.uk.
- Adedoyin, A. D. (2023). A study of the impact of technology on cybercrime in the public and private sectors in Nigeria. *Pure.Port.ac.uk*. Retrieved from Port.ac.uk
- Adisa, O. T. (2023). *The impact of cybercrime and cybersecurity on Nigeria's national security*. Charles University. Retrieved from cuni.cz.
- Adisa, O. T. (2023). *The Impact of Cybercrime and Cybersecurity on Nigeria's National Security*. Charles University Research Repository. [Link](#)
- Akindipe, D., & Akilla, A. (2024). *Merits and Demerits of Applicable Theories to Cybercrime in Nigeria*. Retrieved from SSRN.
- Amali, S.E. (2024). *Cyberbullying Implications among Teenage Undergraduates in a Nigerian Public University*. Retrieved from ResearchGate.

- Atere, T. O. (2022). Cybersecurity regulation in the financial sector: Reflexive risk management in the UK, USA, and Nigeria. *Newcastle University Theses*. Retrieved from [Newcastle University](#)
- Bello, M., & Griffiths, M. (2021). *Routine Activity Theory and Cybercrime Investigation in Nigeria: How Capable Are Law Enforcement Agencies?* Rethinking Cybercrime: Critical Debates. Springer. [Link](#)
- Bulama, L., & Shrivastava, M. (2023). *Framework & Techniques to Improve Cybersecurity in Nigeria*. Journal of Data Acquisition & Processing. [Link](#)
- Chinedu, P. U., Nwankwo, W., & Masajuwa, F. U. (2021). *Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models*. Review of International Cybersecurity Studies. [Link](#)
- Daniels, O. (2023). National cybersecurity policy and strategy of Nigeria: A case study. *ProQuest*. Retrieved from ProQuest
- Edun, J. B. (2024). Cybercrime-ritualism and victimization in central senatorial district of Kwara State, Nigeria. *African Journal of Social and Behavioural Sciences*. Retrieved from [Aphriapub](#)
- Ezeji, C. (2020). *Challenges Faced by the Criminal Justice System in Combating Cybercrime in Nigeria*. Retrieved from [nilds.gov.ng](#).
- Ezeji, C. L. (2024). *Cyber Policy for Monitoring and Regulating Cyberspace and Cybersecurity Measures for Combating Technologically Enhanced Crime in South Africa*. International Journal of Business & Security. [Link](#)
- Idowu, O. A. (2021). Cybercrimes and challenges of cyber-security in Nigeria. *Academia.edu*. Retrieved from [Academia.edu](#)
- Ishiguo, R. O. (2024). *Cybercrime Investigation and Prosecution in Nigeria: The Role of Security and Intelligence Agencies*. International Review of Law & Cybersecurity. [Link](#)
- Ismail, U. (2020). The Nigeria police force and cybercrime policing: An appraisal. *Dutse Journal of Criminology and Security Studies*. Retrieved from [Academia.edu](#)
- Lazarus, S. (2020). Establishing the particularities of cybercrime in Nigeria: Theoretical and qualitative treatments. *PhilPapers*. Retrieved from [PhilPapers](#)
- Makanjuola, A. E., & Ayantunji, M. M. (2024). *Strengthening Cybersecurity in Nigeria: A Holistic Approach*. Journal of Cybersecurity & Digital Law. [Link](#)
- Manasseh, C. O., & Ede, K. K. (2024). *Digital Finance, Cybersecurity Challenges, and Economic Development in Nigeria*. Retrieved from [nou.edu.ng](#).

- Muller, S. R. (2022). Digital forensic readiness of cybercrime investigating institutions in Nigeria: A case study of the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police. *Academia.edu*. Retrieved from [Academia.edu](https://www.academia.edu)
- Nsude, I., Elem, S. N., & Uwaoma, A. N. (2023). *Combating Cybercrime through Artificial Intelligence for Sustainable Development in Nigeria*. Retrieved from [researchgate.net](https://www.researchgate.net).
- Obidimma, E. O. C., & Ishiguzo, R. O. (2023). *Artificial Intelligence and Cybercrime Investigation in Nigeria: Addressing the Legal and Technical Skills Gaps*. Retrieved from ezenwaohaetorc.org.
- Obidimma, E. O., & Ishiguzo, R. O. (2023). *Legal and Institutional Framework for Cybercrime Investigation and Prosecution in Nigeria: The Need to Strengthen the Existing Structures*. *African Journal of Legal Studies*. [Link](#)
- Okibe, E. S. (2024). *Analysis of the Efficacy of Nigeria's Cybercrime (Prohibition, Prevention, Etc.) Act 2015: Legal Frameworks, Challenges, and Prospects for Combating Cybercrime*. Retrieved from nigerianjournalonline.com.
- Okoru, A. O., & Oluku, O. (2024). *Cybercrime, Crime Security, and National Development in Nigeria*. Retrieved from fuoye.edu.ng.
- Olayemi, O. J. (2014). *A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria*. *International Journal of Sociology and Digital Security*. [Link](#)
- Osazuwa, C. M., DoP, A. A., & Chigbu, G. (2024). *Effect of Data Protection Frameworks Against Cybercrimes on Cybersecurity in Nigeria*. Retrieved from inlibrary.uz.
- Phillips, A., Ojalade, I., & Taiwo, E. (2023). *Cyber-Security Tactics in Mitigating Cyber-Crimes: A Review and Proposal*. *International Journal of Cybersecurity Research*. [Link](#)
- Phillips, A., Ojalade, I., Taiwo, E., & Obunadike, C. (2023). *Cyber-Security Tactics in Mitigating Cyber-Crimes: A Review and Proposal*. Retrieved from [academia.edu](https://www.academia.edu).
- Rosanwo, O. A. (2023). Students' perception and increasing rate of cybercrime among Obafemi Awolowo University undergraduates. *ResearchGate*. Retrieved from [ResearchGate](https://www.researchgate.net)