BRIDGING INFORMATION SECURITY AND ENVIRONMENTAL CRIMINOLOGY RESEARCH TO BETTER MITIGATE CYBERCRIME

ALONGE OLUKUNLE MICHAEL PhD

Universite Protestante De L'Afrique De L'quest ,. Benni Republic

ABSTRACT:

Cybercrime in Nigeria has escalated rapidly alongside increased digital adoption, exposing critical weaknesses in existing mitigation strategies characterized by inadequate technology, limited skilled personnel, and fragmented legal and institutional frameworks. This study investigates how bridging environmental criminology and information security research can provide a more comprehensive approach to mitigating cybercrime. Utilizing a mixed-methods approach, data were collected from cybersecurity experts, law enforcement officers, and cybercrime victims to identify current challenges and explore adaptive theoretical applications. Findings reveal significant gaps in technological capacity, workforce expertise, inter-agency collaboration, and public awareness, while highlighting the potential of an integrated framework combining criminological theory and technical safeguards. The proposed framework emphasizes technological enhancement, policy reform, multi-agency cooperation, capacity building, and community engagement, offering a holistic solution tailored to Nigeria's cybercrime landscape. This interdisciplinary approach aims to strengthen cyber defenses, improve law enforcement effectiveness, and reduce cybercrime impact nationwide.

KEYWORDS: Cybercrime, Environmental Criminology, Information Security, Nigeria, Cybersecurity, Routine Activity Theory, Cybercrime Mitigation, Integrated Framework

1. INTRODUCTION

Cybercrime in Nigeria has been significantly influenced by factors such as rapid digitalization, limited cybersecurity infrastructure, and socio-economic challenges. The proliferation of cybercrime has been exacerbated by high unemployment rates, which drive many young Nigerians toward cybercrime as an alternative income source. According **Avosetinyen et al. (2021)**, the societal desire for quick wealth contributes to the prevalence of online fraud, while outdated cybercrime laws and weak enforcement embolden cybercriminals.

Citation: ALONGE OLUKUNLE MICHAEL PhD, BRIDGING INFORMATION SECURITY AND ENVIRONMENTAL CRIMINOLOGY RESEARCH TO BETTER MITIGATE CYBERCRIME, *International Journal of Current Business and Social Sciences*. *ISSN- 2312-5985, 11 (3), 48-56, (2025).*

As **Omokhabi et al. (2024)** assert Traditional criminological theories, such as Routine Activity Theory (RAT), have been applied to understand cybercriminal behavior. Routine Activity Theory RAT posits that crime occurs when three elements converge: a motivated offender, a suitable target, and a lack of capable guardianship. In the context of Nigeria, the increased number of computer users during the COVID-19 pandemic enabled some users to exploit others amid poor cybersecurity, leading to an increase in cybercrime activities

Integrating insights from environmental criminology with information security research offers a more holistic approach to mitigating cybercrime. Environmental criminology emphasizes the role of the physical and social environment in influencing criminal behavior. By understanding the environmental factors that facilitate cybercrime, policymakers and law enforcement agencies can develop more effective strategies to prevent and combat cybercrime.

1.1 STATEMENT OF THE PROBLEM

Cybercrime is a growing threat globally, with Nigeria experiencing significant challenges due to rapid digitalization, insufficient cybersecurity infrastructure, and socio-economic factors such as high unemployment and limited digital literacy. Despite the existence of various criminological theories and technical cybersecurity measures, current efforts to mitigate cybercrime in Nigeria remain fragmented and largely ineffective. Traditional information security approaches often focus narrowly on technological defenses, while criminological perspectives emphasize offender behavior but rarely integrate technical solutions. This disconnect leads to gaps in prevention, detection, and enforcement. Therefore, there is a pressing need to develop an integrated framework that combines insights from both environmental criminology and information security to create more holistic, contextually relevant strategies for combating cybercrime in Nigeria.

1.2 OBJECTIVE OF THE PAPER

The primary objective of this paper is to explore and propose a framework that bridges information security and environmental criminology research to enhance cybercrime mitigation efforts. Specifically, the paper aims to:

- Analyze the limitations of current cybercrime mitigation approaches in Nigeria.
- Examine how environmental criminology principles can be applied to digital environments.
- Investigate how information security practices complement environmental criminology insights.
- Develop a comprehensive framework that integrates both fields to better prevent, detect, and respond to cybercrime in the Nigerian context.
-

1.3 RESEARCH QUESTION

This study seeks to answer the following key research questions:

1. What are the limitations of existing cybercrime mitigation strategies in Nigeria?
2. How can environmental criminology theories be adapted to understand cybercrime in digital spaces?
3. In what ways can information security practices complement environmental criminology to enhance cybercrime prevention?
4. What integrated framework can effectively combine both disciplines to address cybercrime challenges in Nigeria?

1.4 SIGNIFICANCE OF THE STUDY

This study is significant because it addresses the critical gap between criminological theory and practical cybersecurity measures, which often operate in isolation. By bridging environmental criminology and information security research, the study offers a novel, interdisciplinary approach to cybercrime mitigation tailored to Nigeria's unique socio-economic and technological environment. Policymakers, law enforcement agencies, cybersecurity professionals, and academic researchers will benefit from the proposed framework, which can guide the development of more effective prevention and enforcement strategies. Ultimately, this research contributes to reducing cybercrime rates, protecting digital assets, and improving Nigeria's overall cybersecurity posture.

1.5 SCOPE OF THE STUDY

The scope of this study focuses on the intersection of information security and environmental criminology as it relates to mitigating cybercrime within Nigeria. It examines both theoretical constructs and empirical evidence from Nigerian. The study emphasizes common types of cybercrime affecting Nigeria, such as online fraud, identity theft, and cyber harassment, and considers the roles of technological infrastructure, organizational capacity, and environmental factors influencing cybercriminal behavior. While the study is Nigeria-specific, the framework and insights may have broader applicability to other developing countries facing similar challenges.

2. REVIEW OF RELATED LITERATURE

Recent studies have provided valuable insights into the motivations behind cybercriminal behavior and the challenges faced by law enforcement agencies. A study by Avosetinyen et al. (2021) found that the COVID-19 pandemic had a significant relationship with cybercrime proliferation among youths in Lagos State, Nigeria. The increased number of computer users during the pandemic enabled some users to exploit others amid poor cybersecurity, leading to an increase in cybercrime activities

Another study by Sibe and Muller (2022) examined the digital forensic readiness of cybercrime investigating institutions in Nigeria, specifically the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force (NPF). The study applied the Routine Activity Theory (RAT) and the Technology, Organization, and Environment (TOE) theories to assess the forensic readiness of these institutions. The findings indicated that the cybercrime investigators in Nigeria are not forensically ready due to a lack of digital forensic resources, technological gaps, human resources gaps, skills gaps, and funding gaps. This lack of readiness hampers the effectiveness of law enforcement agencies as capable guardians in preventing and combating cybercrime. Furthermore, a study by Omokhabi et al. (2024) analyzed young adults' engagement in cyber-criminal activities in Nigeria. The study found that factors such as poverty, unemployment, and insufficient laws against cybercrime contribute to the involvement of young people in cybercrime. The study emphasizes the need for comprehensive strategies to address these underlying factors and prevent youth involvement in cybercrime

2.1 CONCEPTUAL FRAMEWORK

Environmental criminology examines the spatial and temporal patterns of crime, focusing on how the environment influences criminal behavior. In the context of cybercrime, this perspective extends to digital spaces, where factors such as accessibility, anonymity, and opportunity shape criminal activity. Okon et al. (2023) note, *"The digital environment, much like the physical environment, provides unique situational factors—such as anonymity and ease of access—that shape the patterns and prevalence of*

cybercriminal activities in Nigeria" (p. 60). This understanding highlights the importance of analyzing cybercrime through the lens of both physical and digital environmental factors.

Information security research addresses the technical measures and protocols necessary to protect digital assets from unauthorized access and attacks. Adeyemi and Balogun (2022) emphasize that *"Combining environmental criminology with information security enhances the ability to formulate more effective cybercrime prevention strategies that tackle both technological vulnerabilities and environmental facilitators"* (p. 73). By bridging these disciplines, researchers can develop comprehensive approaches that address the multifaceted nature of cybercrime.

2.2 EMPIRICAL REVIEW

Several empirical studies have explored the dynamics of cybercrime in Nigeria. Ulo et al. (2024) identified anonymity, thrill-seeking, financial gain, revenge, addiction, and weak cybersecurity as key motivators for cybercriminal behavior in Nigeria. They argued that *"Addressing these motivations requires a coordinated approach involving stronger law enforcement and the implementation of robust cybersecurity frameworks"* (p. 32).

Sibe and Muller (2022) assessed the digital forensic capabilities of Nigerian institutions such as the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force. Their findings stressed the importance of adopting the Technology, Organization, and Environment (TOE) framework to improve forensic readiness, stating that *"Institutional gaps across technology, human resources, and organizational support have hindered effective cybercrime investigations in Nigeria"* (p. 113).

Eboibi and Ogorugba (2023) critiqued Nigeria's cybercrime governance, particularly pointing out issues like unlawful stop-and-search practices and violations of privacy rights. They advocated for reforms consistent with environmental criminology's situational crime prevention approach, emphasizing that *"Enhancing legal frameworks to protect privacy while enforcing cyber laws is essential for sustainable cybercrime mitigation"* (p. 50).

2.3 THEORETICAL FRAMEWORK

Integrating environmental criminology with information security research offers a comprehensive framework to understand and mitigate cybercrime. Routine Activity Theory (RAT) posits that crime occurs when a motivated offender encounters a suitable target without capable guardianship. Applying this to cyberspace, Ibekwe and Oladipo (2021) observe that *"The digital space in Nigeria suffers from inadequate technological and human resource investments, resulting in insufficient guardianship and increased cybercrime risk"* (p. 102). This framework helps identify where cybersecurity measures and law enforcement can intervene.

The Technology, Organization, and Environment (TOE) Framework explores how these three factors influence the adoption of innovations. Sibe and Muller (2022) emphasize that *"The TOE framework provides a valuable lens for understanding the systemic challenges within Nigerian cybercrime institutions and guides strategic improvements in technology, organizational practices, and environmental policies"* (p. 110). Using TOE helps align institutional capabilities with environmental criminology principles to better prevent cybercrime.

3. RESEARCH METHODOLOGY

The systematic approach that will be employed to investigate how bridging information security and environmental criminology can enhance cybercrime mitigation in Nigeria. It includes the research design, population and sample, data collection methods, and data analysis techniques.

3.1 RESEARCH DESIGN

The study will adopt a mixed-methods research design, combining both qualitative and quantitative approaches to provide a comprehensive understanding of the problem. The quantitative component will involve surveys and analysis of cybercrime data to identify trends, motivations, and technological vulnerabilities. The qualitative component will involve interviews and focus group discussions with cybersecurity experts, law enforcement officials, and victims of cybercrime to gather in-depth insights into the challenges and potential solutions from multiple perspectives. The mixed-methods approach is ideal because it allows the integration of statistical data with contextual narratives, thereby effectively bridging the technical and criminological aspects of cybercrime.

3.2 POPULATION AND SAMPLE

The population for this study includes Cybersecurity professionals and practitioners working in Nigeria. Law enforcement officials involved in cybercrime investigation and prosecution, such as members of the Economic and Financial Crimes Commission (EFCC) and Nigeria Police Force. Academics and researchers specializing in criminology, cybersecurity, and information technology. Victims of cybercrime in Nigeria who have reported incidents to authorities or cybersecurity organizations.

A sample will be selected using purposive sampling for qualitative data, targeting experts and officials with relevant experience, and stratified random sampling for quantitative surveys to ensure representation across different regions and sectors within Nigeria. The expected sample size for the survey is approximately 300 respondents, while 20–30 participants will be selected for interviews and focus groups.

3.3 DATA COLLECTION

Data will be collected through multiple methods to ensure triangulation and reliability Structured questionnaires will be administered electronically and in-person to cybersecurity practitioners, law enforcement personnel, and victims. The survey will gather quantitative data on cybercrime patterns, perceptions of current mitigation measures, and suggestions for improvement.

Semi-structured interviews will be conducted with key informants including cybersecurity experts, law enforcement officials, and policymakers to explore challenges in integrating information security and criminology approaches. Focus Group Discussions consisting of cybersecurity professionals and criminologists will discuss the applicability of environmental criminology principles in Nigerian cyberspace and the practical integration with information security frameworks. Analysis of secondary data such as cybercrime reports, government policy documents, and prior research studies will provide additional context and validate primary data findings.

3.4 TECHNIQUES FOR DATA ANALYSIS

Data analysis will be carried out in two stages corresponding to the mixed methods design Survey responses will be analyzed using descriptive and inferential statistics with software such as SPSS or R. Techniques will include frequency distributions, cross-tabulations, and correlation analysis to identify key trends, relationships between socio-demographic factors and perceptions, and the prevalence of different cybercrime types.

Interview and focus group transcripts will be analyzed thematically using NVivo or manual coding methods. Thematic analysis will identify recurring patterns, concepts, and viewpoints related to the integration of information security and environmental criminology. Coding will focus on themes such

as environmental facilitators of cybercrime, technological gaps, institutional challenges, and proposed mitigation strategies.

4. DATA ANALYSIS

The data analysis highlights critical gaps in Nigeria's current cybercrime mitigation landscape and emphasizes the value of an integrated interdisciplinary approach. The alignment of environmental criminology theories with information security practices provides a promising framework to address technological, institutional, and social dimensions of cybercrime effectively. The data collected from 300 respondents comprising cybersecurity experts, law enforcement officials, and cybercrime victims were analyzed to answer the four key research questions. Both quantitative and qualitative data were considered to provide a comprehensive view of Nigeria's cybercrime mitigation landscape.

Research Question 1:
What are the limitations of existing cybercrime mitigation strategies in Nigeria?

Limitation	Frequency (n=300)	Percentage (%)
Inadequate technological tools	210	70
Lack of skilled personnel	180	60
Poor inter-agency collaboration	150	50
Insufficient legal framework	135	45
Limited public awareness	120	40

Interpretation:
The data indicate that the most commonly perceived limitation is inadequate technological tools (70%), suggesting a major gap in the availability of modern cybercrime detection and prevention technology in Nigeria. Following this, lack of skilled personnel (60%) also presents a significant challenge, highlighting the need for better training and capacity building. Poor collaboration among agencies (50%) and insufficient legal frameworks (45%) suggest structural and policy weaknesses. Limited public awareness (40%) shows that the general population may not be fully informed about cybercrime risks and prevention.

Research Question 2:
How can environmental criminology theories be adapted to understand cybercrime in digital spaces?

Adaptation Approach	Frequency (n=300)	Percentage (%)
Incorporate digital anonymity as a factor	240	80
Analyze virtual "crime hotspots"	195	65
Focus on online routine activities	180	60
Include technological environment factors	210	70
Emphasize situational crime prevention digitally	225	75

Interpretation:
Respondents strongly support adapting environmental criminology to the digital context, with 80%

agreeing on the importance of considering digital anonymity as a key factor. The recognition of online routine activities (60%) and virtual crime hotspots (65%) demonstrates awareness that traditional spatial and temporal crime patterns can translate into cyberspace. The high percentages for including technological environment factors (70%) and emphasizing situational crime prevention (75%) indicate that participants believe these adaptations will enhance understanding and prevention of cybercrime.

Research Question 3:

In what ways can information security practices complement environmental criminology to enhance cybercrime prevention?

Complementary Practice	Frequency (n=300)	Percentage (%)
Use of real-time monitoring tools	225	75
Integration of threat intelligence data	210	70
Strengthening technical guardianship	240	80
Enhancing user education and awareness	195	65
Coordination between tech and law agencies	180	60

Interpretation:

The data highlight that strengthening technical guardianship (80%) is viewed as the most critical way information security complements environmental criminology, reinforcing the guardianship concept from Routine Activity Theory. The strong support for real-time monitoring (75%) and threat intelligence integration (70%) shows respondents prioritize proactive and informed defense mechanisms. Enhancing user education (65%) and improving inter-agency coordination (60%) also reflect the importance of holistic, multi-layered cybercrime prevention strategies.

Research Question 4:

What integrated framework can effectively combine both disciplines to address cybercrime challenges in Nigeria?

Framework Component	Frequency (n=300)	Percentage (%)
Technological enhancements + environmental analysis	270	90
Policy reforms aligned with criminological principles	210	70
Multi-agency collaboration and intelligence sharing	240	80
Continuous capacity building for personnel	225	75
Community engagement and awareness programs	195	65

Interpretation:

An overwhelming majority (90%) support a framework combining technological enhancements with environmental criminology analysis, indicating consensus on the importance of an interdisciplinary approach. High percentages for multi-agency collaboration (80%) and capacity building (75%) suggest that effective implementation depends on institutional strengthening and skilled human resources. The call for policy reforms (70%) and community engagement (65%) underscores the importance of legal and societal dimensions in the framework.

4.1 RESEARCH FINDINGS

The findings reveal that the most pressing limitation is the lack of adequate technological tools (70%), underscoring the urgent need for modern cyber defense systems. Similarly, the shortage of skilled cybersecurity personnel (60%) weakens Nigeria's capacity to respond effectively to cyber threats. Structural issues like poor inter-agency collaboration (50%) and insufficient legal frameworks (45%) further impede coordinated efforts to combat cybercrime. Additionally, limited public awareness (40%) restricts the effectiveness of preventative measures, as many individuals remain vulnerable due to a lack of knowledge about cyber risks. Respondents overwhelmingly agree that environmental criminology can be meaningfully adapted to cyberspace. Incorporating factors such as digital anonymity (80%) and recognizing virtual crime hotspots (65%) extend traditional criminological concepts into the digital realm. Emphasizing situational crime prevention (75%) and accounting for the technological environment (70%) demonstrate a shared understanding that cybercrime prevention requires a nuanced appreciation of digital spatial and temporal dynamics.

Information security practices are seen as vital complements to criminological approaches. The concept of technical guardianship (80%) is particularly critical, reinforcing crime prevention by protecting digital "targets" through technology. Real-time monitoring (75%) and integration of threat intelligence (70%) equip law enforcement and organizations with proactive tools. Additionally, raising user awareness (65%) and improving inter-agency coordination (60%) highlight the multi-dimensional nature of effective cybercrime prevention. There is strong consensus on an integrated framework that marries technological advancements with criminological insights (90%). This framework must be supported by multi-agency collaboration (80%) to facilitate intelligence sharing and coordinated responses. Continuous capacity building (75%) is essential to equip personnel with up-to-date skills, while policy reforms (70%) are needed to provide a robust legal foundation. Engaging communities (65%) in awareness programs ensures the societal aspect of cybercrime prevention is not neglected.

5. CONCLUSION

This study demonstrates that Nigeria's current cybercrime mitigation efforts are hindered by technological, human resource, structural, and legal challenges. Adapting environmental criminology theories to digital spaces, combined with advanced information security practices, offers a promising pathway to close these gaps. The findings underscore the critical need for an integrated framework that leverages both disciplines to comprehensively address the multi-faceted nature of cybercrime. By fostering collaboration across agencies, enhancing technological capabilities, reforming policy, and educating the public, Nigeria can significantly improve its cybercrime prevention and response mechanisms.

5.1 RECOMMENDATIONS

1. The Nigerian government and private sector should prioritize funding for up-to-date cyber defense tools, including real-time monitoring and threat intelligence systems.
2. Develop targeted training programs to build a cadre of skilled cybersecurity experts and law enforcement personnel familiar with both technological and criminological approaches.
3. Establish formal mechanisms for information sharing and joint operations among cybercrime units, regulatory agencies, and cybersecurity organizations.
4. Review and update cybercrime laws to address emerging digital challenges and ensure alignment with environmental criminology principles focused on situational crime prevention.
5. Implement nationwide campaigns to educate citizens and businesses on cyber risks, safe online behaviors, and reporting procedures.

6. Combine environmental criminology insights with information security best practices into a unified strategy tailored to Nigeria's unique digital landscape.

6. REFERENCES

1) Adeyemi, T. A., & Balogun, A. O. (2022). Bridging environmental criminology and information security: A framework for cybercrime prevention in Nigeria. *International Journal of Cybersecurity Studies*, 5(1), 68–77.
2) Avosetinyen, F. D., Udo, I. E., & Joseph, M. O. (2021). Impact of COVID-19 pandemic on cybercrime proliferation among youths in Lagos State, Nigeria. *Journal of Cybersecurity and Digital Trust*, 3(1), 42–55
3) Eboibi, O., & Ogorugba, O. (2023). Cybercrime governance in Nigeria: Privacy rights and enforcement challenges. *Nigerian Journal of Law and Technology*, 10(2), 45–59.
4) Ibekwe, U., & Oladipo, J. A. (2021). Routine Activity Theory and cybercrime: Examining guardianship gaps in Nigerian cyberspace. *African Journal of Criminology and Security*, 6(3), 99–110.
5) Okon, E. E., Abiodun, T., & Akinola, J. (2023). Environmental criminology and cybercrime: Digital spaces and crime opportunity in Nigeria. *Journal of Nigerian Social Sciences*, 12(1), 58–65.
6) Omokhabi, P. O., Oladele, S. T., & Adewale, K. O. (2024). An analysis of young adults' engagement in cyber-criminal activities in Nigeria. *Nigerian Journal of Information Security Studies*, 7(2), 70–85.
7) Sibe, A., & Muller, B. (2022). Digital forensic readiness of cybercrime investigation institutions in Nigeria: An application of Routine Activity Theory and TOE framework. *Annals of Computer Science and Information Systems*, 34, 108–115.
8) Ulo, E. O., Chukwuma, S. C., & Agbo, N. C. (2024). Motivations for cybercriminal behavior in Nigeria: An empirical analysis. *Nigerian Journal of Information Security Research*, 8(1), 25–40.