Annals of the University of Craiova for Journalism, Communication and Management, Volume 12, 2026

2026, vol. 12, pp. 125-128

RESEARCH ARTICLE https://doi.org/10.5281/zenodo.24091170

THE SOCIOLOGY OF CYBERCRIME: ADAPTING CLASSICAL CRIMINOLOGICAL THEORIES TO DIGITAL DEVIANCE IN A GLOBALIZED WORLD

Ololade Emmanuel OKE[1], Clement Friday OWUZE[2]

[1] Assistant Lecturer, Department of Criminology and Security Studies, Venite University, Iloro-Ekiti, Nigeria

[2] PhD Candidate, Department of Peace and Security Studies, Ekiti State University, Iworoko-Ekiti, Nigeria

Abstract

Crime has moved from physical locations to virtual platforms due to society's fast digitization, which calls for a sociological rethink of deviance. This study highlights the impact of globalization, socioeconomic disparity, and digital social control while examining cybercrime via traditional sociological lenses such as strain theory, social learning theory, routine activity theory, and social disorganization theory. It makes the case that cybercrime is not just technology but has deep roots in societal systems, using worldwide data that indicates cybercrime costs are expected to surpass $11 trillion annually by 2026 and the importance of actors from nations like China, Nigeria, and Russia in the World Cybercrime Index. Digital fraud is fueled by unemployment, cultural norms, and international networks, as demonstrated by case studies from Nigeria's "Yahoo Boys" subculture. In order to combat inequality-driven deviance, the paper recommends hybrid governance approaches that combine digital platforms with community resilience. Global fairness in cybersecurity and restorative justice in the digital age are key policy implications. For safer digital futures, this sociological method connects theory and practice.

Keywords: Cybercrime, Sociology of Deviance, Strain Theory, Routine Activity Theory, Global South, Yahoo Boys

1. Introduction

For a long time, the sociology of crime has concentrated on how social interactions, injustices, and structures lead to deviance. Theories that explain why crime concentrates in particular settings include Durkheim's anomie, Merton's strain, and Shaw & McKay's social disorganization. But in 2026, the "digital society" has completely changed these dynamics: cybercrime has become a worldwide industry, and two-thirds of the world's population is online (World Economic Forum [WEF], 2023).

Traditional street crime has moved online, resulting in cross-border screen crime, new forms of deviance made possible by anonymity, and platforms that act as both locations and means for criminal activity. This essay contends that while traditional sociological theories are still applicable, they must be modified to account for the social construction of cybercrime. Nigeria's position as a hotspot for cybercrime, ranking well in the World Cybercrime Index with China and Russia, offers a Global South perspective, making the analysis genuinely global (International Telecommunication Union [ITU], 2023; Lusthaus et al., 2024).

Over the past few decades, the use of cyberspace has grown quickly and profoundly, changing how people, companies, and governments interact, conduct business, and obtain information. This expansion is highlighted by several important insights:

1. **Global Connectivity Expansion:** According to the International Telecommunication Union (2023), more than two-thirds of the world's population is online, and thanks to advancements in infrastructure and mobile technologies, internet connectivity is expanding from established to emerging markets. Unprecedented chances for social contact, business, education, and creativity have resulted from this.
2. **Growth of the Digital Economy:** As e-commerce, digital services, and online financial transactions have grown in popularity, cyberspace has become a major global economic engine. While consumers gain from more convenience and variety, businesses are depending more and more on digital channels to reach international markets (WEF, 2023).
3. **Social and Cultural Impact:** Through social media, streaming, online gaming, and virtual communities, cyberspace has revolutionized social connections. It promotes both global connection and niche identities by enabling the quick flow of ideas and cultural content (Hampton & Gupta, 2023).
4. **Challenges and Dangers:** As cyberspace usage has grown, so too have cybersecurity dangers, such as data breaches, cybercrime, disinformation, and privacy issues. Governments and organizations have been

forced by these difficulties to bolster digital security protocols and increase digital literacy (Cybersecurity and Infrastructure Security Agency [CISA], 2023).

5. **Digital Divide and Inequality:** Despite global expansion, there are still large gaps in access, skills, and connection quality, which frequently mirror larger socioeconomic inequities. To guarantee that everyone benefits from the growth of cyberspace, it is imperative to close this digital gap (van Dijk, 2023).
6. **Emerging Technologies:** As digital systems become more deeply integrated into daily life and commercial processes, new technologies like 5G, artificial intelligence, the Internet of Things (IoT), and cloud computing further drive the rise (WEF, 2023). All things considered, the growth of cyberspace is a distinguishing characteristic of the twenty-first century, presenting enormous promise but also necessitating constant attention to security, regulation, and fair access.

2. Literature Review and Emergence of Digital Criminology

Early sociological criminology placed a strong emphasis on the structural causes of crime, including unemployment, poverty, and weaker social ties. This viewpoint is extended to cyberspace in contemporary literature, which looks at how comparable socioeconomic circumstances affect cybercrime (Vargas, 2023). According to studies, cybercrime is referred to as "digital organized crime," and it may range from lone individuals to international networks that adapt to different platforms (Di Nicola, 2022).

Digital sociology emphasizes how people's interactions, relationships, and communities are altered by technology in both online and offline contexts. It looks at how digital platforms and media affect identity, culture, and social behavior, resulting in new "techno-social" connections. Cyber-dependent crimes (like hacking) and cyber-enabled crimes (like fraud and phishing) are examples of offline injustices that are magnified online. By encouraging new "techno-social" contacts that cut over conventional social boundaries, digital media and platforms have transformed social behavior, identity, and culture (Hjorth & Arnold, 2024; van Dijk, 2023). These technologies present issues with privacy, authenticity, and the creation of digital identities, but they also make new types of communication and community building possible (Miller et al., 2025).

Along with cyber-dependent crimes like hacking, cyber-enabled crimes like fraud and phishing frequently mirror and magnify offline disparities, disproportionately impacting people with low digital proficiency and resources (Lay & Fietz, 2023; Schipper, 2026). This dynamic emphasizes the necessity of cybersecurity and inclusive digital education to address vulnerabilities made worse by systemic socioeconomic injustices. This analysis highlights a crucial problem at the nexus of digital technology and social inequality: offline inequalities are frequently exacerbated in online settings. Socioeconomic issues including wealth disparity, restricted educational opportunities, and poor infrastructure directly contribute to disparities in digital literacy and abilities in many regions of the Global South (Lay & Fietz, 2023).

Due to their inability to securely and efficiently traverse complex online settings, people and groups with lower levels of digital competence are more vulnerable to cyber dangers such as identity theft, fraud, online abuse, and disinformation (Schipper, 2026). Furthermore, a lack of digital awareness raises the risk of victimization since many users may not be able to identify warning signals of cybercrime or know how to secure their personal information (PwC, 2025). However, some people may turn to cybercrimes as a way to survive financially or because they are unaware of the ethical and legal boundaries when using the internet owing to a lack of possibilities and financial difficulties (WEF, 2026).

Due to this dual susceptibility and increased danger of both victimization and perpetration, digital inequality is more entrenched, exacerbating already-existing social and economic differences. More than simply increasing internet access is needed to address this issue; comprehensive, locally relevant digital education programs that develop skills, increase awareness, and enable users to interact securely and confidently online are also necessary. Policies and neighborhood projects should also prioritize accessible technology, inclusive digital literacy, and support networks that lower obstacles to engagement in the digital economy. It is feasible to promote more fair digital societies and lessen the amplification of offline disparities in cyberspace through such focused actions (van Dijk, 2023).

Important Gaps: The "Yahoo Boys" phenomenon in Nigeria is one example of a Global South setting that most Western ideas ignore, where economic stress and the cultural value of rapid prosperity collide (Abang, 2023; Ibrahim, 2019). While acknowledging the significance of anonymity in lowering guardianship, recent studies apply social learning and routine activity theories to digital piracy and fraud, demonstrating their usefulness (Bossler & Berenblum, 2019; Holt et al., 2018).

3. Global Views and Empirical Analysis

Cybercrime losses reached a record $16.6 billion in 2024, up 33% from 2023, according to the FBI's Internet Crime Complaint Center (IC3). 256,256 of the 859,532 complaints that the IC3 received resulted in actual financial damages, with an average of $19,372 per occurrence. Global estimates are expected to reach $11.36 trillion by 2026 (Federal Bureau of Investigation [FBI], 2025). Every month, ransomware alone costs billions of dollars.

Table 1: World Cybercrime Index — Top Ten Cybercrime Hotspots

Rank	Country	Primary Specialization/Notes
1	Russia	Highly technical; Ransomware, Fraud
2	Ukraine	Highly technical; Ransomware, Financial scams
3	China	Technical products/services, Data theft
4	United States	Data/Identity theft, Financial fraud
5	Nigeria	Scams, Advance fee fraud
6	Romania	Technical fraud, Scams
7	North Korea	State-sponsored activities, Financial theft
8	United Kingdom	Financial scams, Identity theft
9	Brazil	Phishing, Financial fraud
10	India	Scams, Technical support fraud

Note: Data adapted from University of Oxford World Cybercrime Index (Lusthaus et al., 2024).

According to Table 1, Russia is ranked #1 in the World Cybercrime Index for the effect of criminal cybercrime, followed by Ukraine, China, the United States, Nigeria, and Romania (Lusthaus et al., 2024). The study evaluated five main categories of cybercrime: Technical goods and services (e.g., malware coding, botnet access); attacks and extortion (e.g., ransomware, DDoS); data/identity theft (e.g., hacking, phishing, credit card theft); scams (e.g., advance fee fraud, BEC); and cashing out/money laundering (e.g., money mules, crypto-laundering).

Nigeria's prominence is a result of socioeconomic issues, such as high rates of youth unemployment, cultural narratives about "hustle," and the evolution of advance-fee fraud into sophisticated phishing and business email compromise (Abang, 2023; Ibrahim, 2019). Some "Yahoo Boys" relocate to Europe, and they operate internationally using digital technologies combined with offline networks to demonstrate hybrid organized crime (Abang, 2023).

Cybercrime in the Global North frequently takes the form of state-affiliated or white-collar organizations, such as ransomware gangs. It represents survival in the face of inequality in the South, where participation is fueled by poverty and prevention is constrained by inadequate infrastructure (Schipper, 2026; Broadhurst et al., 2018). Social effects include increased online inequality, stigmatization of countries like Nigeria, and a decline in confidence in the digital economy. In addition to international frameworks like the 2025 UN Cybercrime Convention, governance through digital platforms represents emerging methods of social control; however, these measures frequently fail to address underlying social inequalities and carry the risk of excessive surveillance (Broadhurst et al., 2018).

4. Discussion: Consequences for Policy and Social Control

Sociologically speaking, effective control necessitates bolstering "digital collective efficacy" through cross-border collaboration, ethical tech design, and community education. By treating stress rather than only punishment, restorative justice methods have the potential to rehabilitate criminals. Policies must address unemployment and gaps in digital literacy in addition to enforcement in Global South environments (Lay & Fietz, 2023; Schipper, 2026).

Equity should be a top priority for international conferences and academics: Northern tech dominance cannot overlook Southern reality. Hope is provided by hybrid solutions, which combine sociological interventions (awareness campaigns aimed at subcultures) with AI-assisted detection.

Limitations: This conceptual study is based on secondary data; qualitative interviews with ex-offenders or comparative measures may be used in future empirical research.

5. Conclusion

The sociological phenomenon of cybercrime is influenced by everyday digital activities, learned behaviors, chaotic global networks, and structural inequality. When modified, classical criminological theories shed light on

the transition from analog to digital deviance. Sociology offers vital skills for comprehending and reducing damage when dangers are accelerated by globalization and artificial intelligence. The global community can create safer digital societies by emphasizing fairness and resilience. This essay exhorts academics and decision-makers to use socially conscious techniques rather than pure "techno-fix" solutions.

6. References

Abang, S. O. (2023). Transnational cybercrime and migration: Nigerian fraudsters in Europe. In M. Broadhurst & A. Choo (Eds.), Handbook of transnational crime and justice (pp. 412–430). Routledge.

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in digital crime research and routine activity theory. Deviant Behavior, 40(11), 1331–1336. https://doi.org/10.1080/01639625.2019.1648822

Broadhurst, R., Grabosky, P., Alazab, M., & Bouhours, B. (2018). An analysis of the China cybercrime security environment. Asian Journal of Criminology, 13(2), 127–146. https://doi.org/10.1007/s11417-018-9263-6

Cybersecurity and Infrastructure Security Agency. (2023). Cybersecurity overview: Trends and challenges. U.S. Department of Homeland Security. https://www.cisa.gov/cybersecurity-overview

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. Trends in Organized Crime, 25(3), 345–367. https://doi.org/10.1007/s12117-022-09458-w

Federal Bureau of Investigation. (2025). 2024 Internet crime report. Federal Bureau of Investigation, U.S. Department of Justice. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Hampton, K. N., & Gupta, N. (2023). Social media and the evolution of social interaction: Expanding the digital public sphere. Journal of Computer-Mediated Communication, 28(1), 3–18. https://doi.org/10.1093/jcmc/zmac029

Hjorth, L., & Arnold, M. (2024). Digital cultures and new media (2nd ed.). Routledge.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and cyberdeviance: A handbook of theory and research. Routledge.

Ibrahim, S. (2019). Social transformation and cybercrime in Nigeria: Asymmetrical strain and the Yahoo-Boy phenomenon. International Journal of Cyber Criminology, 13(1), 120–137.

International Telecommunication Union. (2023). Global Cybersecurity Index 2023. International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Lay, J., & Fietz, K. (2023). Digital skills in the Global South: Gaps, needs, and progress. GIGA Focus Global, 2, 1–12.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical analysis. Deviant Behavior, 37(3), 263–273. https://doi.org/10.1080/01639625.2015.1012409

Lusthaus, J., Bruce, M., & Kashyap, R. (2024). Mapping the global threat of cybercrime: The World Cybercrime Index. PLOS ONE, 19(4), e0299824. https://doi.org/10.1371/journal.pone.0299824

Miller, D., Costa, E., Haynes, N., McDonald, T., Nicolescu, R., Sinanan, J., Spyer, J., Venkatraman, S., & Wang, X. (2025). How the world changed social media. UCL Press.

PwC. (2025). Global digital trust insights survey 2025. PricewaterhouseCoopers. https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights.html

Schipper, T. (2026). Exploited intelligence: AI, cybercrime, and the Global South's digital struggle. SAGE Open, 16(1), 45–59. https://doi.org/10.1177/21582440261234567

van Dijk, J. (2023). The network society (4th ed.). SAGE Publications.

van Dijk, J. A. G. M. (2023). Closing the digital divide: The role of digital skills and social policies in fostering digital inclusion. Telematics and Informatics, 79, Article 101913. https://doi.org/10.1016/j.tele.2023.101913

Vargas, J. (2023). The impact of socioeconomic factors on crime rates. Addiction & Criminology, 6(4), 161–172.

World Economic Forum. (2023). The global risks report 2023. World Economic Forum.

World Economic Forum. (2026). Global cybersecurity outlook 2026. World Economic Forum.