ASSOCIATION OF COMMUNICATION SCHOLARS & PROFESSIONALS OF NIGERIA BOOK SERIES

Investigating Coverage of Cybersecurity Issues in Select Online Media Platforms in Nigeria

Jane Chinyere Adama

To cite this article:
Jane Chinyere Adama (2025), Investigating Coverage of Cybersecurity Issues in Select Online Media Platforms in Nigeria in Digital Communication and Governance in Africa: Reimagining AI in Communication and Governance ACSPN Book Series 10, pp. 169— 182
Retrieved from http://www.acspn.com.ng

(Institutional or Subscribed access may be required)

Please note that this is an electronic, pre-print version of this article published by the Evan Brothers (Nigeria Publishers) Limited for Association of Communication Scholars & Professionals of Nigeria (ACSPN).

The ACSPN Book Series is exclusive to the Association of Communication Scholars & Professionals of Nigeria.

ISBN: **978-978-690-135-0**

Layout/Design: Ashroph De Grafico Ventures.

CHAPTER 9

Investigating Coverage of Cybersecurity Issues in Select Online Media Platforms in Nigeria

Jane Chinyere ADAMA

Cybersecurity concerns encompass a broad spectrum of actions and laws designed to safeguard people and online activity. The Nigeria Cybercrimes (Prohibition, Prevention etc. Act, 2015's Part III: Offences and Penalties) explicitly defines various cybercrimes and provides appropriate sanctions based on the type of cybercrime. Cybercrime is a worldwide occurrence that impacts virtual enterprises via coordinated online deception. Governments and regulatory agencies have proposed various methods to combat online frauds as cybercrime

continues to develop unabatedly. Cybersecurity issues have unavoidably drawn attention from all throughout the world in an effort to reduce the prevalence of cybercrime (Osho and Onoja, 2015).

In a discussion of cybersecurity and cybercrime, ITU (2012) asserts that preventing cybercrime through the adoption of suitable legislation against the use of ICTs for illegal or other purposes is a crucial part of a national cybersecurity and critical information infrastructure protection strategy. Since cybercrimes are spread through online platforms and target a variety of Internet-related information processing outlets (including e-government, e-commerce, e-education, e-health, and e-environment), it is crucial to determine whether enforcing cybersecurity is legal. These outlets are seen as development enablers because they offer an effective means of delivering a wide range of basic services (ITU, 2007).

According to Online-Community HackerWatch (2010), cybercrimes are attacks on information infrastructure via the Internet, including hacking into private and public online platforms with the intention of distributing false information or earning illegal financial gains. However, the main goal of cybersecurity is to protect cyberspace from danger, specifically cyberthreats (Odumesi, 2014). Cybersecurity safeguards data on hardware and software devices and encompasses a wide range of Internet activities. In Nigeria, The Part III of the Offences and Penalties of the Nigeria Cybercrimes (Prohibition, Prevention etc.) Act, 2015 (Federal Government of Nigeria, 2015) encompasses all matters pertaining to cybersecurity and cybercrimes.

The process of obtaining, assessing, and disseminating current events-related facts is referred to as journalism. Reporters conduct research and create stories for print and digital media,

frequently under the direction of editors or producers (Castro, 2009). According to *Encyclopaedia Britannica* (2009), journalism encompasses the gathering, production, and dissemination of news as well as relevant commentary and feature materials across a variety of media, including books, radio, television, movies, newspapers, and pamphlets. According to Kenechukwu (2014), the journalist has a duty to convey the truth while acting as an impartial watchdog over the government.

The breadth of entrepreneurial inventions has increased with the rise in the Internet. A broad range of techniques and tools for acquiring, processing, and disseminating information are included in innovations in media practice. Digital or netizen journalism, sometimes referred to as online journalism, is a form of journalism where editorial content is disseminated via the Internet (Franklin, 2013). It has to do with news being distributed digitally over the Internet. Online journalism often covers generic online forms of print, broadcast, and social media; however, specific online print media and blogs were content-analyzed for this study.

Review of Related Literature

The Internet has completely changed the way that information is gathered, processed, and shared. It now offers a wealth of knowledge on a wide range of topics that are relevant to people's lives (Kenechukwu, 2014). Users can still easily obtain information with only a mouse click thanks to the interactive nature of the Internet. The world is becoming more and more dependent on computer networks and technologies due to the widespread computerisation of modern society. Cybercrime, or unlawful activity conducted online, is another effect of it. Cybercrime is a worldwide occurrence that impacts virtual enterprises via coordinated online deception. Information management is at risk due to cybercrime, despite the fact that the Internet has changed how people communicate and carry out

various jobs (Osho & Onoja, 2015).

Cybercrime, according to Odumesi (2014), is any criminal activity that involves the improper or abusive use of digital resources in a cyberspace on the internet, computer networks, computer systems, or wireless communication networks. Internet fraud is a computer-mediated crime that hurts the victim financially, emotionally, and physically. According to Akinsehinde (2011), cybercriminals are increasingly breaking into websites belonging to individuals, corporations, and government agencies due to the vulnerability of Internet networks. According to Chigozie-Okwum, Udeaja, Michael, and Osuo-Genseleke (2017), cybercrimes have a negative impact on information gathering and processing because they aim to manipulate computer programs or permanently harm systems and important data by infecting and spreading viruses on computer networks.

Due to website insecurity, the majority of Internet businesses are vulnerable to cyber attacks. According to Akinsehinde (2011), the bulk of Nigerian online companies are vulnerable to cyber attacks, and the country's economy is in danger due to the rise in cybercriminals. Numerous governments and regulatory agencies have proposed various methods to combat online frauds as cybercrime continues to develop unabatedly. The Nigeria Cybercrimes (Prohibition, Prevention etc.) Act, 2015, Part III: Offences and Penalties, lists several types of cybercrimes along with the appropriate legal penalties. The Act stops online scammers in their tracks and gives Internet users their trust and credibility back.

There are various types of cybercrimes. According to Wall (2001), cybercrime can take the following forms:

a. Cyber pornography: This term refers to any computer-based expressions of profanity and indecency, whether overt or covertly suggested through words, visuals, or

codes.

b. Cyber trespass: This includes inserting viruses into a user's internet account in order to deceive or deny him ownership of intellectual property.
c. Cyber violence: This refers to any kind of psychological damage or malfunctions caused by cyber manipulations of machines. Cyberstalking is a type of cyberviolence that entails frighteningly following someone over an extended period of time. One facet of cyber violence involves the introduction of viruses to influence a computer system.
d. Cyber deceptions and thefts: This category includes any computer-based fraud, including the theft of a person's social media or bank account. Cybersquatting is another facet of online fraud and theft. It is the fraudulent purchase and sale of goods through the use of a registered business.

Other types of cybercrimes include:

i. Cyber espionage: It is another kind of cybercrime that involves using technology to spy on someone. The act of spying on people and the government using electronic means is illegal.
ii. Cyber thefts: Hacking into someone's computer database with the intent to take pertinent files or conduct unauthorised financial withdrawals or transfers is a crime. It also includes any dishonest methods of obtaining someone else's social media or company account for questionable ends.
iii. Cyberbullying: This refers to any bullying that occurs online that uses emojis, photographs, and posts to disparage a person. It also addresses the use of the Internet to coerce someone into sending money in order to restore their reputation.
iv. Cyber plagiarism: The practice of copying someone else's words or works without giving credit to the original author or creator is known as plagiarism.

v. The fifth is cyber terrorism, which deals with the use of technology to support terrorism. The Internet has become a veritable informational tool about terrorist activity.

Cybercrimes of Online Journalism

The World Wide Web (www) has completely changed the way that journalism is practised. Nonetheless, concerns about cybercrime have continued to arise in the fields of academia and security. Cyber plagiarism, or the computer-generated act of creating a verbatim clone of another author's literary work, is a frequent cybercrime in online journalism. Plagiarism, according to Kenechukwu (2014), is the act of reproducing someone else's literary work verbatim without giving credit to the original author. Plagiarism is illegal and constitutes a breach of intellectual property rights. It is unfortunate that authors frequently take passages from the Internet and paste them without giving credit. The tendency of blogs and online mainstream media to copy and paste information or duplicate news in ways that suggest they are unique creative works has increased due to citizen journalism.

Media projects have been harmed by cyberspace's susceptibility to cyberattacks. This is due to the fact that computer attacks are similar to network-transmitting disease infections (Gandhi, 2014). Cyberattacks in cyberspace can result in defamation, which is the discrediting or defamation of another person's character. Blogs or online news sites that are renowned for frequently apologising for earlier posts are regarded as excellent news sources.

Cyber theft and cyberbullying are easily carried out through certain online print media and social media blogs, although cases of cyber espionage may be somewhat fostered by these platforms. Cyber theft is the popular practice of accessing someone's social media or bank account for unauthorised

withdrawals using Internet-enabled devices. In a similar vein, it alludes to illegally using online techniques to deceive someone or steal their intellectual property.

Cybersecurity: Using Ingenuity to Overcome Cybercrimes

Innovation is the application of fresh concepts or methods. An ICT economy has difficulties due to its permeable structure and susceptibility to cybercrimes. The term "innovation" has several different definitions. Off-the-shelf products and current technologies can serve as the foundation for new invention. According to Kannengießer (2020), there is a growing correlation between media innovation and social change in media practice. The analysis of the socioeconomic and cultural background of change is emphasised in this relationship.

Cybersecurity is predicated on the idea that cyberspace needs to be safeguarded by suitable laws and technological measures that prevent cybercrimes from continuing. The goal of cybersecurity is to protect cyberspace from risks, namely cyber attacks (Odumesi, 2014). As a result, cybersecurity concerns have unavoidably drawn attention from around the world (Osho and Onoja, 2015). Making cyberspace safe from threats, namely cyber threats, is the main goal of cyber security (Odumesi, 2014). The Nigeria Cybercrimes (Prohibition, Prevention etc.) Act, 2015 criminalises all cybercrimes and governs Internet-related activities in Nigeria. In a nutshell, cybersecurity is the use of instruments and regulations to safeguard the digital environment and offer a framework for the prosecution of violators. It shields individuals and organisations from unauthorised access to data. Cybersecurity, as a strategy driven by policy, employs legal frameworks and functional policies to safeguard cyberspace and lessen the susceptibility of individuals and organisations to cybercrimes (Ibikunle and Eweniyi, 2013).

Theoretical Framework

The study is anchored on theory of technology-enabled crimes which assumes that technology plays critical roles in crime commission and control. It is predicated on the idea that technology has an impact on both the commission and management of crime, thus postulating that there is a nexus between crime and technology, particularly computers and telecommunications (McQuade, 2006). Weakened systems are more susceptible to malware (viruses, worms, Trojan horses, and rootkits), as well as sabotage via the use of computers and related technologies (e.g., online child exploitation, cyberstalking, extortion, tmfraud, and identity theft), as well as ancillary uses such as online marketplaces for illegal goods (Ubas & Cho, 2008). Thus technologies enable the unemployed youths to commit crimes like; scams, harassment, financial frauds, character assassinations and so on.

Statement of the Problem

While the Internet has changed how individuals communicate and carry out various duties, information management is at risk due to cybercrime. The system's password can be compromised with just one click, making it more susceptible to online crimes like cybertheft, cyberbullying, cyberpornography, and cyberhacking. Data are a set of precise values, which when used improperly, turn into a destructive weapon. Without taking into account the potential consequences, a hacker lacking expertise in information management can distribute a significant amount of confidential government material. Smartphone users have come to assume that journalism is about using a smartphone to create and spread unedited and erroneous information, or even to subtly construct meanings in order to mock or discredit characters, thanks to the advent of citizen journalism.

As digitisation advances, there are more innovative methods to use Internet-enabled gadgets to engage in illicit online activity.

Cybercrimes deprive aspiring business owners and organisations of their intellectual property rights and raise the frequency of financial frauds. Governments, particularly the Nigerian government, have made cybercrimes illegal, which has resulted in the enactment of the Nigeria Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, which outlines the offences and penalties associated with it. As a result, this study conducts a content analysis of some online journalism platforms' cybercrimes. However, in spite of the existing laws and regulation, cybercrime is daily on the increase and threatens the national security, compromises business aspirations and impacts negatively on the nation's image globally. It is against this background that this study investigated frequency of reportage of incidences of cybercrimes in select online media platforms in Nigeria.

The broad objective of the study is to examine incidents of cybercrime of online journalism through improved innovations in cybersecurity. Two specific objectives that guided the study include:

i. To determine the frequency of coverage of cybercrimes by select online news platforms; and
ii. To determine the slant (nature) of coverage of cybercrimes by select online news platform.

Materials and Methods

The study took place within a three- month period (April- June June, 2024). Two online news platforms selected for the study are (a) *The Nation Newspaper* Online and (b) Blog (lindaikejisblog.com). The total population of the select publications could not be ascertained because of the fleeting nature of online publications. The quantitative content analysis procedure was adopted with the following content categories as guides:

- Cyber trespasses and thefts- cybercrimes associated with hacking and invading a system with virus etc;
- Cyber bullying- Cybercrime associated bullies through images etc.;
- Cyber pornography: Cybercrime associated with portrayal of obscenity and indecency etc) ;
- Cyber attack- Cybercrime associated with attacks on persons for political or socioeconomic reasons); and
- Cyber plagiarism-Cybercrime associated with violation of intellectual property rights.

The unit of analysis comprises news, pictures and cartoons that suggest potential cases of cybercrimes. The coding guide was the instrument for data collection.

Results and Discussion

Data Presentation and Analysis

Table 1: Frequency of coverage of cybercrimes by select online news platforms

Content Category	The Nation Newspaper Online			Lindaikejisblog	
	Headline/News	Pictures	Cartoons	Headline/News	Pictures Cartoons
Cyber trespasses and thefts	2	2	1	1	-
Cyber bullying	2	2	3	3	-
Cyber pornography	-	-	-	1	
Cyber plagiarism	-	-	-	-	-
Cyber attacks	2	-	-	-	-
TOTAL	**6**	**4**	**4**	**6**	**-**

Table 1 indicates that both online news outlets had low coverage of issues on cybercrime across the categories of cybercrime. Observed too, is the place of aesthetics in online journalism. Both news outlets used images to complement news on identified

content categories. However, *The Nation Newspaper Online* reported more issues of cyber attacks on persons represented in the manner of political attacks on presidential candidates of different political parties. Also, within the period of coverage, *The Nation Newspaper Online* and *Linda Ikeji's Blog* did not report any issue on cyber plagiarism. *The Nation Newspaper Online* did not record any crime related to cyber pornography. On the other hand, Linda Ikejis Blog has significant coverage of issues on attacks that may be classified as cyberbullying.

Table 2: Slant (nature) of coverage of cybercrimes by select online news platforms

Content Category	**The Nation Newspaper Online**			**Lindaikejisblog**		
	Person-to-Person-cybercrime	Person-to-government cybercrime	Politically-motivated cybercrime	Person-to-person-cybercrime	Person-to-government cybercrime	Politically-motivated cybercrime
Cyber Trespasses and thefts	1	1	-	1		-
Cyber bullying	2	-	-	6	-	-
Cyber pornography	-	-	-	7	-	
Cyber plagiarism	-	-				
Cyber attacks	2	-	7	-	-	-
TOTAL	**13**			**14**		

On the slant (nature) of coverage of issues of cybercrimes were directed at persons than to government. This suggests the reason for the propensity of perpetrators to target vulnerable people with less knowledge of the vulnerability of the Internet for committing cybercrime. However, *The Nation Newspaper Online* had no representation of cyber pornography. Both online outfits

had no coverage of issues of cyber plagiarism.

Conclusion and Recommendations

The chapter demonstrates that there is a low level of coverage of cases of cybercrimes in relation to news of general interests by both online news platforms. *The Nation Newspaper online*, , which is an online arm of mainstream media focused on news on general interest with minimal coverage of issues on cybercrimes within the period of study. On the other hand, *Linda Ikeji's Blog* recorded significant news on politics, entertainment but had minimal coverage of cybercrimes. Equally, Cyber plagiarism is seldom reported. In spite of preponderances of reported cases of cybercrime in conventional media, the dearth or low level of attention to the malaise in Online media as demonstrated in this paper appears curious. Issues of cybercrimes continue to pose security challenge to individuals, corporate bodies and government, but the Online media platforms seem to be turning a blind eye to the challenge in the society.

Based on the findings, this chapter recommends that, with the promulgation of Nigeria Cybercrimes (Prohibition, Prevention etc.) Act, 2015, there should be periodic checks on the effective implementation of the provisions of the Act by appropriate regulatory agencies. In the events of legal breaches, extant sanctions should be meted out accordingly. Equally, there is the need for increased coverage of cybercrimes by online news platforms. This is because, youths who are susceptible to Internet frauds are active users of the Internet. Finally, there is the need for workshops on Media and Information Literacy (MIL) which will empower users of different media on strategies and tactics for handling the malaise and menace of cybercrime in the society.

REFERENCES

Akinsehinde (2011). '80% of Nigerian business risk cyber-attacks? *The Punch*, October, 11.

Chigozie-Okwum, C., Ugboaja, S., Michael, D. and Osuo-Genseleke, M. (2017). Proliferation of cybersecurity in Nigeria: A root cause analysis. *International Journal of Science Technology*, 6(2), 53-60.

Castro, J. (2009). *Journalism*. Redmond, WA: Microsoft Corporation.

Encyclopædia Britannica **(2009).** ***Journalism*.** Chicago: Encyclopædia Britannica.

Federal Government of Nigeria (2015). *Cybercrimes (Prohibition, Prevention etc.) Act, 2015* https://www.cert.gov.ng. Accessed on 20-1-2023.

Franklin, B. (2013). Digital journalism. *Digital Journalism*, 1: 1-5.

Gandhi, G. (2014). *Complexity theory of cybersecurity*. https://www.researchgate.net/publication/263652176. Accessed on 24-1-2023.

Ibikunle, F. and Eweniyi, O. (2013). Approaches to cybersecurity issues in Nigeria: challenges and solutions. *International Journal of Cognitive Research in Science, Engineering and Education*, 1(1), 1-11.

ITU (2012). *Understanding cybercrime: phenomena, challenges and legal response*. ITU Telecommunication Development Bureau.

ITU (2007). ITU cybersecurity work programme to assist developing countries 2007-2009. Retrieved on 20-1-2023 from www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

Kannengießer, S. (2020). Fair media technologies: Innovative media devices for social change and the good life. *The Journal of Media Innovations*, 6(1), 3849

Kenechukwu, S.A. (2014). *Mass communication: an introduction to sociology of mass media*. Nnewi: CathCom Press.

McQuade, S. (2006). Technology-enabled crime, policing and security. *Journal of Technology Studies*, 32(1), 32-42.

Online-Community HackerWatch (2010) Hacking attacks. Retrieved on 19-01-2023 from www.hackerwatch.org.

Odumesi, J.O. (2014). Combating the menace of cybercrime. *International Journal of Computer Science and Mobile Computing*, 3(6), 980-991.

Osho, O. and Onoja, A. (2015). National cybersecurity policy and strategy of Nigeria: a qualitative analysis. *International Journal of Cyber Criminology*, 9(1) 120-143.

Ubas, G. & Cho, K. R. (2008) Resource material on technology-enabled crime. Australian Institute of criminals.

Wall, D.S. (2011). *Crime and the internet.* London: Routledge.