Information and communications technology (ICT) and airspace management in Nigeria: An analysis

Utam, Edward Unimke[1], Adams, John Anyabe[2], Ugbe, Justin I.[3]

Institute of Public Policy and Administration, University of Calabar, Calabar, Nigeria, unimkee@yahoo.com, edwardutam@unical.edu.nq
Department of Political Science, University of Calabar, Calabar, Nigeria, anyabeadams@unical.edu.nq, anvabe2003@vahoo.com
Department of Political Science, University of Calabar, Calabar, Nigeria, ugbej68@vahoo.com

Abstract

This study explores the pivotal role of Information and Communications Technology (ICT) in managing Nigeria's airspace, focusing on both civil aviation and defense sectors. Utilizing a descriptive survey method and qualitative data analysis, the research adopts the Routine Activity Theory by Cohen and Felson (1979) as its theoretical framework. The findings highlight that inadequate monitoring and policing of airspace infrastructure have exposed Nigeria to criminal and subversive activities, threatening national security. To address this, the study recommends establishing a multi-stakeholder governance system. This system should integrate various private, public, and international authorities within the ICT sector, under the oversight of the Nigerian Information Technology Development Agency (NITDA). Comprising technocrats skilled in airspace-related criminality, such as cybercrimes, cyber terrorism, and cyber espionage, this regime would be tasked with monitoring, protecting, and securing Nigeria's airspace infrastructure.

Keywords: Information and Communication Technology (ICT), Airspace Management, Threats, National Security, Defence Management.

Introduction

Information and Communications Technology (ICT) has undoubtedly transformed the world into a global village. ICT has significantly enhanced various forms of human communication, international trade, investments, and diplomacy (Idiom & Tormusa, 2016). Among the most powerful elements of ICT, the Internet stands out for merging the world into a network of digital infrastructures marked by computer-generated connectivity and visibility (Idom, 2012). Known as the cloud, cyberspace, or airspace, this domain can host and transmit vast amounts of information within seconds. It has dissolved geographical boundaries, eliminated communication barriers, and facilitated extensive business opportunities and international relations among countries worldwide (Adeniran, 2008).

Idom and Ugal (2016) assert that the primary goal of ICT convergence is the advancement of the Internet, designed to facilitate timely information dissemination, prompt delivery of human services globally, and to make other forms of intangible interaction a reality. Nigeria has reaped significant benefits from these positive aspects of ICT since its adoption in the 1950s. However, ICT has also become a substantial threat to the security of Nigeria's airspace and other vulnerable nations (Okoli & Idom, 2018). This threat is evident in the rising incidents of ICT-based warfare, ideological and religious radicalization, advanced fee fraud, hate speech, and terrorist recruitment and financing. According to Dasuki (2014), while ICT enhances Nigeria's economy by breaking down commercial barriers and facilitating ideological exchanges worldwide, it simultaneously introduces new risks that threaten national security. The unregulated nature of Nigeria's airspace has made it a breeding ground for nefarious activities and potential security breaches (Okoli & Idom, 2018). Omale and Idom (2016) highlight that although ICT advancements were not intended to promote crime, criminals often exploit these technologies to carry out their malicious acts. Such internet-related activities are undermining the integrity of Nigeria's airspace, with serious implications for national security.

The key point to note is that as Information and Communications Technology (ICT) continues to expand, the inevitable consequence is that Nigeria's airspace will become a blend of the GARDEN and the WILDERNESS (Idom & Ugal, 2016). According to Nnamani (2016), fraudsters, spies, terrorists, and hackers will always be drawn to exploit our airspace due to its perceived ungovernability and low risk of apprehension. The vulnerability of Nigeria's airspace to various threats presents a new challenge to national security, necessitating an analysis to develop measures that can secure Nigeria's airspace infrastructure.

Theoretical explanations of ICT in airspace management in Nigeria

To further enrich this paper, it is essential to provide a theoretical explanation of the preceding discussion to thoroughly understand how the airspace has become attractive to criminals, thereby posing a serious threat to Nigeria's national security. For this purpose, the Routine Activity Theory has been selected. Propounded by Cohen and Felson (1979), this theory explains the routine occurrence of crime in society through the interaction of three key variables: the availability of suitable targets, the absence of capable guardianship, and the presence of motivated or potential offenders.

However, it is crucial to provide a theoretical framework to better understand why the airspace has become an attractive target for criminals, thus posing a significant threat to Nigeria's national security. For this purpose, the Routine Activity Theory has been chosen. Introduced by Cohen and Felson (1979), this theory elucidates how crime occurs in society through the interplay of three key factors: the availability of suitable targets, the lack of capable guardianship, and the presence of motivated or potential offenders. Applying this theory to explain airspace threats to Nigeria's national security, we can observe the following: the availability of suitable targets refers to the potential pool of victims and the porous nature of the airspace; the absence of capable guardianship represents the lack of cyber vigilantism, e-policing, national central control, and a functional national database; while the presence of motivated or potential offenders denotes the numerous unemployed Nigerian youths with a strong desire for material gain.

When these variables are present in any given society, there is a greater likelihood that crime, including airspace crimes, will occur. According to Idom and Tormusa (2016), the motivation to commit crime and the supply of offenders tend to remain constant in contemporary society. In most societies, there are always individuals willing to break the law for gain, revenge, greed, or other motives. Greed and gain, from both perpetrators and victims, have fueled the proliferation of cybercrimes in the airspace. The utility of this theory in the context of this study lies in its ability to provide a simple and powerful insight into the factors that lead to airspace crimes in Nigeria. The core idea of this theory is that, in the absence of effective controls, such as cyber security or cyber vigilantism, offenders will exploit attractive targets, such as the porous airspace infrastructure.

Nigeria's airspace management: An analysis

A state's sovereignty is defined by its ability to safeguard and defend its borders and territorial integrity. This jurisdictional control extends to airspace/cyberspace, maritime zones, and land areas (Okoli & Ochim, 2016). In geographical terms, a territory includes the hemisphere, lithosphere, and biosphere. A state should possess the capability to regulate all tangible and intangible activities within its borders without restrictions (Goldsmith, 1998). Although Nigeria has a strong military presence relative to other African nations, its airspace remains notably vulnerable (Okoli & Idom, 2018). According to Longe (2004) and Idom and Ugal (2016), the Nigerian airspace is difficult to manage due to its complexity and the challenges in detecting criminal activities. Even when such activities are identified, securing physical evidence is often problematic because digital traces can be easily altered or erased. Crimes in the airspace can occur across vast distances, bypassing geographical limitations. What remains unexplored in these studies is how developed countries successfully secure their airspaces despite similar complexities. These nations have implemented advanced technologies, robust surveillance systems, and comprehensive regulatory frameworks that might provide insights into how Nigeria and other nations could enhance their airspace security. Understanding these strategies could offer valuable lessons for improving the governance and protection of Nigerian airspace.

As highlighted by Okoli and Idom (2018), the Nigerian airspace faces significant risk exposure, evident in the extent of threats and vulnerabilities it encounters. Major sources of cyber threats in Nigeria include terrorist or extremist groups, organized criminal syndicates, international spies, corporate insiders, and freelance hackers. Nnamani (2016:8) attributes these threats to rising poverty levels, greed (from both perpetrators and occasionally victims), easy access to vulnerable targets, and insufficient legal and regulatory measures to prevent and prosecute such activities. Additionally, the pursuit of "easy money" among Nigerian youth has been a significant contributing factor to cyber criminality, beyond mere survivalist motivations.

The situation is exacerbated by the lack of a robust cyber governance framework capable of enforcing essential regulations within the cyber sector. This inadequacy has led to widespread criminal impunity, manifesting in an increase in cyber scams across Nigeria. Common examples of cyber-based scams in Nigeria include Advanced Fee Fraud (commonly known as "419"), Internal Fraud Compromise, Third Party Application Compromise, Identity Theft, Phishing Sites, Skimming Rogue Mobile Applications, Rogue Merchants, and Ransomware attacks (CBN, 2015). Data indicate that Nigeria's airspace vulnerability is particularly concerning. For example, in 2015, Nigeria experienced approximately 2,175 cyber-attacks, with 585 specifically targeting government websites. Table 1 below provides detailed insights into this issue.

TABLE 1: Nigeria's airspace vulnerability status in 2015

FACT	FIGURE
Estimated number of attacks	2,175
Estimated percentage of people that suffered attacks	14% of 97 million internet users
Nigeria's global airspace attacks rating	17th most attacked nation of the world

Source: Nigerian Information Technology Development Agency (NITDA, 2015), cited in Okoii & Idom (2018).

In 2016, Nigeria incurred a loss of 550 million naira due to crimes in the airspace, making it the most severely affected country in terms of the financial impact of cyber-crimes. Table 2 below presents this data in a comparative context.

TABLE *2:* Nigerian airspace crime cost in comparative terms with country population GDP of internet users and estimated cost of subscribers of airspace crimes (2016)

N	1	2	3	4
Africa	1,185,529,578	USD 2,89T	340,783,342	USD 2 Billion
Nigeria *	186,879,760*	USD 48,10666*	97,210,000*	USD 550M*
Kenya	46,790,758	USD 63,3986	37,716,579	USD 175M
Tanzania	52,482,726	USD 44,95B	17,263,523	USD 85M
Ghana	26,908,262	USD 3,786B	19,125,469	USD 50M
Uganda	38,319,241	26,369B	14,564,660	USD35M

Source: Adapted from Makataiani (2016:9) Nigeria Cyber Security Report 2016 cited in Okoli & Idom (2018).

More recent records indicate that Nigeria's airspace ignominy has persisted. In 2017, for instance, Nigeria ranked the third worst country in terms of cybercrime incidence. By this ignominious record, the country followed the lead of the United Kingdom (1st position) and United States (2nd position) on the global scale. What are the consequences of Nigeria's airspace vulnerability to national security?

Consequences of Nigeria's airspace vulnerability on national security

The primary victim of Nigeria's airspace vulnerability is the nation's image and reputation. Nigeria's growing notoriety for airspace-related crimes has, over time, tainted its global brand with a reputation for fraudulence (Okoli, 2013). As noted by Osho and Onoja (2015:121), "The prolonged occurrence of these crimes has led both Nigerians and foreigners to be excessively cautious, with legitimate interactions originating from or related to Nigeria across cyberspace now marked by heightened skepticism." Additionally, Omale and Idom (2016) observed that Nigeria's international cyber reputation has resulted in the scrutiny and mistrust of the country's crucial financial documents, such as bank cheques and drafts, by other nations. The implications of this situation are significant: Nigeria's financial documents are often perceived as unreliable for international transactions, and emails originating from Nigeria are frequently met with extreme suspicion by the global community. In some cases, internet communications from Nigeria are blocked by foreign internet gateways due to concerns about cyber fraud. This has led to widespread discrimination against Nigerians, largely attributed to the notorious "yahoo boys" syndrome.

According to Idom and Ugal (2016), international banks now conduct thorough investigations and extended research into Nigerian financial transactions before processing them, which often results in delays. Consequently, many foreign investors are deterred from investing in the Nigerian economy. This lack of trust has diminished Nigeria's credibility on the global stage, undermining its appeal as a business and investment destination. It is therefore not surprising that Nigeria has performed poorly in recent World Bank Ease of Doing Business Rankings, with the 2017 report placing the country at the bottom of the list. This is shown in table 3 below:

TABLE 3: Nigeria's Ease of Doing Business Profile (2017) in comparative terms

Country	Ranking
Mauritius	25
Rwanda	41
Kenya	80
Botswana	81
South Africa	82
Nigeria*	145*

Source: World Bank, Ease of Doing Business, 2017 culled from Okoli & Idom (2018)

In addition to hindering international business and investment, airspace crimes have also been linked to communal and sectarian violence in Nigeria. The misuse of social media to spread divisive sentiments has often exacerbated tensions and hostility among different social groups. A notable example is the ongoing farmer-herder conflicts, where social media has aggravated the situation by framing the dispute as an ethnoreligious conflict (Ibrahim & Dabugat, 2016).

A particularly severe challenge to Nigeria's cybersecurity is the use of the airspace for terrorism recruitment and financing. Terrorist organizations exploit this space to solicit funding, donations, and new members. They also use it for ideological indoctrination and radicalization, making it a significant issue for counter-terrorism efforts globally (Jacobson, 2009). For instance, Boko Haram has leveraged Nigeria's airspace to establish transnational connections with other extremist groups, enhancing their capacity for coordinated attacks and recruitment. It is clear from the discussion that the inadequate governance and policing of Nigeria's airspace pose a significant threat to national security. The study reveals that insufficient monitoring has resulted in a porous airspace system, which has compromised the security of civil aviation and defense management.

The financial impact of cyber-crimes represents a substantial economic loss, with significant opportunity costs including a challenging investment climate and business environment. Additionally, the issues of hate speech, terrorism financing and recruitment, and human trafficking further exacerbate the situation, negatively affecting the nation's stability, corporate health, and long-term sustainability. To address these problems, Nigeria has been struggling to fulfill its commitment to enhancing its cybersecurity measures, as illustrated by Table 4.

TABLE 4: Nigeria's global airspace security commitment (2017) in comparative terms

Country Score	Global Bank
Mauritius	0.830 6
Rwanda	0.602.36
Kenya	0.574 .4J
Nigeria*	0.569* 46*
Uganda	0.536 50
South Africa	0.502 58
Botswana	0.430 69
Coted'Ivoire	0.416 74
Cameroon	0.413 75
Ghana	0.325 87

Source: Global Cyber Security Index **(GCI)** 2017, p. 51

Despite the evident efforts outlined in Table 4, Nigeria's cybersecurity profile remains among the worst in Africa. The country continues to be a major hub for airspace crimes, serving as a source, transit point, and destination for such activities. The ongoing prevalence of airspace crimes represents a critical aspect of Nigeria's contemporary national security crisis.

Conclusion and recommendations

The modern world is rapidly evolving under the influence of the digital era brought about by the ICT revolution. The concept of the "global village" has moved beyond mere abstraction and has been realized through the widespread expansion of airspace across the globe. This global ICT renaissance has led to profound changes across all sectors, overcoming traditional barriers of time and space. However, it has also been linked to illicit activities that undermine national security. The virtual lack of effective governance over the global airspace has made it a prime venue for criminal activities conducted by both state and non-state actors.

As demonstrated in this paper, the advent and expansion of ICT in Nigeria have yielded both positive and negative outcomes. While the development has introduced significant innovations that have benefited the economy, it has also exposed Nigeria's airspace to criminal and subversive activities that threaten national security. The susceptibility of Nigeria's airspace to criminal exploitation underscores the lack of effective governance over the country's ICT infrastructure. This situation highlights the urgent need for a pragmatic airspace governance regime that can regulate the activities of ICT operators and users to safeguard national security.

Therefore, this paper recommends the establishment of a multi-stakeholder governance system. This system should integrate various private, public, national, and international authorities within the ICT sector into a cohesive regulatory framework, overseen by the Nigerian Information Technology Development Agency (NITDA). The governance should be led by a team of expert technocrats specializing in airspace criminality, including cybercrimes, cyber-terrorism, and cyber-espionage. This team should focus on enhancing and mainstreaming airspace vigilance through research, innovation, and technical resources. They should guide and support private, corporate, and governmental stakeholders in their efforts to combat all forms of airspace abuse and misappropriation. Effective measures against airspace-based criminality must acknowledge its intelligence-driven nature. Therefore, anti-graft operatives should be equipped with the necessary intellectual and technical skills to outmaneuver the sophisticated perpetrators of these crimes.

References

Abraham. S. (2014). *Who governs the Internet? Implications for freedom and national security. World Wide Web (YOJANA),* April, 41-44.

Adesina, S. O. (2017). *Cyber crime and poverty in Nigeria.* Canadian Social Science, 13 (4), 19-29.

Aladenusi, T.S. (2014). *Solving national security challenges with information technology,* Which way forward? A power-point presentation at the TPAffO14 conference organized by Computer Professionals 2014.

CBN (2015). The Nigeria *Electronic Fraud Forum (NEFF) 2015 Annual Report.* Abuja: Central Bank of Nigeria.

Clop ton, Z. D. (2016). *Territoriality, technology, and national security.* University of Chicago Law Review, 83 (45), 45-63.

Comer, D. E. (2009). *'Internet'^ Microsoft Encarta 2009 [DVD]. Redmond* W.A: Microsoft Corporation, 2018.

Dasuki, M.S. (2014). *'Forward'. National Cyber Security Strategy.* Abuja: Office of the National Security Adviser.

Global Cyber-security Index. GCI (2017). International Telecommunications Union (ITU).

Goldsmith, J.L (1998). *The Internet and the abiding significance of territorial sovereignty.* Indiana Journal of Global Legal Studies, 5 (2), 475-491.

Ibrahim, J. & Dabugat, K. (2016). *Rural banditry and hate speech in northern Nigeria: Fertile ground for the construction of dangerous narratives in Nigeria (257-319),* in MJ. Kuna and 3. Ibrahim (eds), *Rural banditry and conflict in northern Nigerian.* Abuja: Centre for Democracy and Development (CDD).

Idom, A. M & Tormusa, D. O (2016). *Causes, types and likely victims of cybercrimes in selected higher institutions,* 1(1): 202-218.

Idom, A. M. & Ugal, D. B. (2016). *Influence of ICT competence on cybercrimes In selected cities of the six geo-political zones In Nigeria.* FULafia Journal of Humanities and Social Sciences. 1(1): 220-241.

Idom, A. M. (2012). *Fiber optics technology and cybercrimes in Cross River State: A proactive analysis.* Unpublished seminar paper presented in the Department of Sociology, University of Calabar.

Jacobson, M. (2009). *Terrorist financing on the Internet* CTC Sentinel, 2(6), 17-20.

Makatiari, W. (2016). *'Executive Summary'. Nigeria Cyber Security Report 2016,* Serianu Ltd.

NITDf) (2015). *Nigeria Cybersecurity facts. Abuja:* Nigeria Information Technology Development Agency.

Nnamani, I. (2016). 'Foreword^1 *Nigeria Cyber Security Report 2016.* Serianu Ltd.

Nye, J. S. Jr (2014). *The regime complex for managing global " cyber activities, Paper Series No 1,* Global Commission on Internet Governance (Qurintemet.org).

Okoli, A. C & Ochim, F.I. (2016). *Forestlands and national security in Nigeria: A threat-import analysis.* HARD International Journal of Political and Administrative Studies, 2 (2), 43-53.

Okoli, A. C. & Idom, A. M. (2018). The internet and national security in Nigeria: A threat-import discourse. *Covenant University Journal of Politics & International Affairs (CUJPIA), 6(1): 20- 29.*

Okoli, A. C. (2013). *'Rebranding Nigeria's reputation management drive: Implications for national image.* Journal of Communication and Media Research, 5 (2), 81-87.

Okoli, A.C & Okpaleke, F.N. (2014). *Cattle rustling and dialectics of security in northern Nigeria.* International Journal of Liberal Arts and Social Science, 2 (3), 109-117.

Omale, D. J & Idom, A. M (2016). *Fiber optics technology and cybercrimes in Calabar Metropolis, Nigeria.* International Journal of Social Relevance & Concern. 4(4): 1-15. Available online at www.ijQurnalsJn/jlsrc

Osho, O. & Onoja, A. D. (2015). *National Cyber Security Policy and Strategy of Nigeria: A qualitative analysis.* International Journal of Cyber Criminology (IJCC), 9 (1), 120-143. 001: 10. 5281/ZENODO. 22390.