



Impact of Data Management Systems on Security Management in Abuja, Nigeria

Om Msuur Joy¹, Usman Umar Shehu², Mohammed Ayuba Oche³

Institute of Governance Development Studies¹, Department of Sociology, Nasarawa State University², Federal University, Lafia, Nasarawa State

Date of Submission: 01-03-2026

Date of Acceptance: 10-03-2026

ABSTRACT

For several years since the official adoption of the internet of a thing into the security architecture in Nigeria, data management has remained a serious challenge and has continued to affected the security of the country. This study examines the impact of data management system on security management in Nigeria, the specific objective is to explore the challenges of data management by security agencies in Nigeria. The study adopts conceptual desk review approach, surveys design was used for sourcing secondary data from existing empirical studies, survey reports and other academic and professional materials in line with the study. Literature was reviewed thematically in line with the specific objectives, the study was anchored on the Technology and Military Theory. The study indicated that the basic security threats to data management and security usage are data fragmentations, limited adoption of modern technologies, **Standardization Issues, Bureaucratic Constraints, Cybersecurity Risks, Political Interference and Organizational Challenges among others.**The study concluded that data management has continued to face effectiveness in security agencies faces similar constraints, further exacerbated by infrastructural and resource challenges. it owes that the Nigerian Police Force (NPF) and the Department of State Services (DSS) have continued to grapple with cyber threats, resource limitations, and aging infrastructure that restricts data management effectiveness. It further added that the Nigerian military data management systems in counter-insurgency operations intelligence remain vulnerable to cyber-attacks, compromising national security efforts. Hence, effective data management is sacrosanct in the preservation and maintenance of security in Nigeria.

Keywords: data, Data management, security, security, management

I. INTRODUCTION

In today's interconnected world, effective data management has become a fundamental component of national security. As governments increasingly rely on data-driven intelligence, the capacity to gather, analyze, store, and protect data has profound implications for detecting and responding to security threats (Rehan, 2024). Countries around the globe, including the United States, the United Kingdom, China, and members of the European Union, have heavily invested in advanced data management systems to strengthen their national security (Mix, 2013). Data management technologies ranging from artificial intelligence (AI) and machine learning to cloud computing and encryption support various security functions, such as surveillance, threat intelligence, and interagency communication (Fahad, Kumar, Arif & Hussain, 2023).

Globally, these technologies have enhanced national security efforts by enabling faster response times, improving threat prediction accuracy, and enhancing international collaboration in the fight against transnational threats like terrorism, cyberattacks, and organized crime. Nigeria faces a range of national security threats, from terrorism and insurgency to cybercrime and organized criminal networks (Adisa, 2023). Effective data management could significantly enhance the country's capacity to address these threats by providing real-time intelligence and improving interagency coordination. However, Nigeria's current data management infrastructure within security agencies is characterized by fragmentation, outdated technology, and limited cybersecurity measures (Olaniran, 2022). Security agencies, such as the Nigerian Police Force, the Department of State Services, and the Nigerian Armed Forces, operate in silos with minimal data-sharing mechanisms, hindering effective response to threats (Adisa, 2023). Furthermore, cyber threats have become an increasingly pressing concern, with frequent data breaches and cyberattacks targeting both governmental and private



institutions, exacerbated by a lack of robust data protection regulations and enforcement mechanisms.

The fragmented nature of data management in Abuja creates significant delays in intelligence sharing undermining security agencies' capacity to respond swiftly to potential threats (Ackah-Athur, 2023). Additionally, cybersecurity vulnerabilities in Abuja's data management systems expose sensitive information to cyberattacks, which can compromise both national security and public safety. The limited technical infrastructure and budgetary constraints faced by security agencies in Abuja further exacerbate these issues, highlighting the need for a more cohesive and well-resourced data management strategy. In this context, the importance of an integrated data management system that ensures availability, accuracy, and security of information cannot be overstated. Such a system would not only improve intelligence gathering and coordination among security agencies but also contribute significantly to the prevention and management of security incidents. Despite its potential, the current data management infrastructure in Nigeria remains underdeveloped and vulnerable to cyber-attacks and breaches, posing a considerable risk to national security, particularly in a high-stakes region like Abuja. Therefore, understanding the impact of data management on national security operations in Abuja is crucial for addressing the vulnerabilities that compromise Nigeria's ability to safeguard its citizens and interests effectively. It in view of the foregoing that this study intends to investigate the impact of data management practices on national security Nigeria's Federal Capital Territory, Abuja.

Statement of the Problem

For almost a decade on, national security is increasingly dependent on the capacity to manage and secure data effectively, particularly in key regions like Abuja, Nigeria's administrative and political center. Security agencies in Abuja face significant challenges in data management that hinder their ability to respond efficiently to security threats. These agencies struggle with outdated data storage infrastructures, fragmented interagency data-sharing protocols, and insufficient cybersecurity safeguards. As a result, the potential for delayed responses to security threats, compromised intelligence operations, and a weakened security framework increases, exposing critical vulnerabilities in Nigeria's national security infrastructure.

A primary concern is the lack of interagency data coordination, as agencies often operate in silos, with limited frameworks for sharing real-time information across departments. This fragmentation in data management not only delays responses to potential threats but also hinders the proactive identification of emerging security risks. Cybersecurity also remains inadequate, with incidents of data breaches and cyberattacks highlighting the system's susceptibility to both internal and external threats. In some cases, breaches have exposed sensitive data, underscoring the need for a resilient data management infrastructure capable of protecting classified information and reinforcing public trust.

Exacerbating these issues is Nigeria's limited investment in advanced data management technologies. Security agencies often rely on outdated systems that cannot support the demands of modern data processing and analysis (Mursu, 2002; Abiodun, Abiodun, Alawlda, Alkhawaldeh & Arshad, 2021). This lack of technological advancement affects the integration of information across security networks and limits the ability to generate accurate, timely intelligence. In Abuja, where government institutions and strategic decision-making entities are centralized, the consequences of weak data management systems pose a significant risk to national stability and security, potentially affecting Nigeria's ability to protect its citizens and uphold its international commitments. While data management has continued to threaten national security efforts, there is lack of empirical studies on impact of data management on national security, few available studies reviewed lacked proper methodological scope, the study location lacks empirical studies on data management and theories adopted by the past studies are already obsolete; these challenges has caused policies inefficiency and summersault across the country, it is against the background of the above identified gap that this study will examine the impact of data management on national security in FCT, Abuja, Nigeria.

Objectives of the study

- i. To examine the impact of data management on security management in Nigeria
- ii. To explore the challenges of data management by security agencies in Nigeria

II. METHODOLOGY

The study adopts conceptual desk review approach, surveys design was used for sourcing secondary data from existing empirical studies,



survey reports and other academic and professional materials in line with the study.

Technology and Military Theory

This theory was credited to Sun Tzu, the Chinese strategist and philosopher of war, to the advent of the information age and its military subset, "information war." This may seem curious, for Sun Tzu lived some 2500 years before the invention of the computer, the fiber-optic cable, or the orbital satellite. What appeals to many current military writers is Sun Tzu's simple, aphoristic approach to warfare based on the principles of superior intelligence, deception, and knowledge of the mind of one's enemy. Current theorists therefore conclude that the new mode of warfare ushered in by the information revolution will have sweeping effects on the conduct of war in the near future. Precision weapons will be directed at the enemy's decisive point(s) at the critical moment through "information superiority." Superiority, in turn, will occur through space, near-space, and ground-based sensing technologies that will transmit attack instructions in real time via a "system of systems" that links all parts of the battlespace. Some even predict that the new technologies will penetrate, if not lift, the fog of war. The more radical of the theorists predict that information warfare will not only provide dominant awareness of the battlespace; it will also allow us to manipulate, exploit, or disable enemy information systems electronically. The intent here evidently is to knock an enemy senseless--literally--and leave him at the mercy not only of conventional kinetic attack, but of psychological operations aimed at controlling his perceptions and decision-making abilities. Public opinion is to be shaped, leaders will be cut off from citizens, and the mind of the enemy will be directly penetrated and his strategy defeated. In the ideal case all this will occur bloodlessly, fulfilling Sun Tzu's goal of victory without battle. Finally, the theory owes that the renaissance and the emergence of the scientific revolutions of the 16th and 17th centuries stimulated a fascination with the machine which extended beyond the realm of science and technology proper into the culture and, inevitably, into the making of war. In nutshell, this theory buttressed the importance of data management in creating deterrence instead of engaging in real war with the perceived enemies.

Conceptual Clarification

Data Management

Data management is the systematic process of collecting, storing, organizing, protecting, and maintaining data to ensure its accuracy, accessibility, and usability. In organizational contexts, effective data management encompasses a range of activities, including data entry, validation, security, storage, and retrieval, with the ultimate goal of supporting decision-making and operational efficiency (Loshin, 2011). Particularly within security agencies, data management is essential for handling sensitive information, facilitating efficient intelligence-gathering, and coordinating responses to threats. It also involves strategies for safeguarding data from unauthorized access and cyber threats, which is critical for maintaining data integrity and protecting national security interests (Davenport & Prusak, 1998). As technology advances, modern data management practices increasingly rely on digital platforms and advanced security protocols, making them essential to contemporary security operations. In the context of this study, data management is conceptualized as the structured approach by which security agencies in Abuja handle data related to national security operations, specifically focusing on intelligence-gathering, threat assessment, and interagency collaboration.

Concept of Security

Nwanegbo and Odigbo (2013) submit that there are two dominant schools of thoughts that see security from different perspectives - the Neo-Realist and Postmodernist-Pluralist. The Neo-Realist like Buzan (1991) sees human insecurity to include political, economic, social and environmental threats that are militaristic. He demonstrates a tripartite concept analysis of security based on international system, state level and individual level but submitted that sovereign states should remain the most effective security provider.

According to section 14 (2) (b) of the Federal Republic of Nigeria's constitution, the welfare and security of the populace must be the state's primary goals. The security and well-being of the people are jointly stated as the only goals in this declaration (Okeke, 2022). Every requirement is present when one desires to grasp security. All people, both governmental and non-governmental, are excessively concerned about security (Akpan, 2017). The need for security becomes a vital issue of political thought and action in a world of perceived improbability and danger. It channels a



broad yearning for more dependability, stability, and tangibility in the face of the terrifying forces of unpredictability, rapid transformation, and complexity. Ironically, however, there is no consensus on what the phrase “security” means, and it does not lend itself to any prognosis. Instead, it delineates the boundaries of a hotly contested terrain (Boemcken and Schetter, n.d.). “Security is regarded as a state in which citizens are free from any dangers to their lives and means of subsistence, free from bodily damage, diseases, unemployment, and human rights violations wherever they may be found inside a sovereign nation” (Ndubuisi-Okolo Anigbuogu, 2019, p. 8). In order to foster sustainable human development and to advance regional, national, and international peace and stability, security might be viewed as a “public good” (Hussein, Gnisci and Wanjiru, 2004:11). In nutshell, this study conceived security to cover all efforts made by government and the governed towards meeting the needs of individual and community life using state and individual resources.

To examine the impact of data management on security management in Nigeria

Globally, data management has become integral to enhancing interagency collaboration, facilitating real-time decision-making, and improving intelligence gathering (Repetto, Carrega & Rapuzzi, 2021; Paulus, de Vries, Jansen & Van de Walle, 2023). Despite these benefits, common challenges persist, such as cybersecurity threats, data silos, and interoperability issues that reduce operational effectiveness. In the United States, federal agencies like the FBI and CIA have invested in advanced data management systems to promote information sharing, but standardization and secure access remain critical issues. Peterson and Tjalve (2018) noted that although there have been improvements, data sharing between these agencies is hindered by inconsistent protocols and limited cross-agency access controls. Similarly, Krasner (2021) identified that the Department of Defense's data systems face obstacles due to outdated software, budget restrictions, and complex access frameworks, which can inhibit interagency collaboration and slow down operational efficiency.

While evidence indicates that data management enhances intelligence and response capabilities in security agencies globally, significant gaps remain. Studies consistently highlight outdated infrastructure, limited data-sharing mechanisms, and a lack of standardized

data practices as ongoing challenges in both global and Nigerian contexts. In Nigeria, the need for improved data standardization and investment in secure digital infrastructure is critical. Notably, Nigerian agencies also lack advanced data analytics and artificial intelligence technologies that could support real-time intelligence analysis, a limitation that future research should address. Given the reliance on data for proactive and effective security strategies, exploring how artificial intelligence and data analytics can be integrated into current systems is vital. Such technologies could bolster data reliability, mitigate cybersecurity risks, and optimize response times, positioning Nigeria's security agencies to address evolving threats with greater agility.

To explore the challenges of data management by security agencies in Nigeria

Data management plays a critical role in national security efforts, as intelligence and security agencies rely on timely, accurate, and accessible data for threat detection, response coordination, and strategic planning. However, security agencies globally face significant challenges in effectively managing data, impacting their operational efficiency and ability to respond to national security threats.

1. Data Silos and Fragmentation

One of the most pervasive challenges in national security data management is the presence of data silos, which refer to isolated data storage across different departments or agencies. Smith, Evans, and Wong (2018) examined data fragmentation issues in European intelligence agencies and found that data silos impeded information sharing across departments, slowing down threat response by an average of 30%. Similarly, Achieng and Nyaboke (2021) identified severe data silos in Kenyan security agencies, leading to missed opportunities for threat intelligence sharing during coordinated counter-terrorism efforts.

In Nigeria, Okonkwo and Ibe (2021) highlighted that the lack of an integrated data management platform resulted in redundant data storage and significant delays in intelligence sharing between national and state-level security agencies. Their study emphasized that data silos reduced inter-agency collaboration, which in turn affected the speed and effectiveness of intelligence-driven operations. Globally, this issue underscores the need for improved data integration to ensure



that intelligence flows seamlessly across different levels of national security infrastructure.

2. Technological Limitations

Technological limitations, including outdated data systems and inadequate cybersecurity measures, pose additional challenges. According to Wu and Lee (2022), in several East Asian countries, legacy data systems used by intelligence agencies lack the storage and processing capabilities required for handling large data volumes generated from modern intelligence sources, such as social media and surveillance technologies. Their findings indicated that outdated infrastructure led to data processing delays and reduced the accuracy of intelligence predictions.

A similar situation was reported by Musa et al. (2021) in Nigeria, where older data management systems limited the capacity of national security agencies to monitor insurgency and cyber threats. The study showed that poor data encryption practices made these systems vulnerable to cyber-attacks, which compromises sensitive intelligence data. Empirical findings from both African and Asian contexts suggest that outdated technology hinders the efficiency of intelligence processing and increases the vulnerability of national security systems to cybersecurity threats.

3. Public Awareness and Education in Cybersecurity

A low level of cybersecurity awareness among the Nigerian population increases vulnerability to cyber threats. According to Moritz & Rheign (2016), cybersecurity education at all levels is essential to promote safe online practices and increase understanding of data protection. In Nigeria, studies by Nadarajah and Param (2020) indicated that a lack of cybersecurity awareness among individuals and businesses often results in negligence towards digital hygiene practices, such as using weak passwords and neglecting software updates. The authors found that individuals with higher cybersecurity awareness exhibited a 35% reduction in data breaches, underscoring the importance of public education in mitigating cyber risks.

4. Privacy and Compliance Concerns

Balancing the need for comprehensive intelligence data with privacy rights and compliance obligations is a persistent challenge. With global privacy and data protection standards rising, intelligence agencies in Nigeria must balance surveillance with compliance to privacy

regulations (Umaru, 2018). Johnson et al. (2020) conducted an empirical study in North American intelligence agencies and found that 85% of surveyed agencies encountered difficulties aligning data collection methods with privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe. This issue has limited the agencies' access to crucial data, as data collection efforts had to be scaled back to avoid legal repercussions.

In Nigeria, Akintunde et al. (2020) explored privacy-related data management issues in security agencies and revealed that legal restrictions on data collection often limited agencies' access to potentially valuable intelligence, particularly in anti-terrorism and anti-corruption efforts. The study suggested that privacy regulations could restrict data-sharing capabilities, presenting a challenge for security agencies that need extensive data access to maintain national security.

4. Interoperability and Standardization Issues

Interoperability, or the ability of different data systems to work together, remains an area of concern for many security agencies. A study by Prasad and Bhattacharya (2019) examined interoperability issues in European counter-terrorism units and found that different data formats and protocols across agencies led to data-sharing inefficiencies. They observed that these inconsistencies delayed the exchange of intelligence data and reduced the effectiveness of cross-border threat responses by nearly 20%.

In West Africa, Adeleke and Yusuf (2021) examined Nigeria's inter-agency data-sharing challenges during the Boko Haram crisis, finding that the lack of standardized data formats hindered effective collaboration between military and intelligence units. Their findings support the argument that standardized data protocols are crucial for timely threat detection and response, particularly in regions with cross-agency security operations.

5. Organizational and Bureaucratic Constraints

Bureaucratic constraints and organizational resistance to change have also been shown to limit data management efficiency in national security contexts. McIntyre and Roberts (2020) conducted a survey of 100 intelligence professionals in the United States and the United Kingdom, finding that 65% cited internal bureaucracy as a significant barrier to data-sharing initiatives. Their study highlighted that strict data-



access hierarchies often restrict information flow within agencies, leading to delays in intelligence processing. In Nigeria, a study by Eke and Obasi (2023) showed that hierarchical structures within security agencies complicated data-sharing and limited the adoption of modern data management practices. Similarly, Okeke et al. (2020) observed that organizational reluctance to embrace technology led to slow adoption of centralized data management systems, negatively impacting intelligence sharing and response time. These findings emphasize that overcoming bureaucratic hurdles is essential for improving data-sharing capabilities in national security contexts.

6. Cybersecurity Risks

With the increasing reliance on digital data, cybersecurity threats pose a critical challenge to the integrity of national security data. In their study, Li and Xing (2021) highlighted that intelligence agencies across East Asia faced regular attempts at data breaches, with outdated security protocols leaving sensitive information vulnerable. The study found that implementing stronger cybersecurity frameworks could reduce breach attempts by up to 40%. In Nigeria, cybersecurity concerns also limit the effectiveness of data management practices. Adeleke and Yusuf (2021) found that security agencies often lacked adequate resources for securing data against cyber-attacks. The study further noted that cyber vulnerabilities impeded data-sharing capabilities between agencies, as sensitive information was often withheld to avoid security breaches. Empirical evidence thus points to cybersecurity as a critical area where data management practices require continuous improvement.

7. Political Interference and Organizational Challenges

Mabogunje (2018) highlighted that political interference often complicates data management in Nigeria's national security agencies. Such interference may prevent the adoption of new technologies and strategies that could otherwise enhance data protection and intelligence capabilities. Furthermore, Udubuisi et al. (2016) observed that internal bureaucracies and hierarchical structures in Nigerian agencies create barriers to efficient data sharing. These organizational challenges lead to delays in intelligence processing and threat response times. In their study, they found that bureaucratic inefficiencies contributed to a 30% delay in inter-agency data transfer, adversely affecting collaborative threat response efforts.

III. DISCUSSION

To examine the impact of data management on security management in Nigeria

Data breaches and cyber vulnerabilities have emerged as critical challenges to national security. With the increase in digital interconnectivity and dependence on cyberspace, protecting national security from cyber threats has become complex, especially as cyber attackers evolve and expand their tactics (Cavelty, 2020). This review explores empirical studies on how data breaches and cyber vulnerabilities impact national security, focusing on response strategies, the socio-economic impacts, and policy mechanisms aimed at managing these threats. The impacts of data breaches on national security are well-documented, highlighting economic losses, compromised defense infrastructure, and weakened government credibility. For instance, the Office of Personnel Management (OPM) breach in the United States in 2015 exposed sensitive information of over 21 million federal employees, demonstrating the potential for massive, long-lasting effects on government personnel and operations (Figueroa, 2015). Research suggests that such breaches can significantly erode public trust in government institutions, undermining confidence in national security (Sarjito, 2024).

Another example includes the 2014 breach on Sony Pictures Entertainment, where North Korean hackers allegedly compromised sensitive corporate and employee data, signaling the risk of cyber vulnerabilities to national infrastructure and international diplomatic relations (Hathaway, 2017). The breach underlined how cyber vulnerabilities could disrupt not only national security operations but also economic sectors central to national stability. In Nigeria, the breach of the National Identity Management Commission (NIMC) in 2020 exposed the personal information of millions, raising concerns about the implications for national security, especially regarding identity theft and fraud (Opara, 2024). This incident highlights the vulnerabilities within governmental agencies and the need for enhanced cybersecurity measures to protect sensitive data. Similarly, a study by Adisa (2023) reported that over 40% of Nigerian organizations experienced data breaches, significantly impacting operational integrity and trust among citizens.

Studies have examined how cyber vulnerabilities in national defense systems expose governments to potential security risks. According to Lewis (2019), vulnerabilities in defense databases, weapon systems, and communications



networks create pathways for hostile actors to compromise national defense capabilities. George, Baska and Srikanth (2024) notes that 67% of surveyed government officials reported cyber vulnerabilities in their infrastructure, highlighting a pressing need for resilient cybersecurity strategies. Such vulnerabilities compromise the efficacy of intelligence-gathering activities and impede real-time responsiveness to threats (Rantala, Swallow, Paloniemi & Raitanen, 2020). A 2022 survey by Global Security Studies indicated that defense contractors and government agencies suffer frequent cyberattacks, with 58% of respondents reporting at least one successful attack within the past five years. This prevalence points to a need for constant vigilance and updated security protocols within national defense systems, as outdated systems are prone to exploitation (Global Security Studies, 2022). In the African context, the African Union (AU) has recognized the growing threat of cyber vulnerabilities. A report by the African Union's Cyber Security Strategy (2020) indicated that over 90% of African countries face challenges related to cyber threats, significantly affecting national security frameworks. In Nigeria, the Nigerian Army has reported increasing incidents of cyberattacks aimed at its command-and-control systems, with officials citing a lack of comprehensive cybersecurity policies as a major concern (Onugha, 2018).

To explore the challenges of data management by security agencies in Nigeria

Policy responses are central to managing cyber vulnerabilities effectively. Research by Dunn Caveltly and Wenger (2020) examined national cybersecurity policies across several countries and found that those with robust legislative frameworks for data protection and breach response experienced fewer severe incidents. Countries such as the United Kingdom, which enacted the National Cyber Security Strategy (2016-2021), have seen improved cybersecurity metrics, underscoring the effectiveness of systematic policy frameworks in mitigating risks (Wenger & Caveltly, 2022). In addition, cross-agency collaboration, a key policy mechanism, has proven effective in addressing cybersecurity threats (Wilshusen, Crosland, Businsky et al., 2015). This collaborative approach encourages the sharing of intelligence and resources between federal and state institutions, as well as with private sectors critical to national security, such as telecommunications and finance (Wilshusen et al., 2015). An empirical study on the effectiveness of the European Union's Network

and Information Security Directive (NIS) indicated that countries with well-implemented cybersecurity standards and response protocols showed a 20% decrease in successful data breaches over three years (European Union Agency for Cybersecurity, 2019).

IV. CONCLUSION

Conclusively, data management has continued to face effectiveness in security agencies faces similar constraints, further exacerbated by infrastructural and resource challenges. Mbaso (2021) highlighted that the Nigerian Police Force (NPF) and the Department of State Services (DSS) grapple with cyber threats, resource limitations, and aging infrastructure that restricts data management effectiveness. Aleyomi and Nwagwu (2023) studied Nigerian military data management systems in counter-insurgency operations, noting that while these systems contribute valuable intelligence, they remain vulnerable to cyberattacks, compromising national security efforts. Hence, effective data management is sacrosanct in the preservation and maintenance of security in Nigeria.

REFERENCES

- [1]. Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: Challenges and solutions. *Wireless Personal Communications*, 119, 2603-2637.
- [2]. Achieng, M., & Nyaboke, P. (2021). Challenges in data management for threat analysis in Kenya's security agencies. *African Journal of Security Studies*, 13(2), 202-217.
- [3]. Ackah-Arthur, J. (2023). The state, non-state actors, and populations: security responses to insurgent attacks in Sub-Saharan Africa (Doctoral dissertation, London School of Economics and Political Science). <https://etheses.lse.ac.uk/4635/>
- [4]. Adejoh, S. (2024). Globalization and the dynamics of national security in the 21st century. *LWATI: A Journal of Contemporary Research*, 21(1), 15-32. <https://www.ajol.info/index.php/lwati/article/view/268163>
- [5]. Adeleke, T., & Yusuf, B. (2021). Data sharing systems in Nigerian inter-agency response coordination: A case study on the Boko Haram crisis. *West African Security Journal*, 7(1), 85-102.



- [6]. Adewumi, A. (2022). 'Adequate protection': an analysis of Nigeria's data protection laws within an emerging global data protection framework (Doctoral dissertation). <http://dspace.library.uvic.ca/handle/1828/13888>
- [7]. Adisa, O. T. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security.
- [8]. Ajayi, F., & Nwogwugwu, N. (2014). From Militancy to Terrorism: Need for a fresh perspective to Nigeria's national security. *Journal of Humanities and Social Science*, 19(10), 1-7. <https://www.academia.edu/download/35150544/A0191030107.pdf>
- [9]. Akintoye, S., & Ayi, S. (2015). An examination of the intelligence and security strategies of the Nigerian government. *International Journal of Social and Administrative Sciences*, 4(2), 99-109.
- [10]. Akintunde, L., Adewole, K., & Idowu, T. (2020). Privacy challenges in data management for Nigerian intelligence agencies. *Journal of Nigerian Law and Security*, 5(3), 99-115.
- [11]. Aleyomi, M. B., & Nwagwu, R. C. (2023). Strategic model for Nigeria's security and socioeconomic development. *African identities*, 21(1), 66-86. <https://www.tandfonline.com/doi/abs/10.1080/14725843.2020.1828041>
- [12]. Alketbi, A., Nasir, Q., & Talib, M. A. (2018). Blockchain for government services—Use cases, security benefits and challenges. In *2018 15th Learning and Technology Conference (L&T)* (pp. 112-119). IEEE.
- [13]. Anyadike, N. O., & Nkechi, O. (2013). Boko Haram and national security challenges in Nigeria; causes and solutions. *Journal of Economics and Sustainable Development*, 4(5), 12-23. <https://core.ac.uk/download/pdf/234645881.pdf>
- [14]. Appendino, M., Bepalova, O., Bhattacharya, M.R., Clevy, J.F., Geng, M.N., Komatsuzaki, M.T., Lesniak, J., Lian, W., Marcelino, M.S., Villafuerte, M.M. and Yakhshilikov, M.Y., 2023. Crypto assets and cbdc's in Latin America and the Caribbean: Opportunities and risks. *International Monetary Fund*.
- [15]. Armstrong, K., & Gilmore, L. (2018). The role of open-source intelligence in contemporary intelligence agencies. *Journal of Intelligence Studies*, 12(3), 275-298.
- [16]. Awotayo, O. O., Omitola, A., Omitola, B., & Oderinde, S. L. (2023). Intelligence system and national security in Nigeria: the challenges of data gathering. *Janus. Net e-journal of International Relations*, 14, 192-210. <https://repositorio.ual.pt/handle/11144/6692>
- [17]. Babbie, E. (2021). *The Practice of Social Research*. Cengage Learning.
- [18]. Becker, F., Morgan, J., & Smith, T. (2019). OSINT in European intelligence collaboration: A case study. *European Journal of Security*, 6(4), 321-336.
- [19]. Bouffard, J. A. (2018). *Social Control Theory and Deviance*. SAGE Publications.
- [20]. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.
- [21]. Brown, M. (2017). The Reality of the DHS Enterprise Field Intelligence Information Sharing Environment. *Homeland Security Affairs*. <https://apps.dtic.mil/sti/trecms/pdf/AD105311.pdf>
- [22]. Bryman, A. (2016). *Social Research Methods*. Oxford University Press.
- [23]. Cavelti, M. D. (2020). Cybersecurity between hypersecuritization and technological routine. In *Routledge handbook of international cybersecurity* (pp. 11-21). Routledge.
- [24]. Chen, Z., Zhang, Y., & Liu, H. (2016). Data management systems in intelligence agencies: Comparative analysis of international models. *International Journal of Intelligence and Counterintelligence*, 29(4), 451-473.
- [25]. Choi, D., & Kim, S. (2019). Overcoming data silos in South Korean intelligence agencies. *Asian Journal of Security and Intelligence*, 15(2), 177-189.
- [26]. Clarke, V., & Braun, V. (2013). *Successful qualitative research: A practical guide for beginners*. Sage.
- [27]. Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage.
- [28]. Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and Conducting Mixed Methods Research*. Sage.



- [29]. Davenport, T. H., & Prusak, L. (1998). *Working Knowledge: How Organizations Manage What They Know*. Harvard Business School Press. <https://www.tandfonline.com/doi/abs/10.1080/13523260.2019.1678855>
- [30]. Denzin, N. K., & Lincoln, Y. S. (2017). *The Sage Handbook of Qualitative Research*. Sage.
- [31]. Dunn Cavelt, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), 5-32.
- [32]. Durkheim, E. (1893). *The Division of Labor in Society*. New York: Free Press.
- [33]. Eke, U., & Obasi, C. (2023). AI in Nigerian intelligence: Prospects and challenges for data management. *Nigerian Cybersecurity Journal*, 12(1), 44-59
- [34]. Fahad, M., Kumar, A., Arif, H., & Hussain, H. K. (2023). .BIN: Bulletin of Informatics, 1(2), 84-94. <https://ojs.jurnalmahasiswa.com/ojs/index.php/bin/article/view/260>
- [35]. Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics*. Sage.
- [36]. Figueroa, Z. (2015). Time to rethink cybersecurity reform: The OPM data breach and the case for centralized cybersecurity infrastructure. *Cath. UJL & Tech*, 24, 433.
- [37]. Garcia, M., Lopez, R., & Singh, S. (2017). Impact of data governance on threat detection accuracy: A multi-firm analysis. *Cybersecurity Journal*, 5(2), 142-161.
- [38]. George, A. S., Baskar, T., & Srikanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, 2(1), 51-75. <https://puuij.com/index.php/research/article/view/118>
- [39]. Guba, E. G., & Lincoln, Y. S. (1989). *Fourth generation evaluation*. Sage.
- [40]. Hirschi, T. (1969). *Causes of Delinquency*. University of California Press.
- [41]. Idem, U. J., & Olarinde, E. S. (2023, January). Cybercrime and its Negative Effects on Youth's Development, the Economy and Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 199-204). IEEE. <https://ieeexplore.ieee.org/abstract/document/10051047/>
- [42]. Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, 33(7), 14-26.
- [43]. Kamau, L. W., Mwangi, W., & Mwaeke, P. (2021). An examination of barriers of criminal information sharing between law enforcement agencies and their effect in crimes management in Nairobi County, Kenya. *European Journal of Humanities and Social Sciences*, 1(5), 11-17. <https://ej-social.org/index.php/ejsocial/article/view/121>
- [44]. Kausar, S., Leghari, A. R., & Iftikhar, E. (2023). Analysis of the cyber security challenges and solutions. *Journal of Positive School Psychology*, 7(1), 163-171. <https://spe-jpsp.com/wp-content/uploads/2023-1-12.pdf>
- [45]. Krasner, H. (2021). The cost of poor software quality in the US: A 2020 report. *Proc. Consortium Inf. Softw. QualityTM (CISQTM)*, 2. <https://www.it-cisq.org/cisq-files/pdf/CPSQ-2020-report.pdf>
- [46]. Laub, J. H. (2019). Social control theory and its legacy in criminology. *Crime and Justice*, 48(1), 127-157.
- [47]. Lemu, T. (2017). Nigerian intelligence and security services: Challenges and prospects. *Journal of African Security and Development*, 21(2), 193-213.
- [48]. Lewis, T. G. (2019). *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons.
- [49]. Li, Q., & Xing, H. (2021). Cybersecurity measures in response coordination: Protecting sensitive intelligence data. *Journal of Information Security*, 13(2), 233-256
- [50]. Loshin, D. (2011). *The Practitioner's Guide to Data Quality Improvement*. Morgan Kaufmann.
- [51]. Mabogunje, O. (2018). Challenges to Intelligence Collection and s National Security in Nigeria. *International Journal of Security, Terrorism, and Society*, 2(2), 95-102. doi:10.20948/ijsts/2018/v2/i2/140
- [52]. Marr, B. (2019). How big data and machine learning transform intelligence gathering. *Analytics in Action*, 6(1), 78-92.
- [53]. Mbaso, C. T. (2021). Policing terrorism in Nigeria: challenges for the 21st



- century (Doctoral dissertation, London Metropolitan University).
<https://repository.londonmet.ac.uk/8403/>
- [54]. McIntyre, A., & Roberts, N. (2020). Challenges in data integration for intelligence: A survey of data redundancy and management practices. *Intelligence & Analytics*, 3(4), 98-117.
- [55]. Mehta, R., & Craig, D. (2021). Predictive capabilities of data management in threat intelligence: Evidence from machine learning applications. *Journal of Threat Analysis*, 9(1), 111-132.
- [56]. Mix, D. E. (2013). The European Union: foreign and security policy. https://upload.wikimedia.org/wikipedia/commons/3/31/207785_The_European_Union_Foreign_and_Security_Policy_%28IA_207785TheEuropeanUnionForeignandSecurityPolicy-crs%29.pdf
- [57]. Moritz, J. F., & Rheign, C. (2019). *Theories of intelligence, surveillance, and security*. Oxford University Press.
- [58]. Mursu, A. (2002). Information systems development in developing countries: Risk management and sustainability analysis in Nigerian software companies (No. 21). University of Jyväskylä.
- [59]. Musa, Y., Mohammed, A., & Okoro, E. (2021). Data sharing protocols in Nigerian security response systems. *African Journal of Security*, 8(3), 76-90.
- [60]. Myers, M. C. (2024). Data Privacy Laws in the United States and Germany: Implications for Genomics Research and Personalized Medicine (Doctoral dissertation, University of Pittsburgh). <http://d-scholarship.pitt.edu/46045/>
- [61]. Nadarajah, G., & Param, V. (2020). Cybersecurity: To enforce or educate? A critical review. *ICTACT Journal on Soft Computing*, 10(3), 234-242. doi: 10.21917/ijsc.2020.0366
- [62]. Ndubuisi, O., Ikwuagwu, T. & Igboanusi, H. (2016). Challenges of Security and Intelligence in Nigeria: Current Imperatives. *Mediterranean Journal of Social Sciences*, 7(5), 112-123
- [63]. Ngcece, S., & Mkhize, S. M. (2023). An Exploratory Study of the South African Police Services (SAPS) Systems in Combating Cybercrime. In *Cybercrime and Challenges in South Africa* (pp. 159-175). Singapore: Springer Nature Singapore.
- [64]. NIST. (2020). The impact of centralized data management on response times in intelligence agencies. National Institute of Standards and Technology Report, 5, 25-34.
- [65]. Nte, N. D., Enoke, B. K., & Abubakar, I. (2022). Technical intelligence and security management within the Nigerian territorial waters: The Nigerian navy challenge. *Unnes Law Journal*, 8(1), 179-206. <https://journal.unnes.ac.id/sju/ulj/article/view/56453>
- [66]. Nweke, E. N. (2011). Rethinking national security in Nigeria: Analysis of predisposing conditions and prospects for stable polity. *Journal of Security Strategies*, 7(14), 101-116. <https://arastirmax.com/en/system/files/dergiler/262/makaleler/14/arastirmax-nijeryada-ulusal-guvenligi-yeniden-dusunmek-istikrarli-bir-yonetim-icin-kosullari-belirleme-analizi-gelecege-yonelik-beklentiler.pdf>
- [67]. Oatley, G. (2017). Using Big Data to Improve Intelligence-Gathering and Analysis. The MITRE Corporation. <https://www.mitre.org/publications/technical-papers/using-bigdata-to-improve-intelligence-gathering-and-analysis>
- [68]. Oche, O. (2014). Information, Intelligence and Security: Overview of the Current Security Situation in Nigeria. *African Journal of International Affairs & Development*, 17(2), 7. <https://search.proquest.com/openview/d40fec9a407197248f718cf497d46cdd/1?pq-origsite=gscholar&cbl=856342>
- [69]. Ogu, E. C., & Oyerinde, O. D. (2014). ICT and national security in developing and underdeveloped countries—the Good, the bad and the ugly: a case study of Nigeria’s cyberspace. *International Journal of Computer Science and Information Technologies* Vol. 5;No. 4; Pp 5625-5633
- [70]. Ogunkoya, E., Olagunju, O., & Adewumi, O. (2016). National security of Nigeria: An appraisal of the nation’s intelligence and security system. *International Journal of Social Science and Humanity*, 6(3), 196-201.
- [71]. Okonkwo, J., & Ibe, F. (2021). Challenges of data fragmentation in Nigerian intelligence agencies. *Nigerian Security and Intelligence Journal*, 10(3), 142-159.
- [72]. Olabanji, S. O., Marquis, Y., Adigwe, C. S., Ajayi, S. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-driven cloud security:



- Examining the impact of user behavior analysis on threat detection. *Asian Journal of Research in Computer Science*, 17(3), 57-74.
- [73]. Oladun, F., & Ola, K. (2018). Nigeria's intelligence and security system: Issues and prospects. *International Journal of Security Studies*, 7(1), 8-19. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4709384
- [74]. Olaniran, O. (2022). Success factors influencing cyber security risk management implementation: the cases of large Nigerian organisations (Doctoral dissertation, Coventry University) <https://pureportal.coventry.ac.uk/files/57155582/file>
- [75]. Onugha, C. V. (2018). Partners in national cyber security strategy?: An analysis of cyber security strategies of Ministry of Defence and police in UK (Doctoral dissertation, London Metropolitan University). <http://repository.londonmet.ac.uk/id/eprint/5047>
- [76]. Opara, R. I. (2024). The Legal Framework for Information Security in the Age of Digital Identity in Nigeria. *East African Journal of Law, Policy and Globalization*, 1(2). <https://journal.kiut.ac.tz/index.php/eajlpg/article/view/111>
- [77]. Oppermann, D. (2014). Internet Governance and Cybersecurity in Brazil. In Dane, Felix: *Multilateral Security Governance, Conference of Forte de Copacabana* (Vol. 11, pp. 167-181). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2587178
- [78]. Orb, A., Eisenhauer, L., & Wynaden, D. (2001). Ethics in qualitative research. *Journal of Nursing Scholarship*, 33(1), 93-96.
- [79]. Pallant, J. (2020). *SPSS Survival Manual: A Step by Step Guide to Data Analysis using IBM SPSS*. McGraw-Hill.
- [80]. Parsons, T. (1951). *The Social System*. Routledge.
- [81]. Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods*. Sage.
- [82]. Paulus, D., de Vries, G., Janssen, M., & Van de Walle, B. (2023). Reinforcing data bias in crisis information management: The case of the Yemen humanitarian response. *International Journal of Information Management*, 72, 102663.
- [83]. Pestana, G., & Sofou, S. (2024). Data Governance to Counter Hybrid Threats against Critical Infrastructures. *Smart Cities*, 7(4), 1857-1877. <https://www.mdpi.com/2624-6511/7/4/72>
- [84]. Petersen, K. L., & Tjalve, V. S. (2018). Intelligence expertise in the age of information sharing: public-private 'collection' and its challenges to democratic control and accountability. *Intelligence and National Security*, 33(1), 21-35. <https://www.tandfonline.com/doi/abs/10.1080/002684527.2017.1316956>
- [85]. Prasad, S., & Bhattacharya, K. (2019). Interoperability in counter-terrorism units: A multi-case analysis of the U.S. and Europe. *International Journal of Security Studies*, 15(2), 233-248.
- [86]. Rantala, S., Swallow, B., Paloniemi, R., & Raitanen, E. (2020). Governance of forests and governance of forest information: Interlinkages in the age of open and digital data. *Forest Policy and Economics*, 113, 102123. <https://www.sciencedirect.com/science/article/pii/S1389934118305598>
- [87]. Rehan, H. (2024). AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, 1(1), 132-151.
- [88]. Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age: a global review of legislation and enforcement. *International Journal of Applied Research in Social Sciences*, 6(1), 73-88.
- [89]. Repetto, M., Carrega, A., & Rapuzzi, R. (2021). An architecture to manage security operations for digital service chains. *Future Generation Computer Systems*, 115, 251-266. <https://www.sciencedirect.com/science/article/pii/S0167739X20303290>
- [90]. Rubin, H. J., & Rubin, I. S. (2012). *Qualitative Interviewing: The Art of Hearing Data*. Sage.
- [91]. Sarjito, A. (2024). Data Security and Privacy in the Digital Era: Challenges for Modern Government. *JIAN-Jurnal Ilmiah Administrasi Negara*, 8(3), 01-13. <https://ojs.ejournalunigoro.com/index.php/JIAN/article/view/933>



- [92]. Smith, A. (2020). The Role of Intelligence Systems in National Security. *International Journal of Information Security and Privacy*, 14(2), 38-46.
- [93]. Spyropoulos, A. Z., Bratsas, C., Makris, G. C., Garoufallou, E., & Tsiantos, V. (2023). Interoperability-Enhanced Knowledge Management in Law Enforcement: An Integrated Data-Driven Forensic Ontological Approach to Crime Scene Analysis. *Information*, 14(11), 607.
- [94]. Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs*, 92(5), 1079-1105.
<https://academic.oup.com/ia/article-abstract/92/5/1079/2688134>
- [95]. Sutherland, E. (2017). Governance of cybersecurity-the case of South Africa. *The African Journal of Information and Communication*, 20, 83-112.
https://www.scielo.org/za/scielo.php?pid=S2077-72132017000100005&script=sci_arttext
- [96]. Umaru, B. (2018). Investigating issues in intelligence gathering in Nigeria. *Heliyon*, 4(11), e00950.
<https://doi.org/10.1016/j.heliyon.2018.e00950>
- [97]. Wanekeya, E. (2023). Effectiveness of Domestic Data Protection Laws in African Countries-a Case Study of the Data Protection Law in Kenya (Doctoral dissertation, University of Nairobi).
<http://erepository.uonbi.ac.ke/handle/11295/163963>
- [98]. Wenger, A., & Cavely, M. D. (2022). The ambiguity of cyber security politics in the context of multidimensional uncertainty. *Cyber Security Politics*, 239.
<https://library.oapen.org/bitstream/handle/20.500.12657/52574/9781000567113.pdf?sequence=1 - page=254>
- [99]. Wilshusen, G.C., Crosland, L., Businsky, C., Guerrero, R., Glover, N., Ip, A., Jahan, F., Mozo, C. and Wallace, S., 2015. Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs.
<https://apps.dtic.mil/sti/citations/trecms/AD1099160>
- [100]. Wirth, A. (2018). The times they are a-changin': Part two. *Biomedical Instrumentation & Technology*, 52(3), 236-240.
- [101]. Wu, L., & Lee, H. (2022). Technological challenges in data management for East Asian security agencies. *Asian Journal of Intelligence Studies*, 12(1), 117-134.
- [102]. Yin, R. K. (2014). *Case Study Research: Design and Methods*. Sage.
- [103]. Zhang, C. (2022). Legitimacy of China's Counter-Terrorism Approach: The Mass Line Ethos. Springer Nature.