International Journal of Innovative Information Systems & Technology Research 13(4):462-470, Oct-Dec, 2025

 www.seahipublications.org ISSN: 2467-8562

doi:10.5281/zenodo.18076310

Cybersecurity Risk Challenges in Unmanned Aerial Vehicles Operations: Empirical Evidence from Nigerian Unmanned Aerial Vehicles Stakeholders

M. F. Kyari[1], F. N. Ogwueleka[2], and M. O. Adenomon[3]

[1,3] Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria
[2] University of Abuja, Nigeria

ABSTRACT
The growing use of Unmanned Aerial Vehicles (UAVs) across Nigeria in civil, commercial, and defense sectors presents significant opportunities in surveillance, logistics, agriculture, and infrastructure monitoring. However, this rapid adoption also raises serious cybersecurity concerns, threatening UAV operations' safety, reliability, and integrity. This study investigates these challenges by examining the nature and impact of cyber threats facing UAV stakeholders in Nigeria. Using a mixed-method approach, data were collected from 85 participants, including UAV operators, cybersecurity experts, and government officials. Quantitative data were gathered through structured questionnaires to assess the prevalence of cyber threats, security practices, and perceived risks. Qualitative insights were obtained via semi-structured interviews, offering a deeper understanding of stakeholder experiences and perspectives. The data was analyzed using descriptive statistics, regression, and thematic analysis. Key threats identified include Global Positioning System spoofing, signal jamming, and unauthorized access, all of which pose serious operational, safety, and data security risks. These findings underscore the urgent need for proactive cybersecurity strategies tailored to UAV systems. Overall, the study highlights the critical importance of addressing cybersecurity vulnerabilities to ensure the safe, secure, and sustainable integration of UAV technology into Nigeria's socio-economic development. The study recommends establishing national UAV cybersecurity guidelines, implementing robust risk management practices, and enacting regulatory reforms. It also calls for stronger inter-agency collaboration to enhance Nigeria's UAV cybersecurity framework.
Keywords: Unmanned Aerial Vehicles, Cybersecurity, Risks, Technology, Cyber threats, Vulnerabilities.

1. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have emerged as powerful critical tools in various sectors, including agriculture, surveillance, logistics, emergency response, and environmental monitoring, with the capacity to bring about transformative benefits across a multitude of sectors. Their applications are diverse and impactful: in security and surveillance, UAVs provide enhanced situational awareness, enabling more effective monitoring of critical infrastructure and rapid response to security incidents (Labib et al., 2021). In agriculture, they facilitate precision farming techniques, optimizing crop yields and resource management (Kumar et al., 2023; Lin et al., 2023), and in logistics, they offer the potential for efficient delivery of goods, particularly in challenging terrains, and in disaster

response. UAVs play a vital role in damage assessment, search and rescue operations, and the delivery of essential supplies (Kumar et al., 2023; Lin et al., 2023). The adoption of UAV technology promises to drive significant advancements and improve operational efficiencies in various fields.

In Nigeria, their adoption is increasing across both public and private domains due to their cost-effectiveness, accessibility, and versatility (Adeleke & Ogunleye, 2021). However, the growing reliance on UAVs raises significant cybersecurity concerns. Given their dependence on wireless communication systems, GPS navigation, and cloud-based data storage, UAVs are particularly vulnerable to cyber threats such as spoofing, jamming, data interception, and unauthorized remote control (Ajayi, 2022).

Despite the increasing recognition of the severity and urgency of these cybersecurity threats, Nigeria currently lacks a robust, comprehensive, and contextually relevant cybersecurity risk framework explicitly tailored to the unique operational characteristics and vulnerabilities of UAVs. This absence of a dedicated framework creates a significant vulnerability gap, leaving UAV operators, organizations, and regulatory bodies ill-equipped to effectively assess, mitigate, and manage the diverse range of cybersecurity risks associated with UAV operations. The lack of standardized guidelines and best practices further exacerbates the problem, leading to inconsistent security measures and increased susceptibility to cyberattacks.

Cybersecurity risk in UAV operations poses multi-dimensional challenges. From the compromise of sensitive surveillance data to the hijacking of flight control systems, such risks threaten not only mission integrity but also public safety and national security (Chukwu & Obi, 2020). In Nigeria, these issues are exacerbated by regulatory gaps, low cybersecurity awareness, and limited technical capacity among UAV stakeholders (Nwosu & Adebanjo, 2022). Despite the growing deployment of drones in commercial and governmental contexts, little empirical research exists on how Nigerian UAV operators perceive, manage, and mitigate cybersecurity risks.

However, the realization of these substantial benefits is increasingly jeopardized by the growing prevalence of cybersecurity risks, especially in developing countries such as Nigeria. While UAVs offer numerous advantages, their reliance on wireless communication channels, interconnected systems, and software-driven controls inherently exposes them to a range of cyberattacks. These attacks can compromise the operational integrity of UAVs, leading to disruptions, data breaches, and even physical damage, thereby undermining their effectiveness and posing safety hazards.

In the specific context of Nigeria, the cybersecurity threats facing UAVs are not merely theoretical concerns but present real and escalating challenges. Cyberattacks, including GPS spoofing (the manipulation of a UAV's navigation system to provide false location data) and communication jamming (the intentional disruption of control and communication links), have been weaponized by insurgents and criminal groups operating within the country (Safitra et al., 2023). These malicious actors exploit UAV vulnerabilities to carry out unauthorized surveillance, disrupt security operations, or even employ UAVs as part of their operations, posing a significant threat to both national security and civilian safety.

This study endeavours to provide crucial empirical insights into the precise nature, frequency, and potential impact of cyber threats affecting UAVs operating within Nigeria, and seeks to bridge that gap by providing empirical evidence on cybersecurity challenges faced by UAV stakeholders in Nigeria. By gathering and rigorously analyzing data from key stakeholders with direct involvement in UAV activities, including UAV operators with diverse experience levels, cybersecurity experts possessing specialized knowledge of UAV vulnerabilities, and regulatory officials responsible for overseeing UAV operations, this study aims to offer practical, evidence-based, and stakeholder-informed solutions. It investigates key vulnerabilities, evaluates current protective measures, and proposes strategic recommendations to bolster UAV cybersecurity resilience. The ultimate goal is to contribute to the development of effective strategies and policies that will strengthen UAV cybersecurity posture, promote the safe and responsible use of UAV technology, and enable Nigeria to fully harness the benefits of UAVs while mitigating the associated risks. Understanding these dynamics is essential for developing a comprehensive national UAV cybersecurity framework tailored to Nigeria’s unique operational, infrastructural, and socio-political environment.

2. Review of Related Studies

Extensive literature exists on the cybersecurity risks inherent in UAV operations. Researchers globally have highlighted the susceptibility of UAVs to a range of cyber attacks. For instance, Gupta et al. (2020) demonstrated how GPS spoofing could redirect UAVs from their intended path, while Kwon et al., (2018) analyzed man-in-the-middle attacks capable of intercepting control signals. These vulnerabilities are often attributed to weak encryption, open communication protocols, and inadequate authentication mechanisms in commercial UAV systems. The existing body of research increasingly acknowledges the escalating cybersecurity threats confronting UAVs across various operational domains. Studies have consistently demonstrated that UAVs are vulnerable to a range of cyberattacks, which can compromise their functionality, safety, and the security of the environments in which they operate.

Specifically, research conducted by Malik (2024) and Kong (2021) has highlighted the growing threats of GPS spoofing, signal jamming, and malware infections targeting UAV systems. These studies provide valuable insights into the technical aspects of these attacks, including the mechanisms by which they are executed and their potential consequences. GPS spoofing, for instance, involves deceiving the UAV's navigation system with false location data, potentially leading to unauthorized redirection or even the hijacking of the vehicle. Signal jamming disrupts the communication links between the UAV and its operator, resulting in loss of control and potential crashes. Malware infections can compromise the UAV's onboard systems, enabling malicious actors to exfiltrate sensitive data or manipulate the UAV's behaviour. Clark, et al. (2019) explored cybersecurity concerns in military UAVs and emphasized the growing need for resilient architectures that incorporate intrusion detection systems, end-to-end encryption, and adaptive firewalls. Studies by Zhang & Du (2021) have further proposed blockchain and AI-driven approaches to UAV cybersecurity, especially for fleet operations and swarming behaviours.

Furthermore, Zemlianko et al. (2023) introduced innovative risk models, such as the IMECA-based approach, for assessing cybersecurity risks in UAV fleets. These models offer structured frameworks for evaluating the likelihood and impact of various cyber threats, enabling UAV operators and organizations to prioritize security measures and allocate resources effectively. While these models contribute to the theoretical understanding of UAV cybersecurity risk management, their practical applicability and effectiveness in diverse operational settings require further empirical validation.

While the aforementioned studies provided valuable insights into UAV cybersecurity threats and risk management, a significant limitation was their general oversight of the unique empirical contexts of developing nations, such as Nigeria. The cybersecurity challenges faced by UAV operators in these regions are often compounded by specific socio-economic, technological, and regulatory factors that are not adequately addressed in the existing literature.

In contrast, studies specifically focused on Nigeria, such as those by Olowonihi (2024) and Eghweree et al. (2023), shed light on the distinctive cybersecurity challenges within the country's UAV landscape. These studies emphasized the critical role of factors such as insurgency and regulatory weaknesses in exacerbating the vulnerabilities of UAVs to cyberattacks. The ongoing insurgency in certain regions of Nigeria created a heightened threat environment, where UAVs can be targeted or even weaponized by non-state actors. Weak regulatory frameworks and enforcement mechanisms contributed to a lack of standardized security practices and increased the risk of unauthorized UAV operations.

In Nigeria, studies on UAV adoption tend to focus on applications in agriculture, logistics, and disaster management (Akinola et al., 2021; Eze & Okonkwo, 2022). However, cybersecurity in UAV operations has received limited attention. One of the few relevant studies, by Musa & Yekini (2023), identified key vulnerabilities in UAV command-and-control systems used in northern Nigeria’s counterinsurgency operations. Their findings indicated a lack of cybersecurity training among operators and insufficient incident response protocols.

Additionally, Ogunyemi & Olatunji (2022) noted that many UAV vendors in Nigeria do not conduct adequate security assessments before deployment. There is also limited coordination between regulators like the Nigerian Civil Aviation Authority (NCAA) and cybersecurity agencies such as the National Information Technology Development Agency (NITDA), leading to fragmented oversight.

However, even these Nigeria-specific studies often lack the comprehensive empirical investigation needed to fully understand the scope, scale, and impact of UAV cybersecurity challenges in the country. There is a need for research that goes beyond identifying the general threats and vulnerabilities and delves into the practical realities faced by UAV stakeholders in their daily operations.

While global studies offer insight into advanced technological solutions, they may not be directly transferable to Nigeria's socio-technical context due to infrastructural limitations and regulatory inconsistencies. The dearth of empirical data on how Nigerian UAV operators perceive and respond to cybersecurity risks creates a critical knowledge gap. This study addresses that gap by empirically investigating the experiences and strategies of UAV stakeholders in Nigeria, providing contextual evidence to support both policy and technological interventions.

This study addresses this critical gap in the literature by gathering and analyzing field-based evidence directly from key Nigerian stakeholders involved in UAV activities. By incorporating the perspectives and experiences of UAV operators, cybersecurity experts, and regulatory officers, this research aims to provide a more nuanced, contextually relevant, and practically applicable understanding of UAV cybersecurity challenges in Nigeria. The empirical findings of this study will inform the development of evidence-based recommendations and strategies to strengthen UAV cybersecurity and promote the safe and responsible use of UAV technology in the country.

3. METHODOLOGY

This study adopted a mixed-method research approach to comprehensively investigate cybersecurity risk challenges in UAV operations within the Nigerian context. The mixed-method approach was chosen to leverage the strengths of both quantitative and qualitative research paradigms, enabling a more nuanced and in-depth understanding of the complex issues at hand. Quantitative methods were employed to provide statistical data on the prevalence of cybersecurity threats and the adoption of security practices, while qualitative methods were used to explore the experiences, perspectives, and contextual factors influencing UAV cybersecurity in Nigeria (Creswell & Creswell, 2018; Field, 2018).

The study is exploratory and descriptive. An exploratory design was suitable for examining under-researched phenomena, while the descriptive component helped to quantify stakeholder perceptions and behaviours related to UAV cybersecurity in Nigeria. The combination of survey instruments and semi-structured interviews allowed for empirical triangulation and enhanced the validity of findings.

The target population for this study consisted of key stakeholders involved in UAV operations within Nigeria. This population included UAV operators with varying levels of experience, cybersecurity experts possessing specialized knowledge of UAV vulnerabilities and threats, and regulatory officers responsible for overseeing UAV activities and enforcing relevant regulations. These stakeholder groups were selected to ensure a comprehensive representation of the diverse perspectives and experiences relevant to UAV cybersecurity in the country.

The study employed a combination of sampling techniques to select participants. For the UAV operator group, stratified random sampling was utilized to ensure representation across different types of UAV operations (e.g., commercial, agricultural, security). This technique involved dividing the population of UAV operators into subgroups (strata) based on their operational domain and then randomly selecting participants from each stratum. For the selection of cybersecurity experts and regulatory officers, convenience sampling was employed due to the specialized nature of these roles and the limited number of individuals with the requisite expertise. While convenience sampling may have limitations in terms of generalizability, it was deemed appropriate for this exploratory phase of the research, allowing for the inclusion of valuable insights from key informants (cite sources on stratified random sampling and convenience sampling).

The sample size for the quantitative survey was 85 participants, and for the qualitative interviews, 15 key informants, including representatives from government agencies, drone operators, and cybersecurity

experts, were used. The sample size was determined based on feasibility, access to participants, and saturation in qualitative insights.

Data was collected using two primary methods. Quantitative data was gathered through structured questionnaires administered via Google Forms. This online platform facilitated efficient data collection from a geographically dispersed sample. The questionnaire was designed to collect information on demographics, the prevalence of different cybersecurity threats, the adoption of security measures, and the perceived impact of cybersecurity breaches. Qualitative data were collected through semi-structured interviews conducted either in person or via telephone. These interviews allowed for more in-depth exploration of participants' experiences, opinions, and perspectives on UAV cybersecurity challenges and potential solutions. The semi-structured format provided a balance between structure and flexibility, enabling the researchers to cover key topics while also allowing participants to elaborate on issues of particular relevance to them (Bryman, 2016; Creswell & Creswell, 2018).

The collected data was analyzed using appropriate techniques for each data type. Quantitative data were analyzed using descriptive statistics, including means and frequencies, to summarize the characteristics of the sample and the distribution of variables. Regression analysis was performed using SPSS software to examine the relationships between different variables, such as the adoption of security measures and the occurrence of cybersecurity incidents. Qualitative data obtained from the interviews were analyzed using thematic analysis involving the systematic process of coding and categorizing the data to identify recurring themes, patterns, and insights related to UAV cybersecurity challenges and potential mitigation strategies (Field, 2018; Creswell & Creswell, 2018)

4. RESULTS AND DISCUSSION

The empirical insights garnered from this study offer a comprehensive understanding of the current cybersecurity landscape impacting Unmanned Aerial Vehicle (UAV) operations in Nigeria. The demographic analysis of the respondents provides a robust foundation for these insights, reflecting a representative sample of key stakeholders. Specifically, the gender distribution of 60% male and 40% female indicates a commendable breadth of perspectives. Crucially, the occupational breakdown, with UAV operators constituting the largest group at 35%, underscores their invaluable frontline experience regarding the practical cybersecurity challenges. Cybersecurity specialists, making up 25% of respondents, provided essential technical depth, while the significant portion (45%) reporting 4 to 7 years of experience confirms an experienced participant group capable of offering informed insights into the evolving nature of these challenges.

Our investigation into cybersecurity threats unearthed several prevalent and pressing issues within Nigerian UAV operations. GPS spoofing emerged as the most frequently reported threat, cited by 87% of respondents. This alarming prevalence strongly suggests that malicious actors are actively exploiting vulnerabilities in UAV navigation systems to manipulate location data, posing a severe risk of mission sabotage or unauthorized diversion. Equally concerning is signal jamming, reported by 79% of respondents, highlighting the critical vulnerability of UAV communication links to disruption. Such jamming can lead to immediate loss of control, compromise sensitive data transmissions, and significantly escalate the risk of operational accidents. Furthermore, unauthorized access, reported by 63%, points to substantial deficiencies in access controls and broader security measures across UAV systems, particularly within the commercial sector, where inadequately secured drones are highly susceptible to hijacking and sensitive data breaches.

An in-depth analysis of the cybersecurity mitigation practices among Nigerian UAV operators presents a disconcerting picture of mixed adoption. While a majority of operators have implemented basic encryption for communication links, the uptake of more advanced security measures remains critically limited. Our findings indicate a notably low implementation of end-to-end security protocols, which are essential for safeguarding data integrity across the entire communication chain. Similarly, the deployment of anomaly detection systems, vital for identifying suspicious activities indicative of cyberattacks, is not widespread. Moreover, the study points to a pervasive limited adoption of proactive cybersecurity

frameworks, suggesting that many UAV operators and organizations lack a systematic and comprehensive approach to managing inherent cybersecurity risks. This predominantly reactive posture leaves UAVs acutely vulnerable to an increasingly sophisticated array of cyber threats, significantly escalating the potential for severe security breaches and operational failures.

Qualitative insights derived from interviews with experts provided crucial contextual depth and affirmed the systemic nature of these challenges. Experts consistently underscored a critical gap in cybersecurity training for UAV operators, emphasizing the urgent need for comprehensive programs to adequately equip personnel with the requisite knowledge and skills for identifying, preventing, and responding to cyberattacks. A major concern articulated was the lack of rigorous enforcement of national cybersecurity standards, a factor directly contributing to inconsistent security practices and a general deficiency in accountability across the sector. Furthermore, experts highlighted the minimal coordination and communication between UAV regulators and cybersecurity bodies. This institutional fragmentation actively hinders the development of a unified and effective national approach to addressing UAV cybersecurity challenges, creating detrimental silos that impede information sharing, coordinated incident response, and the formulation of holistic security strategies.

4.1 Perceived Cybersecurity Risks

Respondents rated their perception of various cybersecurity risks on a 5-point Likert scale (1 = Not a threat, 5 = Severe threat).

Table 1: Perceived Cybersecurity Risks

Cybersecurity Risk	Mean Score	Interpretation
GPS Spoofing	4.30	High perceived threat
Signal Jamming	4.11	High perceived threat
Data Interception	4.02	High perceived threat
Unauthorized Access (Hacking)	3.95	Moderate–High threat
Malware Insertion	3.72	Moderate threat
Insider Threats	3.41	Moderate threat

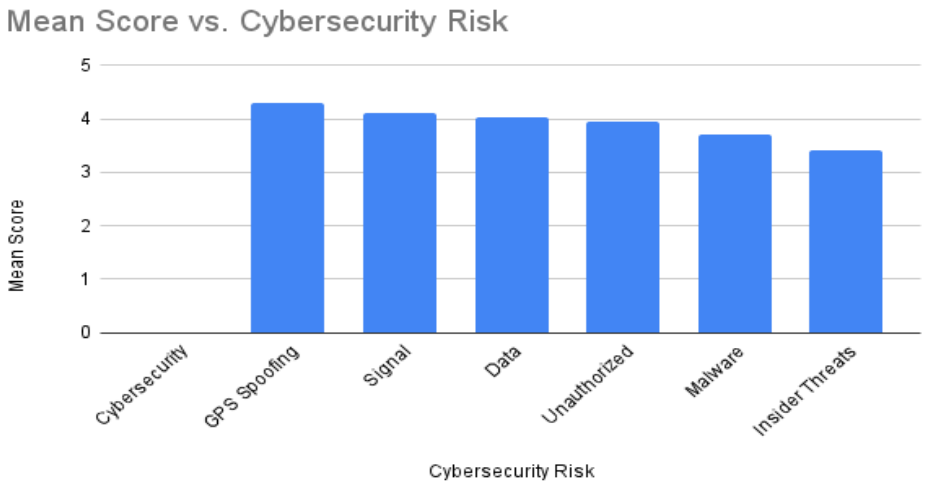

Figure 1: Perceived Cybersecurity Risks

4.2 Cybersecurity Preparedness

Table 2: Cybersecurity Preparedness

Security Measure	Adoption Rate
Use of encryption for data transmission	38%
Regular system/software updates	46%
Multi-factor authentication for drone access	32%
Cybersecurity training for personnel	27%
Use of VPNs or secured networks for control links	21%

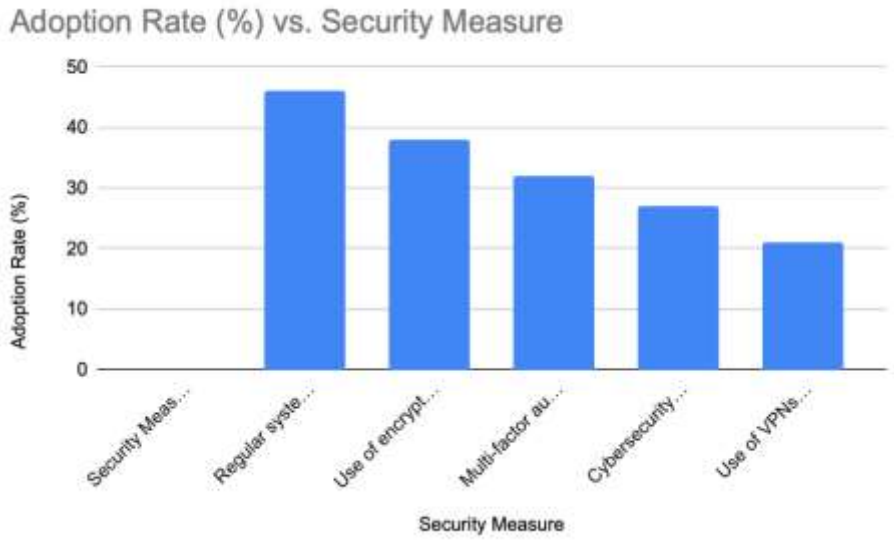

Figure 2: Cybersecurity Preparedness

The above suggests a significant gap in cybersecurity readiness among UAV operators in Nigeria. The study identified a pronounced 'awareness-preparedness paradox' within the domain of UAV cybersecurity. Respondents consistently demonstrated a high level of awareness regarding critical threats, notably GPS spoofing and signal jamming, acknowledging their potential for severe operational impact. However, this high awareness did not correspondingly translate into high levels of practical cybersecurity preparedness. Indicators such as the limited adoption of encryption for communications, insufficient specialized training for personnel, and the lack of robust security measures for ground control systems suggest a considerable gap in current practices. These preliminary findings imply that despite recognizing the dangers, stakeholders may face systemic, resource, or knowledge barriers preventing them from implementing necessary safeguards. Addressing this paradox is crucial; future efforts must prioritize not only continuous threat education but also the development and widespread adoption of practical, accessible, and targeted capacity-building programs to bridge the operational cybersecurity gap in UAV deployments."

This study's findings so far confirm the assertions of Nwosu and Adebanjo (2022), revealing a deeply fragmented cybersecurity governance structure for Unmanned Aerial Vehicles (UAVs) in Nigeria. Our data shows that essential regulatory and operational entities, including the Nigerian Civil Aviation Authority (NCAA), the National Information Technology Development Agency (NITDA), and military bodies, function largely in isolation. This siloed operational model directly results in inconsistent standards, varied applications, and uneven enforcement of cybersecurity protocols. Without a cohesive

and comprehensive regulatory framework, compliance becomes ambiguous, jurisdictional overlaps emerge, and significant gaps in cybersecurity oversight for UAV operations persist. Ultimately, this fragmentation impedes the creation of robust security measures, complicates effective incident response, and undermines accountability, presenting a critical systemic challenge to the development of a secure and resilient UAV ecosystem in Nigeria.

The findings of this study provided compelling empirical evidence that cybersecurity threats pose a significant and growing risk to the operational integrity, safety, and reliability of Unmanned Aerial Vehicles (UAVs) operating within Nigeria. The analysis of data collected from key stakeholders reveals that while specific threats such as GPS spoofing and signal jamming are indeed prevalent and cause considerable disruption to UAV operations, the underlying and more pervasive issue lies in the lack of proactive cybersecurity risk management strategies and insufficient institutional preparedness to address these evolving challenges effectively. This deficiency creates a vulnerable environment where UAVs are susceptible to a wide range of cyberattacks, potentially leading to severe consequences.

To mitigate these risks and strengthen the cybersecurity posture of UAV operations in Nigeria, this study recommends a set of targeted and actionable strategies. Firstly, there is an urgent need for the development and implementation of comprehensive national UAV cybersecurity guidelines. These guidelines should provide clear standards, best practices, and regulatory frameworks to govern the secure operation of UAVs across all sectors. Secondly, the study strongly advocates for mandating the use of robust encryption protocols and multi-factor authentication mechanisms for all UAV systems. These security measures are essential to protect communication links, prevent unauthorized access, and safeguard sensitive data transmitted by UAVs. [1] Thirdly, the implementation of comprehensive and ongoing training programs for UAV operators is crucial. These programs should equip operators with the necessary knowledge and skills to identify, prevent, and respond effectively to cybersecurity threats, promoting a culture of security awareness and responsibility.

While this study provided valuable insights into the current state of UAV cybersecurity in Nigeria, there are several avenues for future research to further enhance our understanding and inform the development of more effective mitigation strategies. Longitudinal studies are needed to evaluate the long-term impact and effectiveness of the recommended cybersecurity strategies, providing empirical evidence of their success and identifying areas for further improvement. Furthermore, it is essential to extend the investigation to UAV deployments in high-risk conflict zones within Nigeria. These environments present unique and heightened cybersecurity challenges due to the presence of non-state actors, the potential for weaponization of UAVs, and the complex interplay of security threats. Future research should also explore the integration of emerging technologies, such as artificial intelligence and blockchain, to enhance UAV cybersecurity.

CONCLUSION

This study underscores the urgent need for a proactive, comprehensive, and collaborative approach to address the growing cybersecurity risks facing UAV operations in Nigeria. By implementing the recommended strategies and pursuing further research, it is possible to create a safer, more secure, and more resilient UAV ecosystem, enabling Nigeria to fully harness the transformative benefits of UAV technology while mitigating its inherent cybersecurity vulnerabilities.

REFERENCES

Adeleke, A., & Ogunleye, T. (2021). The emerging role of drones in Nigerian agricultural innovation. *African Journal of Technology & Development*, 8(1), 45–58.

Ajayi, O. (2022). Navigating drone security in Africa: Challenges and prospects. *International Journal of Cybersecurity Studies*, 5(3), 89–104.

Akinola, K., Yusuf, B., & Salami, R. (2021). Application of UAVs in logistics and agriculture: A Nigerian perspective. *Journal of African Technological Applications*, 6(2), 73–84.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Chukwu, N., & Obi, L. (2020). Cybersecurity challenges in Nigeria's drone surveillance system. *West African Journal of Security Studies*, 9(4), 112–130.

Clark, J., Kumar, S., & Alam, M. (2019). Cyber risk in military drone operations: A systems-based approach. *Journal of Defense Technology*, 23(2), 155–171.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications. 12. Elmarady, M. A., & Hefny, H. A. (2021). Cybersecurity risk assessment methodology for aviation. IEEE Access, 9, 76901-76916.

Davidson, P., Billington, J., & Ganin, M. (2016). Man-in-the-middle attack on a UAV. In 2016 15th International Conference on Control Automation Robotics and Vision (ICARCV) (pp. 1-6). IEEE.

Eghweree, O., Adegbite, A., & Yusuf, K. (2023). Assessing UAV cybersecurity risks in Nigeria: Threats, challenges, and mitigation strategies. African Journal of Cybersecurity Research, 5(2), 112–130.

Eze, U., & Okonkwo, D. (2022). Drones in Nigerian disaster response: A systematic review. *Journal of Disaster and Emergency Management*, 4(1), 21–35.

Field, A. (2018). Discovering statistics using IBM SPSS statistics (5th ed.). SAGE Publications.

Field, A. (2018). Discovering statistics using IBM SPSS statistics (5th ed.). SAGE Publications.

Garba, A. A., & Samuel, O. (2020). Assessment of cybersecurity awareness and practices among undergraduate students of a Nigerian university. International Journal of Computer Networks and Applications (IJCNA), 7(3), 164.

Gupta, P., Singh, A., & Roy, A. (2020). Drone cyber attacks: Techniques and countermeasures. *IEEE Transactions on Aerospace and Electronic Systems*, 56(5), 3854–3865.

Hartmann, T., & Apitz, R. (2013). Concepts of risk management. In Risk Management (pp. 3-17). Carl Hanser Verlag GmbH & Co. KG.

Jain, R., & Pamula, R. (2015). Threats, attacks and counter measures in MANETs: A survey. International Journal of Computer Applications, 114(11).

Kong, P. Y. (2021). A survey of cyberattack countermeasures for unmanned aerial vehicles. IEEE Access, 9(2), 148244–148263. https://doi.org/10.1109/ACCESS.2021.3124996

Kumar, R., Singh, V., & Patel, A. (2023). Statistical methods for behavioral and social sciences: An applied approach. SAGE Publications.

Kwon, D., Kim, H. J., & Kim, D. H. (2018). Vulnerabilities of commercial drones to over-the-air Wi-Fi hacking. IEEE Access, 6, 4927-4939.

Kwon, D., Kim, H., & Hwang, J. (2018). Security analysis of UAV communication protocols. *ACM Transactions on Cyber-Physical Systems*, 2(4), 23–39.

Lin, Y., Zhao, H., & Chen, M. (2023). Qualitative and quantitative research methods in cybersecurity studies. Routledge.

Malik, S. (2024). Security of unmanned aerial vehicle systems through advanced penetration testing. Journal of Applied Security Research, 32(2), 1–17.

Musa, A., & Yekini, A. (2023). UAV cybersecurity challenges in Nigerian security operations. *Nigerian Journal of Cyber Intelligence*, 2(1), 34–51.

Nwosu, P., & Adebanjo, B. (2022). UAV policy gaps in Nigeria: Regulatory and security perspectives. *Nigerian Journal of Policy Analysis*, 11(2), 67–82.

Ogunyemi, A., & Olatunji, O. (2022). Assessing cyber risks in UAV commercial deployment in Nigeria. *Journal of African Information Systems*, 9(3), 101–117.

Olowonihi, A. (2024). Cybersecurity challenges in unmanned aerial vehicle (UAV) operations: A developing nation's perspective. Journal of Cybersecurity Studies, 12(3), 45–67.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18). https://doi.org/10.3390/su151813369

Zemlianko, H., & Kharchenko, V. (2023). Cybersecurity risk analysis of multifunctional UAV fleet systems: A conceptual model and IMECA-based technique. Radioelectronic and Computer Systems, 4225(4(108)), 152–170. https://doi.org/10.32620/REKS.2023.4.11

Zhang, H., & Du, X. (2021). AI and blockchain integration in UAV security architecture. *IEEE Internet of Things Journal*, 8(9), 7340–7351.