ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

INTEGRATING RMF, TOE, C2M2 AND STS FOR PUBLIC SECTOR UAV PROGRAMMES CYBERSECURITY GOVERNANCE: A NIGERIA CENTRED SURVEY BASED ASSESSMENT FRAMEWORK

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

Corresponding author email: fkyari@gmail.com

ABSTRACT

This paper examines how Nigerian public-sector organisations govern cybersecurity for unmanned aerial vehicle (UAV) programmes and proposes a Nigeria-centred, survey-based assessment framework that integrates the Risk Management Framework (RMF), Technology–Organisation–Environment (TOE) framework, Cybersecurity Capability Maturity Model (C2M2) and Socio-Technical Systems (STS) theory. A mixed-methods design was adopted, combining a survey of 150 public-sector UAV stakeholders with ten semi-structured key informant interviews. Quantitative data were analysed using descriptive statistics and reliability analysis; qualitative data were analysed thematically. The findings show that UAV cybersecurity governance is fragmented and largely reactive, with low capability maturity and weak alignment between technology choices, organisational practices and regulatory requirements. Only 10% of respondents considered their organisations highly prepared, while 25% considered them unprepared. GPS spoofing, signal jamming and unauthorised access were recurrent concerns, and policy gaps, capacity limitations and poor incident reporting further increased exposure. On this empirical base, the paper proposes a Nigeria-centred UAV Cybersecurity Governance Assessment Framework that operationalises RMF, TOE, C2M2 and STS through seven governance dimensions, indicators and maturity levels. The framework is intended to help public institutions diagnose governance gaps, prioritise interventions and monitor improvement over time. It is proposed as a diagnostic tool; longitudinal validation remains future work. The paper concludes that a shift towards proactive, risk-based and capability-driven governance is essential if Nigerian public institutions are to secure UAV assets and missions in an increasingly contested cyber-physical environment.

Keywords: UAV governance; cybersecurity assessment; RMF; TOE; C2M2; STS; Nigeria

1. INTRODUCTION

Unmanned aerial vehicle (UAV) programmes are rapidly diffusing across Nigeria's public sector. Beyond defence and internal security, UAVs now support disaster response, agriculture, environmental monitoring, border management and critical-infrastructure surveillance. As these platforms become embedded in public operations, they aggregate significant cybersecurity risk. Attackers can exploit weaknesses in communication links, navigation systems, ground control stations and data infrastructures to disrupt missions, exfiltrate sensitive information, manipulate decision-making or endanger public safety (Tsao et al., 2022; Wang et al., 2023).

Global discourse has acknowledged these risks, but much of the existing work is situated in highly regulated environments and commercial or purely military domains. In contrast, Nigeria's public-sector UAV programmes operate within a complex governance landscape

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

characterised by overlapping mandates, evolving regulation and heterogeneous technical capacity. How cybersecurity is actually governed across these programmes, and how governance capability can be assessed in a structured and context-sensitive manner, remains under-examined.

This paper addresses that gap. It focuses on cybersecurity governance rather than isolated technical controls and asks: how do Nigerian public-sector institutions currently govern cybersecurity in UAV programmes, and how can their governance capability be assessed in a structured, theoretically grounded and context sensitive manner? The study integrates four complementary lenses: RMF provides a life-cycle view of risk management; TOE foregrounds the interplay of technology, organisation and environment; C2M2 offers graded capability maturity levels; and STS emphasises the joint optimisation of social and technical subsystems. On this foundation, the paper develops a Nigeria-centred, survey-based assessment framework for public-sector UAV cybersecurity governance.

The paper makes three contributions. First, it provides Nigeria-specific empirical evidence on how public institutions structure responsibilities, processes, standards and accountability around UAV cybersecurity. Second, it operationalises RMF, TOE, C2M2 and STS in an integrated governance assessment framework rather than applying them in isolation. Third, it translates the framework into dimensions, indicators and maturity levels that public institutions can use to diagnose gaps and prioritise improvement.

The Nigerian public-sector context adds a further layer of complexity. UAV acquisition, operation and oversight are distributed across defence, security, aviation, communications, ICT and emergency-management institutions, each with its own mandate, budget cycle and risk culture. General aviation regulations address airworthiness and operational safety, while broader cybersecurity instruments address information systems rather than airborne platforms. The result is a governance space in which responsibilities overlap but accountability is diffuse. Understanding how institutions actually navigate this space is essential for designing a framework that is usable rather than merely theoretically elegant (NCAA, 2023; Anghuwo et al., 2024).

2. LITERATURE REVIEW

2.1 UAV cybersecurity governance

Empirical and conceptual work on UAV cybersecurity has expanded considerably. Studies catalogue threats such as GPS/GNSS spoofing, signal jamming, denial of service, malware insertion and unauthorised access, and identify communication links, navigation modules, firmware and ground control stations as key vulnerability points (Tsao et al., 2022; Pandey et al., 2022; Kumar & Chaudhary, 2024). Technical contributions have examined detection, authentication, secure communication and resilience (Nayfeh et al., 2023; Ma et al., 2025; Chandolia et al., 2025; Boukabou et al., 2024). However, a significant proportion of this work focuses on platform-level security, with limited attention to governance: how public institutions structure responsibilities, processes, standards and accountability around cyber risk. Abro et al. (2022), Bai et al. (2024), Hadi et al. (2023), Mekdad et al. (2023), Dehbi et al. (2025), Han et al. (2022), Jung et al. (2024) and Sun et al. (2024) document the breadth of technical threats and the limitations of platform-level countermeasures, reinforcing the need for a governance-level assessment.

Governance, in this paper, refers to the decision rights, accountability arrangements, policies, processes and performance mechanisms through which public institutions direct and control UAV cybersecurity. It is broader than a security policy document and narrower than whole-of-government strategy. It includes who decides, who is accountable, how risk is assessed,

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

how controls are funded, how incidents are reported and how performance is reviewed. This definition draws on RMF's life-cycle logic (NIST, 2018), C2M2's maturity domains (U.S. Department of Energy, 2022) and TOE's attention to organisational and environmental conditions (Tornatzky & Fleischer, 1990).

Where governance is discussed, it is often assumed to align with mature civil aviation and critical-infrastructure regimes typical of developed economies (Pyzynski & Balcerzak, 2021). Tran et al. (2021) and Elmarady and Rahouma (2021) provide structured risk-assessment approaches, while Zemlianko and Kharchenko (2023) and Ficco et al. (2024) offer technical threat and vulnerability methods. These contributions are valuable but do not provide a governance assessment tool for public-sector UAV programmes in a developing-country context.

2.2 Theoretical foundations

Four frameworks inform the study. The NIST Risk Management Framework (NIST, 2018) provides a life-cycle process for categorising systems, selecting and assessing controls, authorising operation and monitoring risk. The Technology-Organization-Environment (TOE) framework explains how technological characteristics, organisational resources and external conditions shape adoption and implementation (Tornatzky & Fleischer, 1990). The Cybersecurity Capability Maturity Model (C2M2) offers graded maturity levels for organisational cybersecurity practices (U.S. Department of Energy, 2022). Socio-Technical Systems (STS) theory emphasises the joint optimisation of technical and social subsystems, including people, processes and culture (Trist & Bamforth, 1951).

These lenses are complementary. RMF supplies the risk logic, TOE the contextual determinants, C2M2 the maturity language and STS the human and organisational explanation. Melaku (2023) and Büyüközkan and Güler (2025) show that adaptive, context-sensitive and maturity-based approaches are better suited to changing threats than static compliance models. Yet these frameworks have not been extensively operationalised for UAV-specific public-sector settings in Nigeria.

Integration is necessary because each framework answers a different question. RMF asks whether a repeatable risk-management process exists. TOE asks whether the technology, organisation and environment are aligned in ways that make the process feasible. C2M2 asks how mature and embedded the process is. STS asks whether people, incentives and organisational culture support or undermine it. A governance assessment that used only one lens would mis-specify the problem: it might document controls without explaining why they are not used, or describe culture without connecting it to accountability and process. The proposed framework therefore treats the four lenses as complementary dimensions of a single assessment.

2.3 Research gap

Two gaps are particularly salient. First, UAV cybersecurity research focuses heavily on technical controls, with limited attention to governance capability in public institutions. Second, very few studies examine African or Nigerian public sector contexts, where institutional capacity, regulatory clarity and resource constraints fundamentally shape what can be achieved (Anghuwo et al., 2024; Kyari et al., 2025). This paper situates itself at the intersection of these gaps. It does not seek to redescribe the global UAV threat landscape but to translate established governance concepts into a Nigeria-centred, empirically informed assessment framework.

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The paper's contribution is therefore twofold. Empirically, it documents how a sample of Nigerian public-sector institutions structure UAV cybersecurity governance and where the weaknesses lie. Conceptually, it translates RMF, TOE, C2M2 and STS into a set of governance dimensions, indicators and maturity levels that can be assessed in practice. This is a modest but useful advance: it does not claim to offer a universal model, but it provides a context-sensitive starting point for public institutions that need to move from informal practice to structured governance.

3. METHODOLOGY

3.1 Research design

The study adopted a mixed-methods, survey-based design. Quantitative data provided breadth across public sector entities, while qualitative data supplied explanatory depth and context. The design was cross-sectional and supports description and association rather than causal inference.

The design was informed by a pragmatic stance. The research question is applied and policy-oriented, and the study was designed to produce usable evidence rather than to test a single theoretical proposition. The quantitative strand provided a broad picture of governance practices and preparedness; the qualitative strand explained how responsibilities, incentives and capacity constraints shaped those practices. The two strands were integrated during interpretation, with qualitative findings used to explain, qualify and extend the survey results.

3.2 Population and sampling

The population comprised Nigerian public-sector organisations that operate or oversee UAV programmes, including defence and security agencies, law enforcement bodies, aviation and ICT regulators, emergency-management agencies and selected ministries, departments and agencies using UAVs for civilian missions. Stratified sampling was used across three strata: security and defense entities; civil public sector operators; and regulatory and oversight bodies. Within strata, respondents were selected using purposive and convenience techniques. The survey yielded 150 valid responses, and ten key informants were interviewed. The achieved sample is not statistically representative of all Nigerian public institutions and is treated as exploratory.

The sampling strategy combined stratification with purposive selection. Stratification ensured that security and defence entities, civil public-sector operators, and regulatory and oversight bodies were represented. Purposive selection within strata was used to reach respondents with direct knowledge of UAV acquisition, operation, security or oversight. This approach is appropriate for an exploratory governance study, but it does not support statistical generalisation. The achieved sample of 150 responses and ten interviews is treated as a purposive evidence base rather than a representative survey of all public institutions.

3.3 Data collection instruments

The questionnaire operationalised the four theoretical lenses. Sections covered organisational profile and UAV use; perceived threats and incidents; existing policies, standards and procedures; technology, organisational and environmental constraints; governance and process indicators aligned to C2M2 domains; and socio-technical factors including roles, skills, training and reporting culture. Items were largely Likert-scaled. The interview guide explored how cybersecurity responsibilities are allocated, how risks are identified and monitored, how control decisions are taken, experiences of incidents and perceptions of regulatory clarity and capacity gaps.

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

3.4 Data analysis

Quantitative data were analysed using descriptive statistics and Cronbach's alpha. Descriptive statistics profiled governance practices and preparedness, while reliability analysis assessed the internal consistency of the governance and preparedness scales. Qualitative data were analysed thematically using Braun and Clarke's (2006) six-phase approach, with codes clustered around RMF, TOE, C2M2 and STS constructs. The two strands were integrated through a joint display.

3.5 Framework validation

The draft framework was reviewed by five subject-matter experts from security agencies, regulators, UAV operators and academia. Reviewers assessed the relevance of dimensions, clarity of indicators and feasibility in Nigerian public-sector settings. A pilot application with a small sub-sample was used to test usability and refine item wording. This provided preliminary evidence of relevance and usability, not a full validation of predictive or operational effectiveness.

Several measures were taken to strengthen rigour. The questionnaire was reviewed for content and face validity by subject-matter experts and piloted with a small group of UAV stakeholders. Reliability was assessed using Cronbach's alpha, and items with low item-total correlations were reviewed. Interview transcripts were coded systematically, with an audit trail linking codes to themes. Findings were triangulated across survey, interview and documentary sources. These measures do not eliminate bias, but they make the analytical process transparent and defensible.

4. RESULTS

4.1 Governance practices and preparedness

The survey showed that UAV cybersecurity governance is uneven. Only 10% of respondents considered their organisations highly prepared, 35% somewhat prepared, 30% neutral and 25% unprepared. Many organisations relied on general ICT or information security policies rather than UAV specific cybersecurity requirements. Responsibilities were often dispersed across ICT, operations and security units, and few organisations had documented UAV risk assessment procedures, regular audits or formal incident-reporting channels. Where controls such as encryption, multi factor authentication and intrusion detection existed, they were often applied inconsistently across platforms and missions.

The respondents represented a cross-section of public-sector UAV stakeholders. The largest age group was 25–34 years (45%), followed by 35–44 years (30%). Most held a bachelor's degree (40%), followed by a master's degree (30%) and a PhD (10%). UAV operators constituted 35% of the sample, cybersecurity specialists 25%, government officials and regulators 20%, and academics 15%. Experience was uneven: 45% had one to three years, 20% had four to seven years, and 5% had eight years or more. This profile suggests a young and educated workforce with limited long-term operational experience, which is relevant to governance because experienced staff are often the source of informal risk knowledge.

4.2 Maturity and governance dimensions

Mapped against C2M2, most participating organisations were at an initial or early performed level. Practices depended on individual initiative rather than institutionalised processes. Risk management was reactive; policies were generic; governance structures were unclear; technical controls were partial; training was limited; regulatory engagement was inconsistent; and incident management was weak. These patterns were consistent across the survey and

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

interviews, although security sector entities reported somewhat more structured practices than civil ministries and agencies.

Table 2 summarises the maturity rubric used to interpret these findings. The rubric is intended to make assessment judgements transparent and comparable across organisations. It does not assume that every organisation should reach the highest level; the appropriate level depends on mission criticality, risk exposure and available resources. The rubric therefore supports proportionate improvement rather than a single compliance target.

Table 2: Maturity rubric for the governance assessment framework

Level	Descriptor	Governance characteristics
1. Initial	Ad hoc	Responsibilities unclear; no documented UAV risk process; reactive incident handling
2. Performed	Emerging	Basic policies exist; some controls implemented; practices depend on individuals
3. Managed	Defined	Documented processes; assigned roles; regular training; incident reporting established
4. Measured	Quantified	Performance metrics; audits; risk reviews; evidence-based prioritisation
5. Optimised	Adaptive	Continuous improvement; inter-agency learning; anticipatory risk management

4.3 Qualitative findings

Four governance themes emerged. First, mandate fragmentation: participants described overlapping responsibilities among aviation, telecommunications, ICT and security institutions, with no clear owner for UAV cybersecurity. Second, policy ambiguity: general cybersecurity and aviation rules did not specify UAV specific requirements for procurement, configuration, logging, incident reporting or vendor management. Third, capacity constraints: specialised UAV cybersecurity skills were scarce, and organisations depended heavily on vendors for configuration, maintenance and incident diagnosis. Fourth, weak accountability and reporting culture: incidents were under-reported because of blame, uncertainty about reporting channels and fear of reputational damage. These themes explain why awareness of threats did not translate into governance capability.

A further cross-cutting theme concerned procurement and vendor management. Participants noted that UAV systems were often acquired through suppliers who controlled firmware, configuration and maintenance. Contracts rarely specified cybersecurity requirements, audit rights, incident notification or secure update obligations. As a result, agencies had limited visibility into the security posture of the platforms they operated and limited leverage to demand remediation. This finding links the governance dimensions of policy, technical controls and incident management: procurement is where many governance weaknesses become embedded.

4.4 Implications for assessment

The findings suggest that a governance assessment framework for Nigerian public-sector UAV programmes must address seven dimensions: risk-management processes; policies and standards; organisational structures and accountability; technical controls; human capacity and training; regulatory environment; and incident management. These dimensions map onto

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

RMF (risk processes), TOE (technology, organisation and environment), C2M2 (maturity) and STS (people, culture and reporting). They also reflect the specific weaknesses identified in the survey and interviews.

5. THE PROPOSED FRAMEWORK

The Nigeria centered UAV Cybersecurity Governance Assessment Framework is organised around the seven dimensions summarised in Table 1. Each dimension contains indicators, is linked to one or more theoretical lenses, and is assessed on a five-level maturity scale: Initial, Performed, Managed, Measured and Optimised. Scores are aggregated into a governance profile rather than a single ranking, so that institutions can see which dimensions are weak and prioritize accordingly.

Table 1: Dimensions and indicators of the proposed governance assessment framework

Dimension	Example indicators	Linked frameworks
Risk-management processes	Documented UAV risk assessments; frequency of review; risk owners	RMF, C2M2
Policies and standards	UAV specific cyber policy; procurement security requirements; alignment with national rules	RMF, TOE
Organisational structures	Defined roles; dedicated focal person or unit; escalation paths	TOE, C2M2, STS
Technical controls	Encryption; MFA; IDS; secure firmware; network segmentation	RMF, C2M2
Human capacity and training	Role-specific training; incident drills; awareness	C2M2, STS
Regulatory environment	Mandate clarity; audits; inter-agency coordination	TOE
Incident management	Reporting channels; response plan; forensic capability; lessons learned	RMF, C2M2, STS

The framework is applied in five steps: (i) map UAV assets, missions and data flows; (ii) administer the assessment instrument across relevant units; (iii) score each dimension and compile a governance profile; (iv) identify priority gaps and develop improvement plans; and (v) reassess periodically to track progress. The framework is intended as a diagnostic and planning tool. It does not replace platform-level security testing, certification or incident response.

The governance profile can be used alongside the UAV Cybersecurity Posture Score (UCPS) proposed in the wider study. The UCPS combines threat exposure, vulnerability, preparedness and governance into a 0–100 posture score. The governance assessment provides the detail behind the governance component: it identifies which institutional practices are weak, who owns them and what improvement is required. The two tools are therefore complementary. The UCPS supports overall prioritisation across the four dimensions, while the governance assessment supports targeted institutional reform. Neither replaces platform-level security testing, certification or incident response.

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Table 3 translates the framework into an implementation roadmap. The roadmap is deliberately phased because public institutions cannot reform procurement, training, regulation and technical controls simultaneously. Phase 1 establishes ownership and a baseline assessment. Phase 2 addresses the most critical gaps in risk processes, policies and incident reporting. Phase 3 strengthens technical controls, training and vendor management. Phase 4 embeds monitoring, audit and continuous improvement. The sequence can be adapted to the resources and mandate of each institution.

Table 3: Phased implementation roadmap

Phase	Focus	Key actions	Expected output
1. Baseline	Ownership and diagnosis	Assign accountable owner; inventory UAV assets; complete governance assessment	Baseline profile and priority gaps
2. Foundation	Processes and accountability	Document risk process; issue UAV cyber policy; establish incident reporting	Defined governance framework
3. Capability	Controls and people	Implement priority controls; train staff; strengthen vendor requirements	Improved controls and skills
4. Embedding	Monitoring and learning	Conduct audits; review metrics; update assessment; share lessons	Continuous improvement cycle

6. DISCUSSION

The findings show that UAV cybersecurity governance in Nigerian public institutions is fragmented and largely reactive. This is consistent with the C2M2 distinction between the existence of a practice and its institutionalisation (U.S. Department of Energy, 2022). Many organisations are aware of UAV cyber threats, but awareness has not been converted into documented processes, clear accountability and regular assessment. The result is a governance gap that technical controls alone cannot close.

Theoretically, the study supports the value of integrating RMF, TOE, C2M2 and STS rather than treating them as alternatives. RMF and C2M2 provide the process and maturity architecture, but they do not explain why similar organisations achieve different outcomes. TOE and STS supply that explanation by drawing attention to organisational capacity, regulatory ambiguity, vendor dependence and reporting culture. The integration is therefore not merely additive: each lens corrects the blind spots of the others.

The TOE lens helps explain why. Technology choices are often driven by procurement and operational convenience rather than security requirements; organisational structures do not assign clear responsibility; and the regulatory environment provides general aviation and cybersecurity requirements but few UAV-specific expectations (Pyzynski & Balcerzak, 2021; NCAA, 2023). The STS lens explains why controls are inconsistently used: limited training, vendor dependence and a weak reporting culture constrain the ability of people and institutions to operate controls effectively (Trist & Bamforth, 1951).

The proposed framework responds by combining risk-management logic, contextual analysis, maturity assessment and socio-technical indicators. Its contribution is not a new technical

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

control but an integrated governance assessment structure tailored to Nigerian public sector UAV programmes. The framework can help institutions move from ad hoc responses to a repeatable cycle of assessment, prioritisation and improvement. Its limitations are equally clear: it has been reviewed by experts and piloted on a small scale, but it has not been validated longitudinally or applied across a representative sample of public institutions.

The study also has implications for policy. Regulators should clarify mandates, issue UAV-specific cybersecurity guidance and establish incident-reporting arrangements. Public institutions should designate accountable owners for UAV cybersecurity, adopt risk-assessment procedures and invest in role-specific training. These measures would address the governance gaps identified in the study and create the institutional conditions in which technical controls can function.

For practice, the framework offers a structured way to move beyond generic cybersecurity awareness. Institutions can use it to identify who owns UAV cybersecurity, whether risk assessments are documented, whether incidents are reported and whether controls are maintained. For regulators, it provides a common language for assessing capability and targeting support. For researchers, it offers a testable model whose dimensions can be refined through comparative and longitudinal work.

The central argument is that governance capability, rather than isolated technology, will determine whether Nigerian public-sector UAV programmes can be secured over time. Building that capability requires clear mandates, formal processes, skills, harmonised regulation and continuous assessment. The proposed framework offers a structured way for public institutions to diagnose their current arrangements, benchmark maturity and prioritise interventions. Further validation through larger samples, Delphi studies and longitudinal application is recommended.

This paper examined how Nigerian public-sector organisations govern cybersecurity for UAV programmes and proposed a Nigeria-centred assessment framework integrating RMF, TOE, C2M2 and STS. The evidence points to partial awareness, fragmented responsibilities, low capability maturity and weak regulatory alignment. Cyber threats are understood in broad terms but are not yet embedded in structured, life-cycle risk management.

The study has several limitations. It is exploratory and cross-sectional, relying on self-reported practices and perceptions. The sample of 150 respondents and ten interviews is not statistically representative of all Nigerian public-sector institutions, and access constraints may have excluded some of the most sensitive agencies. The framework was reviewed by experts and piloted on a small scale, but it has not been validated longitudinally or tested against objective governance outcomes. The study also focused on governance rather than technical control effectiveness, and it did not include a full economic evaluation of implementation costs.

Future research should test the framework in a larger and more diverse sample, including state-level agencies and civilian ministries. Longitudinal case studies could examine whether governance improvements are followed by changes in incident frequency, response times and control adoption. Comparative work across African countries would help distinguish Nigeria-specific findings from more general patterns. Further research could also develop and validate a quantitative governance score, similar to the UCPS, to support benchmarking and monitoring.

7. LIMITATIONS AND FUTURE RESEARCH

8. CONCLUSION

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Declarations

Author contributions: M.F.K. conceptualised the study, collected and analysed the data, and drafted the manuscript. F.N.O. and M.O.A. supervised the study and reviewed the manuscript. All authors approved the final version.

Funding: This research received no specific grant from any funding agency.

Conflict of interest: The authors declare no conflict of interest.

Ethics approval: Ethical clearance was obtained from the relevant institutional review committee. Informed consent was obtained from all participants.

Data availability: The data are not publicly available because they contain sensitive institutional information. Aggregated data may be obtained from the corresponding author on reasonable request.

REFERENCES

Abro, G. E. M., Zulkifli, S. A. B. M., Masood, R. J., Asirvadam, V. S., & Laouiti, A. (2022). Comprehensive review of UAV detection, security, and communication advancements to prevent threats. Drones, 6(10), 284. https://doi.org/10.3390/drones6100284

Anghuwo, J. S., Imanuel, P., & Nangolo, S. S. (2024). Anti-unmanned aerial vehicle detection system for airports: Aviation and national security perspective. Journal of Transportation Security, 17(1), 12. https://doi.org/10.1007/s12198-024-00280-w

Bai, N., Hu, X., & Wang, S. (2024). A survey on unmanned aerial systems cybersecurity. Journal of Systems Architecture, 156, 103282. https://doi.org/10.1016/j.sysarc.2024.103282

Boukabou, I., Kaabouch, N., & Rupanetti, D. (2024). Cybersecurity challenges in UAV systems: IEMI attacks targeting inertial measurement units. Drones, 8(12), 738. https://doi.org/10.3390/drones8120738

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

Büyüközkan, G., & Güler, M. (2025). Cybersecurity maturity model: Systematic literature review and a proposed model. Technological Forecasting and Social Change, 213, 123996. https://doi.org/10.1016/j.techfore.2025.123996

Chandolia, L., Singh, P., Pal, O., Misbahuddin, M., Kumar, V., & Prakash, R. (2025). Authentication and security challenges for unmanned aerial vehicles: A survey. Ad Hoc Networks, 174, 103842. https://doi.org/10.1016/j.adhoc.2025.103842

Dehbi, F., Zraib, M., & Chebak, A. (2025). PASTAD: A context-aware threat modeling methodology for unmanned aerial systems. Cyber Security and Applications, 3, 100111. https://doi.org/10.1016/j.csa.2025.100111

Elmarady, A. A., & Rahouma, K. (2021). Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. IEEE Access, 9, 143997–144016. https://doi.org/10.1109/ACCESS.2021.3121230

Ficco, M., Granata, D., Palmieri, F., & Rak, M. (2024). A systematic approach for threat and vulnerability analysis of unmanned aerial vehicles. Internet of Things, 26, 101180. https://doi.org/10.1016/j.iot.2024.101180

Hadi, H. J., Cao, Y., Nisa, K. U., Jamil, A. M., & Ni, Q. (2023). A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. Journal of

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Network and Computer Applications, 213, 103607. https://doi.org/10.1016/j.jnca.2023.103607

Han, P., Yang, X., Zhao, Y., Guan, X., & Wang, S. (2022). Quantitative ground risk assessment for urban logistical unmanned aerial vehicle (UAV) based on Bayesian network. Sustainability, 14(9), 5733. https://doi.org/10.3390/su14095733

Jung, J. H., Hong, M. Y., Choi, H., & Yoon, J. W. (2024). An analysis of GPS spoofing attack and efficient approach to spoofing detection in PX4. IEEE Access, 12, 46668–46677. https://doi.org/10.1109/ACCESS.2024.3382543

Kumar, N., & Chaudhary, A. (2024). Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security. Computer Networks, 252, 110695. https://doi.org/10.1016/j.comnet.2024.110695

Kyari, M. F., Ogwueleka, F. N., & Adenomon, M. O. (2025). Cybersecurity risk challenges in unmanned aerial vehicles operations: Empirical evidence from Nigerian UAV stakeholders. International Journal of Innovative Information Systems & Technology Research, 13(4), 462–470. https://doi.org/10.5281/zenodo.18076310

Ma, T., Zhang, X., & Miao, Z. (2025). Detection of UAV GPS spoofing attacks using a stacked ensemble method. Drones, 9(1), 2. https://doi.org/10.3390/drones9010002

Mekdad, Y., Aris, A., Babun, L., El Fergougui, A., Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. Computer Networks, 224, 109626. https://doi.org/10.1016/j.comnet.2023.109626

Melaku, H. M. (2023). Context-based and adaptive cybersecurity risk management framework. Risks, 11(6), 101. https://doi.org/10.3390/risks11060101

National Institute of Standards and Technology. (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (NIST SP 800-37 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2

Nayfeh, M., Li, Y., Shamaileh, K. A., Devabhaktuni, V., & Kaabouch, N. (2023). Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification. Computers & Security, 126, 103085. https://doi.org/10.1016/j.cose.2022.103085

Nigeria Civil Aviation Authority. (2023). Nigeria Civil Aviation Regulations: Part 21—Remotely Piloted Aircraft Systems (RPAS). https://ncaa.gov.ng/media/l2vjnlce/nig-cars-part-21-remotely-piloted-aircraft-system.pdf

Pandey, G. K., Gurjar, D. S., Nguyen, H. H., & Yadav, S. (2022). Security threats and mitigation techniques in UAV communications: A comprehensive survey. IEEE Access, 10, 112858–112897. https://doi.org/10.1109/ACCESS.2022.3215975

Pyzynski, M., & Balcerzak, T. (2021). Cybersecurity of the unmanned aircraft system (UAS). Journal of Intelligent & Robotic Systems, 102(2), 35. https://doi.org/10.1007/s10846-021-01399-x

Sun, X., Hu, Y., Qin, Y., & Zhang, Y. (2024). Risk assessment of unmanned aerial vehicle accidents based on data-driven Bayesian networks. Reliability Engineering & System Safety, 248, 110185. https://doi.org/10.1016/j.ress.2024.110185

Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523048
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Tran, T. D., Thiriet, J.-M., Marchand, N., & El Mrabti, A. (2021). A cybersecurity risk framework for unmanned aircraft systems under specific category. Journal of Intelligent & Robotic Systems, 104(1), 4. https://doi.org/10.1007/s10846-021-01512-0

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. Human Relations, 4(1), 3–38. https://doi.org/10.1177/001872675100400101

Tsao, K.-Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Networks, 133, 102894. https://doi.org/10.1016/j.adhoc.2022.102894

U.S. Department of Energy. (2022). Cybersecurity capability maturity model (C2M2) (Version 2.1). Office of Cybersecurity, Energy Security, and Emergency Response. https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

Wang, Z., Li, Y., Wu, S., Zhou, Y., Yang, L., Xu, Y., Zhang, T., & Pan, Q. (2023). A survey on cybersecurity attacks and defenses for unmanned aerial systems. Journal of Systems Architecture, 138, 102870. https://doi.org/10.1016/j.sysarc.2023.102870

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