ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

CYBERSECURITY VULNERABILITIES AND RESILIENCE STRATEGIES IN NATIONAL SECURITY UAV OPERATIONS IN NIGERIA: A FRAMEWORK BASED ON SECURITY OPERATIVES' AND GOVERNMENT AGENCIES' PERSPECTIVES

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 study examines cybersecurity vulnerabilities and resilience strategies in national security UAV operations in Nigeria and proposes a context-specific, adaptive assessment framework grounded in the perspectives of security operatives and government agencies. Drawing on the Risk Management Framework (RMF), Technology–Organisation–Environment (TOE) framework, Cybersecurity Capability Maturity Model (C2M2) and Socio-Technical Systems (STS) theory, the study adopted an explanatory sequential mixed-methods design: a survey of 150 stakeholders and semi-structured interviews with ten key informants. Quantitative data were analysed using descriptive statistics, reliability analysis, correlation and regression; qualitative data were analysed thematically. GPS spoofing (75%), signal jamming (68%) and unauthorised access (60%) were the most frequently reported threats, while communication links (70%), navigation systems (60%) and ground control stations (60%) were perceived as the most vulnerable components. Only 10% of respondents considered their organisations highly prepared. Preparedness was negatively associated with reported incident frequency ($r = -0.54$, $p < 0.01$; $\beta = -0.41$, $p < 0.001$), and high-risk operational geography was positively associated with perceived impact severity ($\beta = 0.29$, $p = 0.001$). Qualitative evidence revealed fragmented regulation, weak incident reporting and human-capacity deficits. The study proposes a Nigeria-specific, adaptive UAV Cybersecurity Risk and Resilience Framework that integrates technical controls, organisational practices and regulatory measures through context-sensitive assessment, periodic reassessment and feedback from incidents. The framework is empirically informed and preliminarily assessed through expert review and pilot application; operational validation remains future work. It concludes that strengthening national security UAV resilience requires coherent policy, sustained capacity building and continuous risk monitoring.

Keywords: UAV cybersecurity; national security; vulnerabilities; resilience; RMF-TOE-C2M2-STS; Nigeria

1. INTRODUCTION

Unmanned aerial vehicles (UAVs) have become critical assets in Nigerian national security operations, supporting surveillance, reconnaissance, border monitoring, crisis response and counter-terrorism. Their capacity to provide real-time intelligence in hostile or inaccessible environments makes them central to the work of the armed forces, law enforcement agencies and intelligence services. However, the digital connectivity and autonomy that enable these capabilities also introduce cybersecurity vulnerabilities. GPS spoofing, signal jamming, malware injection and unauthorized access to command-and-control links can compromise operational integrity, cause mission failure and create wider national security risks (Tsao et al., 2022; Wang et al., 2023).

Nigeria's security landscape, including insurgency, banditry, kidnapping, oil theft and transnational organised crime, magnifies the consequences of compromised UAV systems.

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Adversaries increasingly possess the technical capacity to exploit cyber physical weaknesses in state security infrastructure, including drones (Anghuwo et al., 2024). While global literature has documented generic UAV cyber threats, there is limited empirical evidence on how these risks manifest in Nigerian national security operations, how prepared agencies are to respond and what resilience strategies are currently in place.

This study addresses these gaps by investigating cybersecurity vulnerabilities and resilience strategies in national security UAV operations in Nigeria, using the experiences of security operatives and government agencies as its foundation. Its objectives are to: (i) identify prevalent cyber threats and vulnerabilities affecting national security UAVs; (ii) assess the impact of these threats on operational integrity; (iii) examine existing resilience and mitigation strategies; and (iv) develop a context specific framework to guide cybersecurity risk assessment and governance in Nigerian UAV operations.

The study makes three contributions. First, it provides Nigeria-specific empirical evidence on UAV cybersecurity vulnerabilities and resilience, an area dominated by studies from developed and highly regulated aviation contexts. Second, it integrates RMF, TOE, C2M2 and STS into a single analytical framework rather than applying them in isolation. Third, it translates the framework into a practical assessment structure that security agencies and regulators can use to prioritise controls and monitor improvement.

Nigeria's regulatory framework provides an important part of this context. The Nigeria Civil Aviation Regulations establish requirements for remotely piloted aircraft, including operator security programmes, but they do not yet prescribe detailed cybersecurity controls for national security UAV operations (NCAA, 2023). The result is a hybrid environment in which general aviation rules, ICT security requirements and agency-specific practices coexist without a coherent UAV cybersecurity standard. This regulatory gap is not merely administrative: it shapes procurement decisions, incident reporting, vendor accountability and the willingness of agencies to invest in controls whose value is difficult to demonstrate without a common assessment framework (Pyzynski & Balcerzak, 2021; Anghuwo et al., 2024).

2. LITERATURE REVIEW

2.1 UAV cyber threats and vulnerabilities

Recent scholarship has documented an expanding attack surface created by UAV deployment in civilian and security domains. Common threats include GNSS/GPS spoofing, signal jamming, denial of service, malware infection and unauthorised access to control systems, with consequences for confidentiality, integrity, availability and safety (Tsao et al., 2022; Pandey et al., 2022; Kumar & Chaudhary, 2024). Communication links, navigation modules, firmware and ground control stations are consistently identified as core technical vulnerabilities (Abro et al., 2022; Hadi et al., 2023; Mekdad et al., 2023). Bai et al. (2024) further show that the convergence of communication, computing and control in unmanned aircraft systems creates security challenges that are distinct from those of conventional information systems.

The threat landscape can be organised into four interacting layers. The communication layer includes command-and-control links, telemetry and video feeds, which are exposed to jamming, interception and man-in-the-middle attacks. The navigation layer includes GNSS receivers and inertial sensors, which are vulnerable to spoofing and electromagnetic interference. The platform layer includes firmware, operating systems, onboard computers and payload interfaces, which may contain unpatched vulnerabilities or insecure default configurations. The ground layer includes control stations, mission-planning software, data

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

storage and human operators, whose practices can either mitigate or amplify technical weaknesses (Tsao et al., 2022; Kumar & Chaudhary, 2024; Hadi et al., 2023).

Resilience is not simply the absence of vulnerabilities. It refers to the capacity of a system and its operators to anticipate disruption, absorb shock, recover functionality and adapt to changing conditions. In UAV operations, resilience depends on redundant navigation and communication, graceful degradation, trained personnel, documented response procedures and organisational learning after incidents. This is why a purely technical reading of UAV security is insufficient: the same control may be effective in one organisation and ineffective in another, depending on training, accountability and institutional support (Melaku, 2023; Büyüközkan & Güler, 2025).

Specific studies show how these threats operate. Nayfeh et al. (2023) and Ma et al. (2025) demonstrate that GPS spoofing can be detected through signal and navigation features, but detection does not eliminate the operational risk. Jung et al. (2024) show that stronger attacker models can evade some detection mechanisms in the PX4 autopilot, while Boukabou et al. (2024) demonstrate that intentional electromagnetic interference can distort inertial measurement unit readings. Chandolia et al. (2025) identify authentication and key management as persistent weak points. Together, these studies show that UAV cybersecurity requires layered protection across communication, navigation, sensor and ground segments.

2.2 Risk assessment and governance frameworks

Methodological contributions have emerged around UAV-specific risk assessment. Tran et al. (2021) proposed a cybersecurity risk framework for UAS under the Specific category, linking operational context to security objectives. Elmarady and Rahouma (2021) developed an aviation-wide cybersecurity risk assessment approach, while Zemlianko and Kharchenko (2023) applied IMECA-based techniques to multifunctional UAV fleets. Ficco et al. (2024) combined threat modelling with penetration testing of a real UAV, and Dehbi et al. (2025) proposed PASTAD, a context aware threat-modelling methodology for UAS. These approaches provide structured technical analysis but give limited attention to organisational preparedness, governance and the socio-technical conditions of developing-country operations.

Broader governance frameworks offer complementary lenses. The NIST Risk Management Framework (NIST, 2018) provides a life-cycle process for identifying, assessing, treating and monitoring risk. The Technology-Organization-Environment (TOE) framework explains how technological, organisational and environmental conditions shape adoption and implementation (Tornatzky & Fleischer, 1990). The Cybersecurity Capability Maturity Model (C2M2) provides graded maturity levels for organisational cybersecurity practices (U.S. Department of Energy, 2022), while Socio-Technical Systems (STS) theory emphasises the joint optimisation of technical and social subsystems (Trist & Bamforth, 1951). 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. In the Nigerian context, the Nigeria Civil Aviation Regulations provide a regulatory baseline for remotely piloted aircraft, but they do not yet prescribe detailed UAV cybersecurity requirements (NCAA, 2023). Pyzynski and Balcerzak (2021) similarly note that UAS cybersecurity remains only partially addressed in aviation law.

The four lenses operate at different levels of analysis and are therefore complementary rather than interchangeable. RMF provides the process logic: categorise the system, assess risk, select and implement controls, monitor performance and repeat. TOE explains why apparently similar organisations adopt different controls: technology readiness, organisational

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

capacity and the regulatory environment shape what is feasible. C2M2 translates those conditions into a maturity pathway, from ad hoc practices to measured and optimised processes. STS explains the human and institutional mechanisms through which controls succeed or fail. Integrating them produces a framework that is process-driven, context-sensitive, measurable and socio-technically realistic.

2.3 Research gap

Three gaps emerge. First, empirical evidence on UAV cyber incidents and preparedness in Nigerian national security operations remains thin. Second, RMF, TOE, C2M2 and STS are rarely integrated into a single UAV-specific framework. Third, the perspectives of frontline security operatives and government agencies are insufficiently represented. This study addresses these gaps by combining survey and interview evidence from Nigerian stakeholders and using the findings to develop a context-specific risk and resilience framework.

The African evidence base remains particularly thin. Most UAV cybersecurity studies are situated in Europe, North America or East Asia, where regulatory enforcement, industry maturity and data availability differ substantially from Nigeria. The few African studies tend to focus on counter-UAS detection, airport security or regulatory commentary rather than on organisational preparedness and resilience in national security operations (Anghuwo et al., 2024). This limits the transferability of international findings and reinforces the need for primary evidence from Nigerian security agencies and government institutions.

3. METHODOLOGY

3.1 Research design

The study adopted an explanatory sequential mixed-methods design. A cross-sectional survey of UAV stakeholders was conducted first, followed by semi structured key informant interviews. The survey measured reported threats, perceived vulnerabilities, organisational preparedness and perceived operational impact. The interviews explored the organisational, regulatory and human factors that explain the survey patterns. The two strands were integrated through a joint display.

The design was underpinned by a pragmatic philosophical stance. Pragmatism is appropriate because the research question is practical and policy-oriented: what risks exist, how prepared are institutions, and what framework would improve decisions? The study was not concerned with defending a single epistemological position but with producing usable evidence from multiple sources. The quantitative strand provided breadth and comparability; the qualitative strand provided depth and contextual explanation. Integration occurred at the interpretation stage rather than through statistical merging of the two datasets.

3.2 Population and sampling

The target population comprised individuals directly involved in UAV operations, regulation, procurement, cybersecurity and research in Nigeria, estimated at approximately 15,000. The quantitative strand used stratified random sampling across three strata: state security and military operators; commercial and security-relevant operators; and civilian/academic experts. Using Yamane’s (1967) formula with a 5% margin of error, the initial target was approximately 390 respondents. Access restrictions and institutional gatekeeping reduced the achieved sample to 150 valid responses, which is acknowledged as a limitation. The qualitative strand used purposive sampling with maximum variation to select ten key informants from security agencies, commercial operators, regulators and academia.

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Stratification was used to avoid over-representing any single category of stakeholder. Security and military operators work in classified, high-threat environments and may perceive risk differently from commercial operators working under civil aviation rules. Regulators make and enforce rules but do not necessarily operate UAVs. Cybersecurity specialists understand the technical attack surface but may have less insight into mission constraints. Academics may be more familiar with international standards than with day-to-day practice. Treating these categories as strata improves the representativeness of the sample and allows group comparisons without confounding stakeholder differences with sampling differences.

3.3 Instruments and data collection

The structured questionnaire covered socio-demographic characteristics, perceived cyber threats and vulnerabilities, exposure and incident frequency, organisational preparedness and resilience strategies. Items were rated on five-point Likert scales. The instrument was reviewed by five subject-matter experts and piloted with ten respondents. The interview guide explored perceived threats, incidents, organisational practices, regulatory constraints and recommendations. Interviews lasted 45-75 minutes, were recorded with consent and transcribed verbatim.

3.4 Data analysis

Quantitative data were analysed in SPSS and Python using descriptive statistics, Cronbach's alpha, exploratory factor analysis, independent-samples t-tests, one-way ANOVA, Pearson correlation and multiple regression. The regression models examined the association between preparedness and reported incident frequency, and between high-risk operational geography and perceived impact severity. Statistical significance was set at $p < 0.05$. Qualitative data were analysed using Braun and Clarke's (2006) six-phase thematic analysis, with codes mapped onto the RMF, TOE, C2M2 and STS constructs.

Several analytical safeguards were applied. Reliability was assessed using Cronbach's alpha, with values of 0.70 or above treated as acceptable. Exploratory factor analysis was used to examine whether the items clustered around the intended constructs. Regression assumptions were checked through inspection of residuals, variance inflation factors and heteroskedasticity tests. Effect sizes and confidence intervals were reported alongside significance tests to avoid overstating small differences. The cross-sectional design means that the regression results describe associations, not causal effects.

3.5 Ethical considerations

Ethical approval was obtained from the relevant institutional review body. Participation was voluntary and informed consent was obtained from all respondents. Given the sensitivity of national security information, confidentiality and anonymity were maintained, and role-based rather than agency-specific identifiers were used. Data were stored securely and reported in aggregate.

4. RESULTS

4.1 Reported threats and vulnerable components

Table 1 presents the threats most frequently reported by respondents. GPS spoofing (75%), signal jamming (68%) and unauthorised access (60%) were dominant. Malware injection was reported by 30% and other threats by 10%.

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The respondents reflected the diversity of the Nigerian UAV ecosystem. The largest age group was 25–34 years (45%), followed by 35–44 years (30%). Educational attainment was high: 40% held a bachelor's degree, 30% a master's degree and 10% a PhD. UAV operators constituted 35% of the sample, cybersecurity specialists 25%, government officials and regulators 20%, and academics 15%. Most respondents had between one and three years of professional experience (45%), while 20% had four to seven years and 5% had eight years or more. This profile is consistent with a young, rapidly expanding sector in which technical expertise is unevenly distributed.

Threat	**Respondents (%)**
GPS spoofing	75
Signal jamming	68
Unauthorised access	60
Malware injection	30
Other	10

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Table 1: Reported UAV cybersecurity threats (N = 150)

Table 2 shows the components perceived as most vulnerable. Communication links (70%), navigation systems (60%) and ground control stations (60%) were the main points of weakness, followed by payload data (40%).

Table 2: Perceived vulnerability of UAV components (N = 150)

Component	Respondents (%)
Communication links	70
Navigation systems	60
Ground control stations	60
Payload data	40
Other	5

4.2 Preparedness and perceived severity

Only 10% of respondents considered their organisations highly prepared, while 35% were somewhat prepared, 30% neutral and 25% unprepared. Table 3 shows the perceived severity of threats on a five-point scale. GPS spoofing recorded the highest mean (4.5), followed by signal jamming (4.2), unauthorised access (4.0), data interception (3.8) and denial of service (3.5).

Table 3: Preparedness and mean severity ratings

Measure	Category / threat	Value
Preparedness	Highly prepared	10%
Preparedness	Somewhat prepared	35%
Preparedness	Neutral	30%
Preparedness	Unprepared	25%
Severity (mean)	GPS spoofing	4.5
Severity (mean)	Signal jamming	4.2
Severity (mean)	Unauthorised access	4.0
Severity (mean)	Data interception	3.8
Severity (mean)	Denial of service	3.5

4.3 Reliability and hypothesis tests

The instrument showed acceptable to good internal consistency: threat awareness $\alpha = 0.84$, vulnerability perception $\alpha = 0.78$, preparedness $\alpha = 0.82$ and impact severity $\alpha = 0.88$, with an overall α of 0.83. Preparedness was negatively associated with reported incident frequency

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

(r = −0.54, p < 0.01; β = −0.41, 95% CI [−0.58, −0.24], p < 0.001). High-risk operational geography was positively associated with perceived impact severity (β = 0.29, 95% CI [0.12, 0.46], p = 0.001). Education and occupational role were not significantly associated with threat severity (p = 0.18 and p = 0.62, respectively). Confidence in controls differed significantly by years of experience (p = 0.03), with more experienced respondents reporting lower confidence (mean 2.7 for 8+ years versus 3.3 for 1–3 years).

The regression results should be interpreted alongside the correlation analysis. The negative correlation between preparedness and reported incident frequency indicates that organisations with stronger controls, training and incident-response arrangements reported fewer incidents. The regression coefficient for preparedness remained negative after controlling for other variables, which suggests that the association is not simply an artefact of organisational size or sector. The positive coefficient for high-risk operational geography indicates that mission context matters: organisations operating in contested areas reported more severe consequences, even where preparedness was similar. These findings support the framework's dual emphasis on organisational capability and environmental exposure.

4.4 Qualitative findings

Four themes emerged from the interviews. First, participants described recurring GPS interference and communication jamming, often initially mistaken for hardware failure. Second, preparedness was largely reactive: incident response depended on individual initiative, with few documented procedures or rehearsed recovery arrangements. Third, regulatory responsibilities were fragmented across aviation, telecommunications, ICT and security institutions, and no agency had clear ownership of UAV cybersecurity. Fourth, human and technical capacity was limited, with dependence on foreign vendors for configuration, maintenance and incident diagnosis. These themes reinforced the survey findings and explained why awareness did not translate into preparedness.

A fifth cross-cutting issue concerned vendor dependence. Several participants explained that firmware updates, configuration changes and fault diagnosis were often performed by foreign suppliers or their local representatives. This created delays, reduced transparency and made it difficult for agencies to verify whether security patches had been applied correctly. Vendor dependence also shaped incident reporting: where a problem was attributed to a supplier, agencies were sometimes reluctant to record it as a cybersecurity incident. This finding reinforces the need for supply-chain assurance and local technical capacity as part of any resilience strategy.

5. DISCUSSION

The findings confirm that national security UAV operations in Nigeria face significant and multifaceted cybersecurity risks. The dominance of GPS spoofing and signal jamming is consistent with international evidence (Tsao et al., 2022; Pandey et al., 2022; Nayfeh et al., 2023), but the Nigerian context amplifies the consequences because platforms are imported, regulatory enforcement is fragmented and adversaries operate in a contested electronic environment. The finding that communication links, navigation systems and ground control stations are the most vulnerable components supports the layered view of UAV security advanced by Kumar and Chaudhary (2024) and Chandolia et al. (2025). This is consistent with safety-risk studies showing that cyber-induced failures can escalate into ground-impact and third-party harm (Sun et al., 2024; Han et al., 2022).

Compared with international studies, the Nigerian evidence shows a similar threat profile but a different institutional context. Tsao et al. (2022) and Pandey et al. (2022) identify communication and navigation links as core attack surfaces; the present study confirms this

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

but shows that the consequences are amplified by import dependence, fragmented regulation and limited forensic capacity. Studies from mature aviation regimes assume the existence of certification, incident reporting and enforcement mechanisms that are still emerging in Nigeria (Pyzynski & Balcerzak, 2021; Tran et al., 2021). The framework therefore cannot simply import those assumptions; it must build in the institutional strengthening that they presuppose.

The preparedness results are particularly important. Only 10% of respondents considered their organisations highly prepared, despite high awareness of the threat. This is consistent with the C2M2 distinction between the existence of a practice and its institutionalisation (U.S. Department of Energy, 2022). Many organisations have some controls, but few have documented procedures, regular training, incident-response arrangements and continuous improvement mechanisms. The negative association between preparedness and incident frequency supports the framework's emphasis on organisational capability rather than technical controls alone.

The qualitative evidence explains the mechanisms behind this gap. Regulatory fragmentation creates uncertain incentives and diffused accountability. Human-capacity deficits limit the ability to configure, monitor and maintain controls. A weak reporting culture means incidents are under-recorded and lessons are not shared. These findings are consistent with the STS perspective, which holds that technical controls are effective only when embedded in a social system that has the knowledge, incentives and authority to use them (Trist & Bamforth, 1951).

The study therefore proposes a Nigeria specific UAV Cybersecurity Risk and Resilience Framework. The framework uses RMF to structure continuous risk identification, assessment and monitoring; TOE to situate technology choices within organisational and regulatory conditions; C2M2 to grade capability maturity; and STS to embed human and institutional factors. It is intended to support a shift from reactive troubleshooting to proactive, evidence-based governance. The framework is a diagnostic and prioritisation tool, not a substitute for platform-level testing or incident response.

The framework is organised around four dimensions. Threat exposure captures the frequency and severity of threats such as GPS spoofing, jamming and unauthorised access. Vulnerability captures weaknesses in communication links, navigation systems, ground control stations and operational procedures. Preparedness captures the policies, controls, training and incident-response arrangements available to the organisation. Governance and operating environment captures regulatory clarity, accountability, inter-agency coordination and security culture. Each dimension is scored from 0 to 1, and the weighted posture score is calculated as $100 \times [0.40P + 0.25G - 0.20T - 0.15V]$. Scores of 0–39 indicate a weak posture, 40–59 developing, 60–79 established and 80–100 strong. For example, dimension scores of $T = 0.65$, $V = 0.60$, $P = 0.55$ and $G = 0.50$ produce a score of 12.5, indicating a weak posture. The framework is adaptive in three senses: it supports context-sensitive weighting, periodic reassessment and feedback from incidents into control prioritisation.

The framework has three practical uses. First, it can be used as a diagnostic tool: agencies can assess their current practices across the four dimensions and identify the weakest areas. Second, it can support prioritisation: limited resources can be directed to the controls and capabilities that are most likely to reduce risk, rather than spread thinly across every possible measure. Third, it can support accountability: a common assessment structure allows regulators and oversight bodies to compare practices, track improvement and identify where support is needed. These uses are consistent with the RMF philosophy of continuous monitoring and the C2M2 logic of staged capability improvement.

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Several theoretical implications follow. The findings support the argument that UAV cybersecurity is a socio-technical phenomenon rather than a purely technical one. They also show that the four frameworks are not equivalent: RMF and C2M2 provide process and maturity structure, TOE explains contextual variation, and STS explains the human mechanisms through which controls operate. Integrating them is therefore not a matter of combining acronyms but of assigning each lens a distinct analytical role. This has implications for future research, which should test the relative explanatory power of each dimension rather than treating the framework as a single undifferentiated model.

Strengthening UAV cybersecurity in Nigeria requires coordinated policy reform, inter-agency collaboration and sustained investment in human capital. Specifically, the study recommends: (i) UAV-specific cybersecurity standards and certification requirements for national security operators; (ii) clearer mandates and coordination among aviation, ICT and security regulators; (iii) specialised training for operators, engineers and analysts; and (iv) institutionalised incident reporting, forensic investigation and lessons-learned mechanisms. Implementing the proposed framework can support security agencies in moving from reactive responses to proactive, capability driven cybersecurity governance.

This study examined cybersecurity vulnerabilities and resilience strategies in national security UAV operations in Nigeria using a mixed-methods approach grounded in RMF, TOE, C2M2 and STS. The evidence shows that UAV systems are exposed to serious cyber threats, notably GPS spoofing, signal jamming and unauthorised access; that communication, navigation and ground control components are critical points of weakness; and that organisational preparedness remains low. Regulatory fragmentation, capacity deficits and weak incident reporting compound these vulnerabilities.

The study has several limitations. It is cross-sectional and relies on self-reported perceptions, so it identifies associations rather than causal relationships. The achieved sample of 150 respondents is below the initial Yamane target of approximately 390, reflecting access restrictions and institutional gatekeeping; the findings are therefore not statistically representative of the entire Nigerian UAV ecosystem. The qualitative sample of ten key informants provides depth but not saturation across all stakeholder categories. The study did not conduct platform-level penetration testing or flight trials, so it does not independently verify the technical effectiveness of specific controls. Finally, the framework has been developed and preliminarily assessed but not tested longitudinally or across a representative sample of agencies.

Future research should address these limitations in four ways. First, a larger, multi-agency survey would improve representativeness and permit confirmatory factor analysis and structural equation modelling. Second, longitudinal case studies could examine whether improvements in preparedness are followed by reductions in incidents. Third, controlled technical testing and flight trials could validate the effectiveness of specific controls under Nigerian operating conditions. Fourth, comparative studies across African countries would help distinguish context-specific findings from more general patterns.

6. LIMITATIONS AND FUTURE RESEARCH

7. CONCLUSION AND POLICY IMPLICATIONS

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.

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

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

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

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

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

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

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.

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

ISSN: 2971-7760 | VOL 10, ISS 1 | 25 NOVEMBER 2026
https://doi.org/10.5281/zenodo.24523085
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

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

Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper & Row.

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