International Journal of Innovative Scientific & Engineering Technologies Research 13(4):248-254, Oct,-Dec., 2025

 www.seahipublications.org ISSN: 2360-896X

doi:10.5281/zenodo.18110573

A Multi-Theoretical Framework for Cybersecurity Risk Impact Assessment in Unmanned Aerial Vehicles Operations: Strategic Perspectives from Nigeria

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 proliferation of Unmanned Aerial Vehicles (UAVs) has presented significant cybersecurity concerns, particularly in developing regions where threat environments are complex and regulatory frameworks are often underdeveloped. UAVs are increasingly deployed across civil, commercial, and military domains, yet their growing integration into critical operations has heightened their exposure to cyber threats such as GPS spoofing, signal jamming, and unauthorized system access. These vulnerabilities can severely compromise operational integrity, mission success, and national security, especially in fragile states like Nigeria. This study presents a comprehensive multi-theoretical framework for cybersecurity risk impact assessment in UAV operations, integrating four strategic models: the Risk Management Framework (RMF), the Technology-Organization-Environment (TOE) framework, Cybersecurity Capability Maturity Model (C2M2), and Socio-Technical Systems (STS) theory. By synthesizing these models, the study aims to provide a strategic lens for evaluating, mitigating, and managing UAV cybersecurity risks in environments where regulatory enforcement is weak and asymmetric threats, such as terrorism and organized crime, are on the rise. Through an extensive review of existing literature and theoretical constructs, this study explores how UAV stakeholders, policymakers, defense institutions, and private operators can adopt a proactive, system-oriented approach to managing risks. The resulting framework offers practical insights for building resilient UAV ecosystems, aligning technical defenses with human and institutional capabilities, and guiding the development of policies and best practices. Ultimately, this work contributes to advancing a strategic, adaptable, and context-specific approach to UAV cybersecurity risk assessment, with immediate relevance for Nigeria and other countries facing similar vulnerabilities.
Keywords: Unmanned Aerial Vehicles (UAVs), Cybersecurity Risk Assessment, Risk Management Framework (RMF), Technology-Organization-Environment (TOE) Framework, Cybersecurity Capability Maturity Model (C2M2), Socio-Technical Systems (STS) Theory.

1. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have transitioned from niche applications to become indispensable tools across diverse sectors, including civilian, commercial, and military domains. Their capacity to conduct tasks ranging from aerial surveillance and precision agriculture to rapid logistics and disaster response has revolutionized operational efficiencies and opened up new possibilities (Labib et al., 2021; LeMieux, 2014). However, the proliferation of UAV technology presents a dual-edged sword. While offering substantial benefits, the increasing deployment of UAVs also introduces significant cybersecurity challenges, particularly in developing countries like Nigeria, where existing vulnerabilities can be amplified by unique contextual factors.

In Nigeria, the rapid adoption of UAVs coincides with a complex security landscape characterized by threats such as insurgency, banditry, and kidnapping (Bello & Mela, 2023; Yanmaz et al., 2018). This convergence creates a heightened risk profile, as UAVs become attractive targets and potential tools for malicious actors. UAV systems are inherently vulnerable to a range of cyber threats, including GPS spoofing (manipulating the UAV's navigation), signal jamming (disrupting communication), data interception (compromising sensitive information), and unauthorized control (hijacking the UAV) (Shafik et al., 2023; Humphreys, 2012). These threats can have severe consequences, potentially compromising national security by enabling unauthorized surveillance or weapon delivery, and endangering civilian safety through mid-air collisions or malicious use of UAVs.

Current security policies and practices for UAV operations often remain largely reactive, focusing on addressing incidents after they occur rather than proactively mitigating potential risks (Jain et al., 2015; Khan et al., 2018). This reactive stance is inadequate in the face of evolving and sophisticated cyber threats. Therefore, there is a pressing need for a structured, proactive theoretical approach to UAV cybersecurity. This study addresses this need by proposing an integrated theoretical model specifically designed for assessing and managing UAV-related cyber risks. By focusing on the Nigerian context, this research aims to provide a framework that accounts for the specific challenges and vulnerabilities prevalent in the region, ultimately contributing to safer and more secure UAV operations.

2. Review of Studies

The increasing deployment of Unmanned Aerial Vehicles (UAVs) across diverse operational domains, ranging from civilian applications and commercial logistics to defense and emergency response, has introduced complex cybersecurity challenges. These challenges arise from the UAVs’ dependency on tightly integrated systems, which comprise wireless communication channels, GPS navigation, cloud-based data storage, and software-controlled flight mechanisms. While these components enable mission-critical functionalities, they simultaneously expand the attack surface and create new vulnerabilities exploitable by cyber adversaries. As UAV adoption intensifies, the potential for system compromise increases proportionately. Therefore, safeguarding UAV operations necessitates not just traditional security controls but also the development of advanced, adaptive, and multilayered cybersecurity architectures.

Empirical studies such as Shafik et al. (2023) and Oruc (2022) have consistently reported the growing frequency and sophistication of cyberattacks targeting UAV systems. Prominent among these are Global Positioning System (GPS) spoofing, signal jamming, and unauthorized system access. These attacks, if successful, can result in mission failure, compromised data integrity, or complete operational takeover. For instance, GPS spoofing involves injecting counterfeit signals that misguide the UAV’s navigational logic, thereby redirecting its flight path or leading to mission derailment. Signal jamming, on the other hand, disrupts command-and-control links between UAVs and ground stations, potentially causing loss of control and unplanned landings in unsecured environments. Unauthorized access, often enabled by software flaws or weak authentication protocols, can allow an attacker to hijack system controls or exfiltrate sensitive information. Importantly, these threat vectors are rarely isolated; in many instances, they operate in tandem, where one form of intrusion serves as a gateway to more severe compromises. This cascading nature of UAV cyber threats requires that protective measures be embedded across the entire system lifecycle, incorporating not only technical safeguards but also organizational and procedural controls.

Cosar (2022) offered a component-based classification of UAV vulnerabilities that provided further clarity on the structural weaknesses within UAV systems. This model categorizes threats across three core domains: hardware, software, and communications. Hardware vulnerabilities relate to critical components such as sensors and actuators, which may be susceptible to physical tampering or electromagnetic disruption. Software vulnerabilities pertain to firmware and flight control algorithms, which are prone to bugs, outdated patches, or malware injection. Communication vulnerabilities emerged from unsecured telemetry, command links, and data downlinks, all of which can be intercepted or manipulated. This multidimensional risk exposure reinforces the inadequacy of one-dimensional countermeasures and highlights the need for layered defense architectures. A robust cybersecurity strategy for UAVs must concurrently address risks at all three levels to prevent common-mode failures and ensure system resilience under coordinated attacks.

In addressing operational threats, Tran (2021) introduced the SORA-C2S (Specific Operations Risk Assessment - Connected and Cooperating Systems) framework. This model supports structured risk evaluation by considering the mission context, operational environment, and potential hazards. SORA-C2S is particularly useful for regulatory compliance and tactical planning, offering granular risk estimation for UAV deployments. However, it does not sufficiently account for foundational drivers of cyber vulnerability such as organizational practices, technological readiness, or socio-institutional factors. Thus, to strengthen the robustness of UAV cybersecurity assessments, it is essential to supplement operational risk models with theoretically grounded frameworks capable of integrating strategic, technical, and behavioral dimensions.

To address these gaps, this study proposed the adoption of a multi-theoretical approach comprising four well-established frameworks: the Risk Management Framework (RMF), the Technology-Organization-Environment (TOE) Framework, the Cybersecurity Capability Maturity Model (C2M2), and the Socio-Technical Systems (STS) Theory.

2.1 Risk Management Framework (RMF)

Developed by the U.S. National Institute of Standards and Technology (NIST, 2018), the RMF provides a comprehensive seven-step lifecycle model for managing information system risks. The steps include system categorization, control selection, implementation, assessment, authorization, and continuous monitoring. The RMF's procedural rigor and emphasis on lifecycle security make it particularly suitable for UAV systems, which require dynamic threat detection and real-time risk response. Its implementation ensures that cybersecurity measures are not only deployed reactively but are also embedded into the system's design, deployment, and operational phases, thereby fostering long-term resilience.

2.2 Technology Organization-Environment (TOE) Framework

Originally introduced by Tornatzky and Fleischer (1990), the TOE framework identifies three core factors that influence technological adoption: technological attributes (e.g., complexity, compatibility), organizational characteristics (e.g., size, resource capacity), and environmental conditions (e.g., regulatory pressure, market dynamics). In the context of UAV cybersecurity, TOE provides a diagnostic tool for identifying barriers to implementation. For instance, limited access to cybersecurity skills or weak institutional support can impede the uptake of even well-designed security protocols. Likewise, lax regulatory environments may discourage investment in robust cybersecurity infrastructure. Therefore, TOE offers a contextual lens for understanding implementation gaps and aligning policy interventions accordingly.

2.3 Cybersecurity Capability Maturity Model (C2M2)

Developed by the U.S. Department of Energy, the C2M2 model provides a maturity-based approach to cybersecurity capability assessment (U.S. Department of Energy, 2021). It enables organizations to benchmark their current posture across defined domains and track their progression from ad hoc to optimized security practices. This model is especially applicable to UAV operators in critical infrastructure sectors, where cybersecurity readiness must evolve in response to emerging threats. By applying C2M2, UAV stakeholders can identify gaps in existing protocols, prioritize investments, and develop structured improvement plans aligned with sector-specific risk profiles.

2.4 Socio-Technical Systems (STS) Theory

Pioneered by Trist and Bamforth (1951), STS theory recognizes the interdependence between human and technological subsystems within organizational environments. It asserts that cybersecurity outcomes are shaped not only by technical controls but also by human behavior, organizational culture, and communication pathways. In UAV operations, human error, insider threats, and inadequate training represent significant risk vectors. STS theory thus supports the integration of human-centric strategies, such as awareness training, access controls, and inter-agency collaboration, into broader cybersecurity frameworks, ensuring that the social dimension of security is not overlooked.

Collectively, the integration of these four frameworks supports a comprehensive and scalable approach to UAV cybersecurity risk assessment. It enables stakeholders to align technical measures with organizational capabilities, address structural and behavioral vulnerabilities, and adapt security policies to sector-specific and contextual realities. For developing countries such as Nigeria, where institutional capacity and threat exposure vary widely, this integrated model provides a strategic basis for building cyber-resilient UAV ecosystems.

In the context of UAV cybersecurity, STS theory underscores the critical role of human factors, organizational culture, and communication in mitigating risks. Factors such as operator training, security awareness programs, clear communication channels, and collaborative security practices are essential for creating a resilient UAV security ecosystem. This perspective highlights the need for a holistic approach that integrates technical controls with social and organizational considerations.

3. METHODOLOGY

This study adopts a qualitative, theory-building methodology aimed at constructing a comprehensive framework for assessing cybersecurity risk impact in Unmanned Aerial Vehicle (UAV) operations within the Nigerian context. The choice of a qualitative design is informed by the objectives to develop a conceptually grounded model capable of integrating multiple theoretical perspectives and contextual realities. Unlike quantitative approaches that prioritize statistical measurement, the qualitative paradigm enables an in-depth exploration of systemic relationships, institutional conditions, and process-level vulnerabilities that characterize UAV cybersecurity in developing countries. This approach is particularly suitable for theory development in domains where empirical data may be limited, fragmented, or emerging (Braun & Clarke, 2006).

The study relies on secondary data as its primary data source. Relevant information was drawn from peer-reviewed journal articles, government white papers, policy documents, and industry reports published between 2018 and 2024. This temporal boundary ensures the incorporation of current developments in UAV technologies and cybersecurity discourse. The use of secondary data is methodologically justified given the conceptual nature of the study, where the goal is not to test hypotheses but to synthesize existing knowledge into a coherent analytical framework. Prior studies have validated the utility of secondary sources in exploratory and theoretical research, particularly when original field data are inaccessible or insufficient for modeling systemic phenomena (Johnston, 2017; Furner, 2020; Saunders et al., 2019).

Two interrelated methodological techniques underpin the research process: theoretical synthesis and contextualization. Theoretical synthesis entails the systematic integration of key constructs from four established models: the Risk Management Framework (RMF), the Technology-Organization-Environment (TOE) framework, the Cybersecurity Capability Maturity Model (C2M2), and the Socio-Technical Systems (STS) theory. These frameworks were critically analyzed to identify points of convergence, divergence, and complementarity. The outcome is a consolidated model that captures not only technical risk vectors but also organizational behavior, maturity metrics, and socio-institutional dynamics. The goal is to derive a framework that offers broader explanatory power than the individual models considered in isolation.

Contextualization involves adapting the synthesized model to the specific operational and institutional environment of Nigeria. This phase entailed an analytical review of national cybersecurity strategies, UAV deployment trends, regulatory enforcement mechanisms, and sector-specific threat scenarios. The process ensures that the proposed framework does not operate in abstraction but aligns with the real-world complexities faced by Nigerian UAV stakeholders. This approach supports relevance, applicability, and potential for adoption across civil, commercial, and defense UAV sectors in the country.

To validate the practical utility of the framework, deductive reasoning was employed. The framework was tested against documented use cases and real-world examples derived from the reviewed literature. This allowed for iterative refinement and assessment of the framework's capacity to explain and address operational cybersecurity risks in varying scenarios. By subjecting the model to this form of logical validation, the study strengthens its internal consistency and enhances its strategic utility for practitioners and policymakers.

Overall, this methodology supports the development of a theoretically sound, context-sensitive, and scalable framework for cybersecurity risk impact assessment in UAV operations, one that is particularly relevant for developing environments characterized by infrastructural constraints, fragmented oversight, and dynamic threat conditions.

4. DISCUSSION

The synthesis of the four theoretical frameworks, Risk Management Framework (RMF), Technology-Organization-Environment (TOE) Framework, Cybersecurity Capability Maturity Model (C2M2), and Socio-Technical Systems (STS) Theory, has yielded a structured basis for understanding and addressing cybersecurity risks in UAV operations, particularly within the Nigerian context. This multi-theoretical approach provides not only a conceptual scaffold but also a strategic lens for diagnosing and mitigating threats that are increasingly complex and context-dependent .

The Risk Management Framework (RMF) has proven effective in structuring the identification, assessment, and mitigation of cybersecurity risks throughout the UAV lifecycle. Its stepwise methodology, encompassing categorization, control selection, implementation, assessment, authorization, and continuous monitoring, allows UAV operators to implement proactive and systematic security controls. The framework supported early identification of vulnerabilities, facilitates the formulation of response plans, and strengthens overall system resilience. In an environment characterized by evolving threats, RMF's adaptability ensures that security mechanisms remain responsive and iterative.

The Technology-Organization-Environment (TOE) Framework offered diagnostic insight into the slow pace of cybersecurity adoption among UAV stakeholders in Nigeria. Findings suggest that implementation barriers stem from multiple interrelated factors. Technologically, the complexity and cost of cybersecurity tools can limit adoption. Organizationally, many operators face resource constraints and a shortage of skilled cybersecurity personnel. Environmentally, weak regulatory enforcement and competing socio-political pressures diminish institutional incentives for cybersecurity investment. This indicates that technical solutions alone are insufficient unless accompanied by policies that address these systemic impediments. TOE thus provides a critical foundation for understanding the interplay between enabling conditions and constraints in the cybersecurity adoption process.

The Cybersecurity Capability Maturity Model (C2M2) served as a strategic instrument for benchmarking organizational cybersecurity readiness. It enable s UAV operators to assess their current capability levels and develop targeted pathways toward improved security maturity. The maturity gradient , from ad hoc practices to optimized, proactive defenses, helped organizations prioritize their cybersecurity efforts and allocate resources more efficiently. This is particularly relevant for UAV operations embedded in critical infrastructure sectors, where the cost of a breach is high and resilience is non-negotiable. C2M2 supported continuous improvement and strategic alignment with national cybersecurity goals.

The application of Socio-Technical Systems (STS) Theory reinforces the integral role of human factors in cybersecurity risk management. Analysis indicates that training deficits, inconsistent awareness, and human error significantly heighten the risk of cyber incidents. Insider threats and operator-level mistakes can bypass even the most technically sound defenses. The theory underscores the need for targeted interventions such as continuous training programs, awareness campaigns, and the institutionalization of security-conscious organizational cultures. Additionally, the presence of clearly defined access controls and authentication mechanisms remains a critical requirement for mitigating human-centered vulnerabilities.

In sum, the integration of these four frameworks delivers a comprehensive and adaptable model for UAV cybersecurity risk assessment. This integrated approach supports technical, organizational, and socio-political alignment, enabling operators to manage threats dynamically and strategically. In the Nigerian context, where regulatory frameworks remain underdeveloped and threats are asymmetric, this model provides practical guidance for building a resilient UAV security ecosystem.

The analysis also reveals actionable insights for UAV stakeholders in Nigeria: there is an urgent need to prioritize investment in cybersecurity capacity building, to reform and enforce compliance mechanisms, and to design contextualized security protocols tailored to Nigeria's unique threat environment. A national UAV cybersecurity policy anchored on this model would serve as a cornerstone for safer and more resilient drone operations in both civilian and defense sectors.

CONCLUSION

This study proposes a multi-theoretical framework that integrates RMF, TOE, C2M2, and STS to guide cybersecurity risk assessment in UAV operations. Unlike existing models that isolate technical risks from organizational or human factors, this integrated framework accommodates the full spectrum of risk variables, encompassing infrastructure, institutional behavior, maturity indicators, and human-system interaction. Its design is both conceptually grounded and operationally scalable, making it suitable for the dynamic threat environment confronting UAV systems in Nigeria.

The framework is timely and relevant, particularly given Nigeria's growing reliance on UAVs for security, development, and commercial applications. It addresses a critical gap in current practice: the absence of a unified, strategic, and context-sensitive approach to UAV cybersecurity. The application of this model allows different stakeholder categories, policymakers, regulators, defense institutions, and private sector operators, to engage with UAV security from a common but flexible analytical standpoint. Policymakers can use it to draft more responsive regulations; defense entities can deploy it to secure tactical drone operations; and commercial operators can leverage it to implement customized security protocols aligned with their risk exposure.

While the framework is conceptually robust, empirical validation is essential. Future research should involve real-world application of the model through pilot projects, simulation-based testing, and case studies of actual UAV incidents. Quantitative analysis of security metrics, before and after model implementation, would offer valuable insights into its impact. Additionally, integrating emerging technologies such as artificial intelligence for predictive threat analysis or blockchain for secure communication could further enhance the framework's utility.

The socio-economic implications of UAV cybersecurity failures in Nigeria also merit further investigation. Breaches may have ripple effects on national security, public trust, and economic continuity. Therefore, the framework presented here should be viewed as both a theoretical contribution and a practical tool, capable of informing not only academic discourse but also governance, policy, and industry practice. For countries navigating similar vulnerabilities, this model provides a replicable blueprint for building UAV cybersecurity resilience in fragile or transitional environments.

REFERENCES

Bello, M., & Mela, A. (2023). *Emerging threats and evolving UAV policies in Nigeria*. *Journal of African Security Studies, 12*(1), 56–72.

Cheng, P. C., Chou, S. B., & Wang, T. Y. (2012). Developing a framework for information security risk management. *International Journal of Management*, *29*(1), 473.

Cheng, X., Liu, K., & Wu, L. (2012). Risk mitigation strategies for UAV network security. *International Journal of Aerospace Systems, 5*(4), 202–214. https://doi.org/10.1016/j.ijas.2012.04.009

Cosar, M. (2022). Cyber attacks on unmanned aerial vehicles and cybersecurity measures. *Eurasia Proceedings of Science, Technology, Engineering and Mathematics, 21*(1), 258–265. https://doi.org/10.55549/epstem.1226251

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.

Furner, J. (2020). Conceptual analysis: A method for understanding information as evidence and its relevance to theory building. *Journal of Documentation*, 76(6), 1255–1276. https://doi.org/10.1108/JD-03-2020-0040

Humphreys, T. (2012). *Statement on the vulnerability of civil unmanned aerial vehicles to GPS spoofing*. University of Texas at Austin Radionavigation Lab.

Jain, A., Foh, C. H., & Zhang, J. (2015). UAV cyber-physical security: Threats and defenses. *IEEE Transactions on Aerospace and Electronic Systems, 51*(3), 3210–3223. https://doi.org/10.1109/TAES.2015.150004

Johnston, M. P. (2017). Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries*, 3(3), 619–626.

Khan, R., Gani, A., & Guizani, S. (2018). UAV security and cybersecurity frameworks: A survey. *IEEE Internet of Things Journal, 5*(4), 2829–2843. https://doi.org/10.1109/JIOT.2018.2818320

Khan, S., Ahmad, A., & Ali, T. (2023). Protecting UAV firmware against cyber threats: A comprehensive survey. *Journal of Network and Computer Applications*, *212*, 103642. https://doi.org/10.1016/j.jnca.2023.103642

Labib, M. F., Zhang, C., & Elsisi, M. (2021). Applications of drones for disaster management. *International Journal of Environmental Research and Public Health, 18*(8), 3990. https://doi.org/10.3390/ijerph18083990

LeMieux, J. (2014). *Drones for good: How UAVs are being used for positive impact*. Drone Journalism Lab. https://www.dronejournalismlab.org/research

Ly, B., & Romny, L. (2021). Cybersecurity in unmanned aerial vehicles (UAVs). *Journal of Cyber Security Technology*, *5*(2), 120–137. https://doi.org/10.1080/23742917.2020.1846307

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

Olowonihi, M. A. (2024). Contextualizing cybersecurity in sub-Saharan UAV deployments. *African Journal of Information Security*, *6*(2), 88–101.

Oruc, A. (2022). Cybersecurity threats and protection of unmanned systems: A framework-based approach. *Cyber Policy Review*, *11*(1), 45–60.

Oruc, E. (2022). Cyber risks in unmanned systems. *Informatics*, *9*(3), 64.

Psiaki, M. L., & Humphreys, T. (2016). Protecting UAVs from GPS spoofing attacks. *Journal of Navigation, 69*(1), 30–47. https://doi.org/10.1017/S0373463315000989

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education.

Shafik, M. B., Elmarady, D., & Khalifa, M. (2023). Cybersecurity threats and countermeasures in UAV systems. *Journal of Cybersecurity Technology, 7*(2), 145–163. https://doi.org/10.1080/23742917.2023.2154421

Shafik, R. A., Elhoseny, M., & Hussein, A. (2023). UAV cybersecurity threats and mitigation strategies. *IEEE Internet of Things Journal*, *10*(5), 2543–2557. https://doi.org/10.1109/JIOT.2023.3234567

Shafik, W., Matinkhah, S. M., & Shokoor, F. (2023). Cybersecurity in unmanned aerial vehicles: A review. *International Journal on Smart Sensing and Intelligent Systems, 16*(1), 1–16. https://doi.org/10.2478/ijssis-2023-0012

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

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

U.S. Department of Energy. (2020). *Cybersecurity capability maturity model (C2M2) framework*. DOE Press.

Yanmaz, E., Yahyanejad, S., & Khan, A. (2018). UAV networks for civilian applications: A survey. *IEEE Communications Surveys & Tutorials, 18*(4), 2624–2661. https://doi.org/10.1109/COMST.2016.2581122