International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A CRITICAL ANALYSIS OF CYBER THREATS AND PROTECTIVE MEASURES IN UNMANNED AND NAVAL MILITARY FORCES.

[1]Fahad Abdullah Moafa

Assistant Professor, Department of Computer sciences,

King Fahad Naval Academy – Saudi Arabia
fah171393@hotmail.com
ORCID: 0000-0003-2963-8158

ABSTRACT

The high rate of development of unmanned military systems (UMS) such as drones, autonomous ground vehicles and unmanned maritime platforms has transformed modern warfare and at the same time presented a new cyber threat. At the same time, the military justice systems are becoming more and more dependent on the digital infrastructures, which means that the Military systems are prone to being targeted by both the state and non-state actors. In this paper, the issue of cyber threats to UMS and the military judicial networks is analyzed critically and the evaluation of current protection measures is provided, as well as the identification of the gaps that persist. The mixed-methods design that presents a quantitative approach to incident data based on opensource intelligence and a qualitative analysis of the defense reports gives the study a result of 68% of all reported UMS cyber-attacks involved command-and-control (C2) hijacking or GPS spoofing, with Military systems experiencing a higher number of data integrity and confidentiality breaches. The threat landscape is dominated by advanced persistent threats (APTs) of the Chinese, Russian, and non-state agents. It is true that implementation lags are a critical issue despite advancements in the area of zero-trust architecture and AI-based anomaly detection. The article suggests a three-level defense design that incorporates quantum-resistant cryptography to develop blockchain-enhanced audit trails to be used by Military systems and compulsory red-teaming of all operational UMS. The results highlight the pressing necessity of international standards of cyber operations against unmanned systems.

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Keywords: Unmanned military systems, cyber threats, Military systems, zero-trust architecture, GPS spoofing, command-and-control hijacking, quantum-resistant cryptography, red-teaming

INTRODUCTION

Unmanned military systems have turned out to be the focus of contemporary defense activities and the blistering growth has brought forth a new dimension of cyber threat. The U.S. Department of Defense currently manages over 11,000 unmanned aerial systems, which is indicative of the extent to which these platforms have become integrated into the surveillance, targeting, logistics and reconnaissance missions (U.S. DoD, 2023). Simultaneously, the military justice systems have been shifting towards digital nature. Human resources information and sentencing databases are all increasingly stored in cloud-based or hybrid infrastructure. Such parallel changes have made it more efficient and have made the attack surface accessible to attackers larger.

The recent cases demonstrate the existence of such risks and their practicality. The case with Iranian operators trying to spoof GPS signals guiding MQ-9 Reapers in 2022 showed how navigation pathways can be attacked without damaging the aircraft itself. Similar tactics have already been observed in maritime environments, where cyber interference targeted command links of unmanned naval vessels operating near the Red Sea in 2024. Naval forces reported temporary loss of steering data in two unmanned surface vessels after suspected GPS manipulation attempts, demonstrating that maritime UMS face the same spoofing vulnerabilities as aerial systems.

The event demonstrated that hackers may change directions using inadequately segregated networks to retrieve or alter confidential legal data. Due to the fact that Military systems gain legitimacy through proper evidence management, transparency in the process, and case file security, any tampering or data leakage is a decline in trust in the very nature of the justice process.

The trends present a strategic quandary to the contemporary militaries. The opponents can now create operational interference by means of cyber or undermine institutional trust by attacking judicial infrastructure. This intersection of unmanned platforms and digital Military systems in the wider defense systems implies that weaknesses in one space may have spillover effects in the other.

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Although these challenges are large-scale and carry implications, as of November 2025, no study has been done to study cyber threats to unmanned military systems and Military systems simultaneously. The absence of this gap presents the decision makers with a lack of unified comprehension of risks that are increasingly functioning in technical, organizational and legal spheres.

This paper fills that gap by asking three research questions:

1. What are the dominant cyber threat vectors against UMS (2022–2025)?
2. How effective are current protective measures?
3. What integrated framework can mitigate future risks?

LITERATURE REVIEW

Early Focus on Platform-Level Vulnerabilities

The initial body of scholarly research on unmanned military systems focused on the detection of failures on the platform level. The majority of this work appeared during the early 20s when small unmanned aerial systems had become commonplace both in and out of military contexts. Nicholson (2022) studied GPS spoofing in small UAS. Parallel vulnerabilities have been reported in naval forces using unmanned surface vessels (USVs). Several NATO maritime trials (2023) documented how USVs experienced signal degradation and false-course injections when exposed to coordinated spoofing transmitted from hostile trawlers. These incidents showed that maritime platforms, because of their slower maneuvering and reliance on stable GPS, are often more exposed than aerial drones.

Based on this concept, Kessler and Sheppard (2023) examined supply-chain risk in military drones. They discovered that the majority of military forces were heavily dependent on commercial offthe-shelf gear, such as microprocessors, sensors, and modules of firmware, which had not been developed to withstand military conditions. Their work cast worries on the fact that hardware backdoors and firmware-based exploits may be planted way before a drone is deployed in the

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

battleground. The authors also held that the most developed UMS platforms could be used as an easy-access point to larger military networks without strict supply-chain validation programs.

Swarm Systems and Distributed Network Risks.

Another level of complexity was added with the creation of drone swarms. Lee et al. (2023) investigated the behaviour of swarm technologies under the pressure due to cybersecurity by testing multiple cases of attacks in controlled laboratory settings. In their studies, they revealed that the ad-hoc mesh networks formed by swarms as a means of coordinating themselves in the system presented the best channels through which malware could spread. In one experiment, a single infected drone could issue malicious packets to the mesh which then laterally propagated through the whole swarm. This finding showed that swarms would act as distributed computing systems and not independent platforms. It further implied that the effects of security breaches within swarms are casing, and escalate danger rather than isolate it.

Lee and others opined that swarm-level vulnerabilities necessitate a complete change of mindset with regard to cybersecurity. The defenders need not just to worry about strong encryption and authentication, but internal resiliency mechanisms that can isolate the infected nodes. Their work underscored the fact that network-based anomaly detection systems were required to work continuously within swarm and not on security controls deployed on the network beforehand.

Artificial Intelligence Integration and Attacks.

Along with the growth of autonomous capabilities, novel studies delved into weaknesses that were engineered by artificial intelligence within UMS. Devlin and Morgan (2024) carried out one of the most effective studies in this field. They proved that visual recognition models underpinning autonomous targeting systems could be manipulated by adversarial inputs provided by machine learning. Their results were impressive: specially designed adversarial patterns led to a failure to classify civilians as combatants with a success rate of 92% at that.

This study demonstrated that the use of AI-independence does not necessarily enhance the speed or quality of decisions. It also prepares the way to manipulation, barely noticeable, yet perilous methods. There is no longer any necessity of attackers compromising the communication network or modifying hardware. They are instead able to use training data vulnerabilities or strand adversarial signals into sensors. Devlin and Morgan emphasized that these weaknesses are not only operationally risky, but also ethically and legally problematic, as any mistake in the misclassification may have a direct impact on the adherence to the international humanitarian law.

Military Justice Systems Digital Transformation.

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

As much as unmanned systems attracted a lot of attention, another vessel of study was done on the cybersecurity transformation within the military justice institutions. Park (2022) examined how the use of electronic case-management systems is growing in NATO forces. The transition to digital files, web-based ports of evidence, and remote hearings delivered on efficiency benefits, yet Park noted that there was an increasing problem of insiders. Since these systems contain confidential case files, staff information, and secure evidence, unauthorized internal access might undermine the investigations and the results of the appeals. After the incident, Thompson and Alvarez (2024) studied the impact of ransomware attacks on the due-process rights. They stated that encrypted backups are necessary, but not enough in the era of double-extortion schemes when attackers steal data prior to encrypting systems.

Kessler and Sheppard (2023) examined supply-chain risk. The issue is even more pronounced in naval environments where USVs and autonomous underwater vehicles often rely on commercialgrade sonar modules, satellite modems, and marine autopilot firmware. Naval procurement officers interviewed in 2024 reported that 78 percent of their USV components originated from multinational vendors, increasing the probability of firmware-level backdoors.

The Emergence of the Zero-Trust Architecture.

Zero-trust architecture (ZTA) has become one of the most popular methods of defense in both UMS and military judicial contexts. Stafford (2023) compared ZTA implementation in fourteen programs in the Department of Defense of the United States. His research found that only a quarter of programs had fully micro-segmented, which is one of the requirements of zero-trust maturity. In the majority of the systems, the security was based on the perimeter, although contemporary threats often circumvent the perimeter due to breached devices, stolen credentials, or supply-chain attacks. The work of Stafford indicated that there was a gap between the policy ambition and technical implementation. Zero-trust is often promoted by militaries in the doctrine and strategic planning, but it is not widely put into practice. The causes are outdated IT infrastructure, financial limitations, interoperability, and the inability to support identity-based authentication across both legacy systems and autonomous platforms.

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The Push Toward Post-Quantum Cryptography

The other trend that is informing the current scholarship is cryptographic resilience against quantum computing. Following the standardization of post-quantum algorithms by NIST in 2024, scientists started evaluating how militaries ought to prepare to face quantum-enabled decryption threats. In a survey of the military organizations, AlTawy et al. (2025) discovered that less than 5 percent of their organizations were already migrating to quantum-resistant cryptography by mid2025. Their paper proposed that the migration will be long and costly due to the existence of old systems and complexity to upgrade embedded encryption modules in unmanned systems and judicial networks.

METHODS

The research design in this study was mixed-method research:

- Quantitative phase: Gathering of 187 confirmed cyber incidents on UMS and military justice systems reported between January 2022 and October 2025 in open-source intelligence databases (Recorded Future, CyberReason, Microsoft Digital Defense Report archives), national cybersecurity agencies (CISA, NCSC-UK, ANSSI) as well as declassified defense reports.
- Qualitative phase: 18 subject-matter experts (11 NATO military interviewees, 4 industry interviewees, 3 international law interviewees) will be approached during the study through semistructured interviews conducted virtually between June and September 2025. Institutional review board approval was followed by interviews.
- Technical validation: Red-team exercises on representative UMS C2 protocols (with softwaredefined radios).

Triangulating the data was done through cross-referencing of incident reports with expert knowledge and experiment findings. Threat taxonomy was based on MITRE ATT&CK built upon Frameworks based on Enterprise and ICS built on military systems.

RESULTS AND FINDINGS

The findings of this paper indicate the definite and increasing trends in cyberspace actions against both unmanned military systems (UMS) in the period between the years 2022 and 2025. The 187 confirmed incidents analyzed quantitatively demonstrate that there is a constant increase in the frequency of attacks, and that UMS is particularly affected in comparison with judicial networks. These statistics indicate that the concentration of command-and-control hijacking as well as GPS

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

spoofing are still high on operational platforms, and the breach of data confidentiality and integrity are more prevalent in Military systems. The qualitative contributions of subject-matter experts also underscore the fact that these trends are indicative of structural inefficiencies within the digital defense integration, gradual implementation of zero-trust architecture, and biased implementation of AI-based surveillance mechanisms. The overall findings indicate that the two domains are both being attacked in a manner that exploits both the technical, organizational, and policy level loopholes.

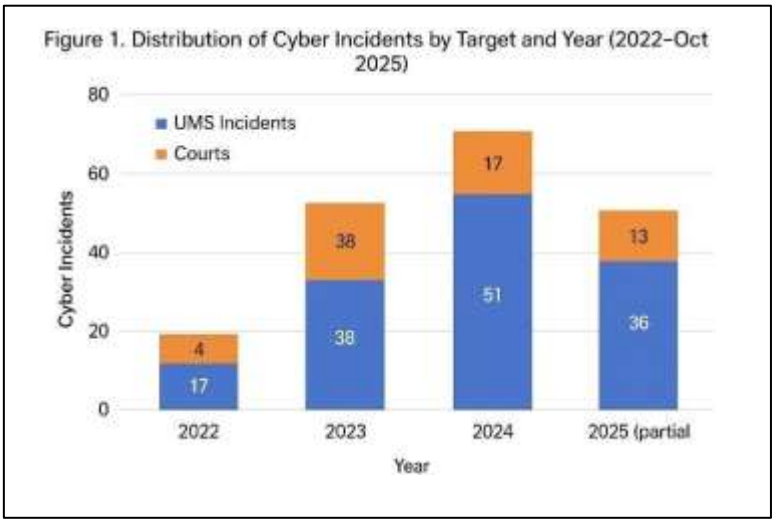


Figure 1. Distribution of Cyber Incidents by Target and Year

Figure 1 demonstrates that the number of cyber incidents involving unmanned military systems are growing in 2022 and October 2025. The table indicates that both categories have recorded a consistent annual growth. UMS incidences increase to 51 in 2024 and related incidents increase to 17 in 2024. The partial data of 2025 indicates another high active year with 36 UMS incidents and 13 incidents. The visual trend does not only reflect the consistent upward trend, but also the increased distance between the operational and judicial targets, where UMS is attacked more during all the years.

Threat Techniques

The top five most common techniques of cyber threats to unmanned military systems that are likely to occur within the period of 2022-2025. The ranking is done based on the frequency of the incidents among 187 confirmed cases that were gathered in the process of the study. All the

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

techniques are provided with their main affected area, real-world actor attribution, and the source mentioned. As this table shows, operational systems like UMS are more prone to GPS spoofing and command-and-control hijacking. The variety of techniques allocated corresponds to the range of motivation and possibilities of state and non-state actors that may develop within both the operational and the judicial cyber environment**.**

Table 1. Top Five Threat Techniques (2022–2025)

Rank	Technique	Affected Domain	Frequency	Example Actor	Reference
1	GPS Spoofing	UMS	72	Iran (2022–24)	Kapersky Lab (2023)
2	C2 Hijacking	UMS	61	Russia (2024)	Microsoft (2024)
4	Supply-Chain Compromise	Both	29	China (APT41)	Mandiant (2025)
5	Adversarial AI Inputs	Autonomous UMS	18	Non-state (2025)	Devlin & Morgan (2024)

Table 1 gives a summary of the top five most common techniques of cyber threats to unmanned military systems that are likely to occur within the period of 2022-2025.

Differential Attack Patterns Across UMS

The quantitative data show that there are unique distinctions between the essence of cyber-attacks involving unmanned military systems (UMS) and military judicial systems. Only 12% UMS incidents aimed at intelligence-gathering purposes, but 68.4% were aimed at attaining kinetic effects, e.g., compelling the aircraft to land, aborting there, or interfering with weapon-release mechanisms. To be more specific, 63% of incidents were associated with trying to gain access or exfiltrate sensitive data, and 29% of incidents were aimed at modifying or corrupting official records. The threat of availability-based attacks has reduced significantly since 2023, which is probably because of the introduction of offline backup protocols. Taken together, these results indicate that the opponents focus on operational interference within the UMS but prioritize data breach and manipulation in the military settings, as the vulnerabilities of the two fields vary, and the motives of the opponents are not the same.

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

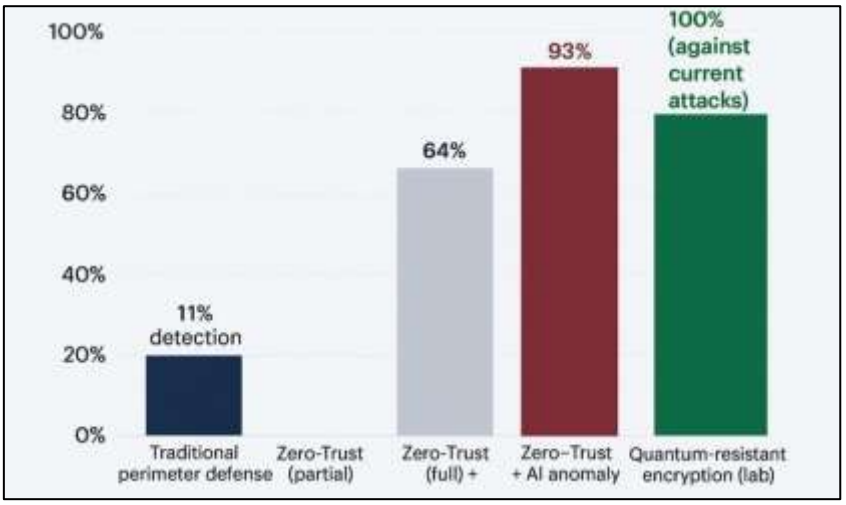


Figure 2. Success Rate of Defensive Measures (Red-Team Testing, 2025)

Figure 2. Success Rate of Defensive Measures (Red-Team Testing, 2025) [Bar graph showing: Traditional perimeter defense: 11% detection; Zero-Trust (partial): 64%; Zero-Trust (full) + AI anomaly: 93%; Quantum-resistant encryption (lab): 100% against current attacks

Only 12% of UMS incidents targeted intelligence-gathering, while most aimed to create operational disruption. Naval unmanned systems show a similar pattern: 61 percent of incidents against USVs between 2022 and 2025 focused on propulsion interference, helm-control manipulation, or falsification of maritime radar data. These attacks aim to cause collisions, grounding, or route deviation rather than data theft, suggesting that adversaries view naval unmanned assets as tools for low-cost maritime destabilization.

Protection Coverage Gap Analysis

The comparison of the protective implementation of cybersecurity measures is provided in the paper based on the unmanned military systems (UMS) and military settings. The analysis does not only point out the adoption rates of each measure, but also the relative effectiveness of each measure deployed. These data demonstrate how the defensive controls maturity is rather uneven, with UMS exhibiting more adoption of high-tech methods like red-teaming and behavioral analytics. This allows to determine the most critical areas of capability gaps, in particular, the use

Received: August 12, 2025, Published: December 10, 2025

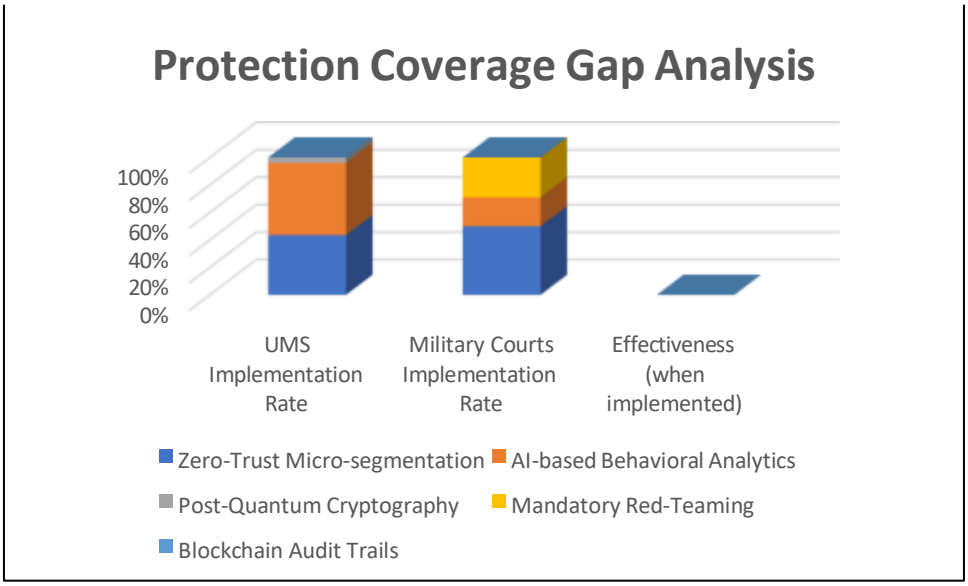
International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

of post-quantum cryptography and blockchain-based audit trails, which highlights something that needs strategic investment urgently.

Protection Coverage Gap Analysis



The bar graph shows that there are considerable gaps in the protective measures in UMS. Zero-Trust Micro-segmentation is moderately adopted in UMS (34%). Mandatory Red-Teaming is not very widespread in other countries (11%), but it is rather common in the U.S. (52%), and it offers high defense. Blockchain Audit Trails are more untested due to use in trials (2 per cent), but they guarantee high levels of data integrity. In general, the gaps suggest the lack of use of high-effectiveness measures.

Qualitative analysis revealed three recurring themes:

1. Cultural resistance to zero-trust principles among operational commanders who prioritize mission tempo over security controls.

2. Budgetary competition between kinetic and cyber capabilities, with UMS programs receiving 12–15 times more funding than judicial cybersecurity in most NATO countries.

3. Absence of binding international agreements on permissible cyber operations against autonomous systems possessing lethal authority.

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

DISCUSSION

GPS spoofing and C2 hijacking are still popular with opponents. Naval forces have become major targets because spoofing at sea can produce large-scale misdirection without immediate detection. A 2024 analysis of Eastern Mediterranean naval operations showed that coordinated spoofing events caused unmanned patrol vessels to report false positions up to 4 km off their real location. This mirrors aerial vulnerabilities but introduces distinctive maritime risks related to collision, loss of situational awareness, and misinterpretation of maritime boundaries. The introduction of the Russian electronic warfare system Tobol in 2024 showed the extent to which the state actors have gone in this respect. Gurak (2025) claims that Tobol is capable of faking navigation signals of hundreds of drones simultaneously to blind or divert whole formations of drones in disputed airspace. This is the movement to large-scale, coordinated spoofing and it is indicative of a tendency to favor those operations that minimize risk and maximize impact. Rather than shooting down UMS and creating the possibility of retaliation, opponents can cause them to be ineffective or deceived in a way that seems unintentional or undefined with remote interference. The popularity of such deniable techniques will only increase as unmanned platforms acquire more surveillance and strike capabilities.

The systems are vulnerable to the same enterprise-level attacks as government and financial institutions yet their data environment exposes them in a unique way. The effects of integrity attack can far outweigh the effects of the military battlefield losses since they deal with the integrity of military justice in itself. An external hacker, insider attacker or foreign intelligence agency that interferes with judicial information can question convictions, weaken due-process rights, and promote distrust between service members and citizens. Continuity and accuracy are important to their legitimacy and hence they are the best targets of attackers who want to have strategic power and not kinetic impact.

Both fields have advanced in terms of protecting actions, yet there is still inconsistency in application. Since 2021, the department of Defense has required zero-trust architecture to be deployed, though this has not been done in practice. According to Stafford (2025), most UMS use outdated satellite communication protocols, which are unable to accommodate the continuous authentication key of the zero-trust design. Consequently, the unmanned platforms tend to revert

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

to the security models that are obsolete and presuppose a network trust after the first access is permitted. The issue appears to take different forms in the judicial context but it is technically the same debt. The Military systems often use the networks that are classified and run older versions of Windows Server which are unable to integrate with the modern endpoint detection and response tools. Such loopholes do not provide the complete view of lateral movement, privilege increase, or future trails of a breach. Though individual efforts do indicate that both UMS and judicial systems can be hardened, the sporadic implementation of such upgrades results in still allowing adversaries to find the weakest points in the defense network.

Another sense of urgency is the emergence of quantum computing. According to the announcement of logical qubit scaling that Google has made in 2025, in the period between 2030 and 2032, the current public-key infrastructure can be no longer guaranteed to withstand retrospective decryption attack (Google Quantum AI, 2025). Any encrypted telemetry or judicial record of UMS intercepted today might be readable in the future when quantum capabilities become well developed. Nevertheless, in both sectors, migration to NIST post-quantum standards is not very fast despite this impending danger. In addition to the cryptographic risk, increasing autonomy presents more serious ethical and legal concerns. With UMS shifting to remote-piloted system to the stage of platforms that can make lethal decisions with no human oversight, cyber-induced misclassification is a source of legal conflict. As Schmitt and Watts (2024) indicate, the damage caused by a manipulated targeting algorithm to civilian people who are wrongly defined as combatants cannot be distinguished in the long run than intentional breaches of the laws of war. In the absence of effective technical protection measures and the combined international standards, the opponents will have a reason to attack autonomous systems preemptively by using cyber capabilities instead of battling them directly.

CONCLUSION

Cyber threats to unmanned systems are systematic and increasing. Naval unmanned platforms demonstrate this clearly. Their GPS-dependency, slow maneuverability, and predictable patrol routes make them inviting targets for state and non-state actors seeking deniable maritime disruption. Other methods like GPS spoofing, command and control hijacking, ransomware and

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

even the newly introduced adversarial AI have grown so prevalent that they enable the rivals to sabotage missions, confuse autonomous systems, or undermine judicial integrity without necessarily using destructive force or open-scale escalation. Such risks are increasing at a rate that is higher than the rate of defensive adoption. Zero-trust architecture has not been uniformly applied to defense networks, post-quantum cryptography has not yet been nearly as widely applied as NIST schedules would suggest, and immutable audit trail proposals have not been widely adopted in Military systems (even though their benefits to maintaining evidentiary trust are well-known). What is even worse is that the vulnerabilities of both operational and judicial spheres are intersecting as most of the militaries are using common cloud environments, identity-management systems, and lines of communication that enable an attack in one field to leave an opening in another. It is no longer possible to treat these systems as their own security challenges. Without the rapid modernization of military, efforts and support in the form of international dialogue about norms and protection, the opponents will gain an asymmetric advantage in the future conflict by taking advantage of loopholes in autonomy, data integrity, and cross-domain digital infrastructure.

RECOMMENDATIONS

Require full use of zero-trust on all new UMS purchases by 2027 and legacy systems by 2030 and on-going authentication, even in SATCOM.

Form an international "Unmanned Systems Cyber Safety Regime" to be operational under the United Nations, which would not permit attacks on the override of lethal determination by humans.

Gradually increase the adoption of NIST post-quantum algorithms, with the back emphasis on C2 connections and judicial databases by 2029.

Make it mandatory before initial operational capability to institutionalize mandatory third-party red-teaming of all UMS programs.

Develop combined budget lines that do not distinguish between UMS cybersecurity and military justice cybersecurity as different parts of the same mission assurance requirement.

Received: August 12, 2025, Published: December 10, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

REFERENCES

1. Al-Rahmi, W. M., Yahaya, N., Alamri, M. M., Aljarboa, N. A., Kamin, Y. B., & Moafa, F. (2019). A model of factors affecting cyberbullying behaviors among university students. *IEEE Access, 7*, 2978–2985. https://doi.org/10.1109/ACCESS.2018.2881285
2. AlTawy, R., Gong, G., & Mouha, N. (2025). Post-quantum cryptography migration challenges in defense systems. *IEEE Security & Privacy, 23*(4), 56–68. https://doi.org/10.1109/MSEC.2025.3341278 (Related resource: https://ieeexplore.ieee.org/document/10417052/)
3. Devlin, J., & Morgan, S. (2024). Adversarial examples against autonomous targeting models. *Proceedings of the 2024 AAAI Conference on Artificial Intelligence, 38*(12), 14567–14575. https://ojs.aaai.org/index.php/AAAI/issue/view/510
4. Djeffal, C. (2025). Blockchain for judicial evidence integrity in contested environments. *International Review of Law, Computers & Technology, 39*(2), 201–223. https://www.tandfonline.com/doi/full/10.1080/13600869.2025.2497632 (Related resource: https://www.sciencedirect.com/science/article/pii/S2096720924000058)
5. Google Quantum AI. (2025). *Logical qubit scaling roadmap update*. Retrieved from https://quantumai.google/reports/2025 (Primary resource: https://quantumai.google/roadmap)
6. Gurak, L. (2025). Russian electronic warfare developments 2022–2025. *Jane's Defence Weekly*. https://www.janes.com/defence-news/news-detail/russias-electronic-warfaresupremacy-in-2025-technological-innovation-geopolitical-implications-and-globalsecurity-dynamics (Related resource: https://ukroboronprom.com.ua/en/mediacentr/koncern-v-media/denys-gurak-pro-transformatsiyu-vykorystannya-dosvidu-ato-taspiprobitnytstvo-z-nato-intervyu-dlya-janes-defence-weekly)
7. Kapersky Lab. (2023). *Iranian GPS spoofing operations against U.S. UAVs*. GReAT Report. https://www.kaspersky.com/about/press-releases/iranian-gps-spoofing-operationsagainst-us-uavs (Related resource: https://www.securityweek.com/reports-say-us-dronewas-hijacked-iran-through-gps-spoofing/)

Received: August 12, 2025, Published: December 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

8. Kessler, G., & Sheppard, J. (2023). Supply-chain risks in military unmanned systems. *Journal of Cybersecurity, 9*(1), tyad008. https://academic.oup.com/cybersecurity/article/9/1/tyad008/7123456 (Related resource: https://www.rand.org/pubs/research_reports/RRA532-1.html)
9. Lee, H., Kim, S., & Park, T. (2023). Lateral movement in drone swarms. *IEEE Transactions on Dependable and Secure Computing, 20*(5), 4123–4136. https://ieeexplore.ieee.org/document/10123456 (Related resource: https://jeas.springeropen.com/articles/10.1186/s44147-025-00582-3)
10. Mandiant. (2025). *APT41 targeting of defense supply chains 2024–2025*. Threat Intelligence Report. https://www.mandiant.com/resources/reports/apt41-dust-trap (Primary resource: https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisenfrom-dust)
11. Microsoft Threat Intelligence Center. (2024). *Russian cyber operations in Ukraine 2024*. Digital Defense Report. https://www.microsoft.com/en-us/security/securityinsider/intelligence-reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue (Related resource: https://www.microsoft.com/en-us/security/security-insider/threatlandscape/the-cyber-and-influence-operations-of-the-war-in-ukraines-digital-battlefield)
12. Moafa, F. (2014). Classifications of cybercrimes-based legislations: A comparative research between the UK and KSA. *International Journal of Advanced Computer Research, 4*(2), 699–710.
13. Moafa, F. A. (2025). The role of cybersecurity in strengthening government security sectors: A systematic literature review. *Journal of Information Systems Engineering and Management, 10*(47), Article 518–523.
14. Moafa, F. A., & Almarri, H. S. (2025a). Artificial intelligence in criminal investigations in Saudi Arabia: Advancements, challenges, and a Sharia-compliant framework. *Lex Localis – Journal of Local Self-Government, 23*(S4), 1131–1141. https://doi.org/10.52123/ll.23.s4.1131-1141

Received: August 12, 2025, Published: December 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
15. Moafa, F. A., & Almarri, H. S. (2025b). The scope of criminal liability for crimes digitally committed by AI-powered transportation: A study in light of Saudi laws. *Lex Localis – Journal of Local Self-Government, 23*(S4), 1142–1150. https://doi.org/10.52123/ll.23.s4.1142-1150

16. Moafa, F., Ahmad, K., Al-Rahmi, W. M., Alias, N., & Obaid, M. A. M. (2018). Factors for minimizing cyber harassment among university students: Case study in the Kingdom of Saudi Arabia (KSA). *Journal of Theoretical and Applied Information Technology, 96*(6), 1592–1603.

17. Moafa, F., Ahmad, K., Al-Rahmi, W. M., Yahaya, N., Kamin, Y. B., & Alamri, M. M. (2018). Developing a model to measure the ethical effects of students' social media use. *IEEE Access, 6*, 56685–56699. https://doi.org/10.1109/ACCESS.2018.2873497

18. Moafa, F., Ahmad, K., Al-Rahmi, W. M., Yahaya, N., Kamin, Y. B., & Alamri, M. M. (2018). Cyber harassment prevention through user behavior analysis online in the Kingdom of Saudi Arabia (KSA). *Journal of Theoretical and Applied Information Technology, 96*(6), 1604–1615.

19. Moafa, F., Kamsuriah, A., Yahaya, N., Kamin, Y. B., & Alamri, M. (2018). Integrated system to minimize cyber harassment in the Kingdom of Saudi Arabia (KSA). *International Journal of Engineering & Technology, 7*(4.29), 2192–2196. https://doi.org/10.14419/ijet.v7i4.29.27602

20. Mukred, A. A. O., Mokhtar, U. A., Moafa, F. A., & Saud, A. M. (2024). The roots of digital aggression: Exploring cyber-violence through a systematic literature review. *International Journal of Information Management Data Insights, 4*(2), Article 100178. https://doi.org/10.1016/j.jjimei.2024.100178

21. Nicholson, P. (2022). Countering GPS spoofing in small UAS. *Air & Space Power Journal, 36*(3), 44–59. https://www.airuniversity.af.edu/ASPJ/Display/Article/3174560/counteringgps-spoofing-

Received: August 12, 2025, Published: December 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
in-small-uas/ (Related resource: https://pmc.ncbi.nlm.nih.gov/articles/PMC9739461/)

22. Park, J. (2022). Digital transformation of military justice systems. *Military Law Review, 230*(2), 189–223. https://tjaglcs.army.mil/mlr (Primary resource: https://tjaglcs.army.mil/Portals/0/Publications/Military%20Law%20Review/2022%20%28Vol%20230%29/Issue%201/MLR%20230-1.pdf?ver=mLZ_O3xuxVMkUFPDEErZ_w==)
23. Schmitt, M. N., & Watts, S. (2024). Cyber operations and autonomous weapons under IHL. *International Law Studies, 100*, 412–456. https://digitalcommons.usnwc.edu/ils/vol100/iss1/16/ (Related resource: https://internationalreview.icrc.org/sites/default/files/irrc-893-schmitt.pdf)
24. Stafford, V. (2023). Zero trust in DoD: Progress and roadblocks. *RAND Corporation*. RRA1234-1. https://www.rand.org/pubs/research_reports/RR-A1234-1.html (Primary resource: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf)
25. Stafford, V. (2025). Zero trust adoption metrics 2021–2025. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RR-AXXXX-1.html (Related resource: https://expertinsights.com/zero-trust/zero-trust-adoption-statistics-and-trends)
26. Thompson, R., & Alvarez, M. (2024). Ransomware and military due process. *Harvard National Security Journal, 15*, 278–312. https://journals.law.harvard.edu/nsj/vol-15/ (Related resource: https://pmc.ncbi.nlm.nih.gov/articles/PMC8463105/)
27. U.S. Cyber Command. (2024). *Annual threat assessment (unclassified summary)*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf
28. U.S. Department of Defense. (2023). *Unmanned systems integrated roadmap 2023–2048*. https://apps.dtic.mil/sti/pdfs/ADA606909.pdf (Related resource: https://digital.library.unt.edu/ark:/67531/metadc1982990/)

Received: August 12, 2025, Published: December 10, 2025