Cybersecurity Risk in Unmanned Aircraft Systems (UASs): Strategic Cybersecurity Threats of Unmanned Aerial Systems

Mohammed Almuthaybiri and Diane Murphy
Marymount University, Department of IT, USA

mma84343@marymount.edu (corresponding author)
dmurphy@marymount.edu

Abstract: Unmanned Aerial Systems (UASs) have emerged as critical components across various sectors, including military, commercial, and civilian applications. However, their increasing prevalence has raised significant cybersecurity concerns. This paper explores the strategic cybersecurity threats associated with UASs, focusing on vulnerabilities inherent in their architecture, communication protocols, and operational frameworks. identifying key risk areas such as data interception, command-and-control (C2) breaches, and adversarial attacks on autonomous decision-making systems by analyzing recent incidents and emerging threat vectors. Additionally, examine the implications of these threats on national security, privacy, and infrastructure integrity. The paper advocates for a multifaceted approach to UAS cybersecurity, emphasizing the need for robust regulatory frameworks, enhanced encryption methods, and continuous threat assessment strategies. By addressing these cybersecurity challenges, stakeholders can better safeguard the operational integrity of UASs, thereby improving their utility and reliability in an increasingly complex digital landscape.

Keywords: Cybersecurity risk, AI, Unmanned aircraft systems, Workforce, Strategic threats, Warfare, UAVs

1. Introduction

Air superiority has played a significant role in victory in wars and conflicts since the early 20th century. Controlling skies allows forces access for reconnaissance, surveillance, swift logistics deployment, and defending ground and maritime forces. However, until five years ago, only wealthy nation-states could use aircraft to conduct power against the enemy. UAS development is a significant technological advance for recreational and commercial uses. Nowadays, unmanned aircraft are used across the United States to support firefighting and search-and-rescue operations, monitor and assess critical infrastructure, provide disaster relief by transporting emergency medical supplies to remote locations, and aid border security. However, UAS can also be used by terrorists, criminal organizations (including transnational organizations), and lone actors. This underscores the need for legal scrutiny of UASs usage, invoking a sense of responsibility and accountability. Non-state organizations like the Islamic State and Hezbollah used low-cost and commercially available materials to wreak havoc on defense forces to achieve their objectives. Today, some terrorist groups like the Iran-backed Houthis possess the capability to fly UAVs at long distances and project power into Saudi Arabian territory w. This new technology gives rebellion a tool not available in past insurgencies. This research paper aims to determine Strategic cybersecurity threats and impacts of unmanned aircraft systems economically and geopolitically. (Hutchinson, 2021). In recent years, unmanned aerial systems (UAS) have been widely used in military and civilian fields. However, their open-source software and protocols have made their security vulnerable, resulting in many cybersecurity issues. While unmanned aircraft systems (UAS) are considered aircraft, they are also information and communication technology systems (ICTS) devices that receive and transmit data. Each connection point is a potential target for malicious actors to compromise sensitive information.

This paper explores the security implications of the rapid growth in UAS technology, focusing specifically on Strategic cybersecurity threats economically and geopolitically. According to one estimate conducted in 2021, sales of piloted or autonomous drones exceed $12 billion. The rapid growth in UAS technology underscores the urgency of addressing the associated cybersecurity threats. (Best et al., 2020). Armed drones, whether deployed by State or non-state actors, can nowadays strike deep into national territory, targeting individuals and public infrastructure. While some "incidents," such as the UAVs strike in January 2020 against Iranian Major General Qasem Soleimani or that against Saudi Arabian oil facilities, generate solid political reactions, most targeted killings by UASs are subjected to little public scrutiny at both the national and international levels. The ICAO defines unmanned aircraft as an aircraft intended to operate with no pilot on board. and the unmanned aircraft system as an aircraft with all associated elements being operated without a pilot onboard. So, the UAS, under the international regime of air law, is considered an aircraft. (International Civil Aviation Organization, 2011).

From a cybersecurity perspective, the adversaries may use UAS or already used as a (mobile platform) to interrupt or modify digital services or conduct unauthorized access to data systems. The dangerous capabilities of UAS continue to grow with longer flight times, greater ranges, and increased payload capacities. Unmanned Aerial Systems (UASs) can be considered cybersecurity threats. Due to several factors in their design, usage, and

potential vulnerabilities. Such as vulnerabilities in communication links, data interceptions, and breaches built with weak or outdated software security measures. This could make them easy targets for hackers who could exploit the Autonomy and AI Risk, which refers to the potential dangers that arise from the autonomous behavior of UAS and the use of AI in cyber-attacks. In one of the reports, the Federal Aviation Administration (FAA) forecasted that in the United States, by 2023, there will be a growth of 300% in the number of registered UAS.

2. Background and Literature Review

Background As a digital forensic officer in the Kingdom of Saudi Arabia and dealing with terrorist attacks and drones, before the Ukraine War, the Kingdom of Saudi Arabia was the most prominent country that received attacks by drones and missiles. Abqaiq is the world's largest oil processing plant. Since 2015, the Houthis began directing their military efforts at Saudi targets using stockpiles of ballistic missiles and drones acquired by Yemen before the crisis. They seized from Yemeni military stockpiles by the Houthis during the 2014 –15 coup d'état. During the attack on the Saudi Aramco facility in Abqaiq, Russia's nuclear doctrine approved changes to "Under the changes, a large attack on Russia with conventional missiles, UASs, or aircraft could meet the criteria for a nuclear response, as could an attack on Belarus or any critical threat to Russia's sovereignty. Moscow would see any aggression against Russia by a state member of a coalition as aggression from the whole group. According to the state-run news agency Tass, the updates expand the number of countries and coalitions and the kinds of military threats subject to a possible nuclear response". (Davies, 2024).

UASs are playing a pivotal role in reshaping the cybersecurity world in two keyways. Firstly, UASs are emerging as a significant and potentially devastating cybersecurity target. Cyberattacks on these platforms could undermine critical law enforcement or data collection missions using UAS. Secondly, UAS, in the hands of adversaries, could present novel avenues for cyberattacks, with UAS themselves serving as 'cyber weapons' intended to deliver malicious content or kinetic impacts. A serious concern is the potential for UAS swarms carrying explosives in significant numbers to attack U.S. symbols of political power and disrupt interdependent systems, like critical elements of the U.S. electric power grid (Best et al., 2020). Non-state actors' use of weaponized UAVs is a recent phenomenon that has mainly taken place since 2016 and almost exclusively only occurs in the Middle East. Immediate action is needed to address this issue. The U.S. government's ability to identify, track, and mitigate weaponized or dangerous UASs in the skies hinges on the urgency of policy changes. Specifically, DHS lacks the authority and equipment to effectively deal with UAS threats that are local to DHS assets. Regardless of the form future legislation takes, it will be crucial to enhance DHS's actions and capabilities when combating a UAS threat while respecting citizens' privacy and freedom of the press to portray public opinions that can oppose DHS authority. It underscores the critical need for technical innovation in the form of limited resources.

Utilizing the UASs, cyber attackers can wirelessly exploit points of access, unsecured networks, or other devices. By doing so, the malicious actors may execute malicious code, inject malware, perform a man-in-the-middle attack, and much more. It is also possible that a UAV can be hacked by using another UAV, which can be possible by using a Wi-Fi network. For example, in 2014, researchers from Sense point security firm developed an application installed on a UAV. Through an open Wi-Fi network, a flying drone with that application could steal users' data, like usernames, passwords, and credit card details, from connected devices (Geoff & Steuter, 2017, p. 43). Compromising FEMA UAS could significantly hamper the agency's ability to identify, reach, or supply individuals in peril or medical distress in disaster zones. This could occur if the compromised UAS asset is rendered inoperable or used to disrupt other aerial operations, such as helicopter flights or other UAS activities. The compromised FEMA UAS could also reduce situational awareness if UAS are used for ISR in disaster zones. Furthermore, Compromised CISA UAS would impair CISA's ability to conduct critical infrastructure inspections in some cases and could be used in a cyber-physical attack to damage the critical infrastructure it was meant to survey. (Best et al., 2020).

The White House's 2023 National Cybersecurity Strategy and the Annual Threat Assessment from the Office of the Director of National Intelligence both identify the PRC as the most advanced, active, and persistent cyber threat to the United States. Their analysis details how the PRC has expanded its cyber operations to challenge global order and US interests. At the core of this strategy is the acquisition and collection of data, which the PRC views as a strategic resource and a growing arena of geopolitical competition. Since 2015, the PRC has enacted or updated comprehensive national security, cybersecurity, and data privacy laws and regulations, extending their oversight of domestic and foreign companies operating within China. One such law, the PRC's 2017 National Intelligence Law, mandates Chinese companies to collaborate with state intelligence services, including

granting access to data collected in China and worldwide. (Federal Bureau of Investigation, 2024). China and Russia were frequently mentioned across events, focusing on China's use of AI. China's engagement in intellectual property espionage has significantly advanced its technological military capabilities, with this "asymmetric threat" subjecting the US to the "death of a thousand cuts" when the world" was used "to subvert and control" targets (CyCon). Emerging threats, such as the use of swarm UAVs and drones as weapons by rebel groups, have raised concerns within the US DoD, underscoring the potential danger of these technologies (Ertan, 2022).

3. Analysis

The swarms have become a demoralizing fact of life for Ukrainians. Even the decoys can be helpful to Russia. One decoy with a live-feed camera allows the aircraft to geolocate Ukraine's air defenses and relay the information to Russia in the final moments of its mechanical life. Decoy drones using thermobaric bombs. (Los Angeles Times, 2024).

Law enforcement establishments and offices could become targets of a UASs-led botnet or data exfiltration attack. Offices and components have physical locations with sensitive data and wireless networks; they might be potential targets for these attacks. Awareness of these risks and implementing effective mitigation strategies is crucial. Moreover, the ubiquity of connected devices grows, and the danger of a UAV-injected worm or similar attack, personal devices, or home networks could also be accessing points for nefarious code to gain entry to citizens, law enforcement members, and executive people or people with sensitive responsibilities.

An adversary can also use UAS in various malicious ways, including the following:

- Hostile Surveillance. An adversary uses UAS to collect information about federal government operations, security measures, or law enforcement operations.
- Smuggling or Contraband Delivery. An adversary uses UAS to bypass security measures to deliver illegal or prohibited items onto federal property.
- Disruption of Government Business. An adversary uses UAS to interfere with federal government operations through the presence of the UAS, use of on-board cyber-capabilities, or by using the UAS to distribute propaganda onto federal property.
- Implementing a Zero Trust (ZT) framework for the UAS fleet is crucial for Weaponization. An adversary mounts a firearm, explosive, chemical, or biological agent on a UAV or deliberately crashes the UAV into an attack. (CISA, 2020) cybersecurity kill chain identifies a cyberattack's seven stages (reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions). The same security vulnerabilities are used to target UAS directly, and UASs are also used as the last step in the kill chain of cybersecurity attacks. It refers to such attacks as 'UASs as vectors.' The utility of the 'UAS as target' versus 'UAS as vector' distinction underscores the need for a comprehensive defense strategy, as different attack types are associated with varying defense postures.

The professor at Marymount University and co-author, Dr. Diane Murphy, outlined the different communication systems of UAVs or commercial aircraft. Each system poses cybersecurity risks for unauthorized users to remotely obtain information or gain control of the plane with malicious intent or mislead the communication.

The individuals responsible for the attack often document their methodology on websites such as YouTube or personal blogs. Indeed, in many cases, the code used in the exploit is posted to searchable code repositories such as GitHub. Nor are these exploits limited to early-generation or low-end UAS. Documented exploits have targeted the DJI Phantom 4, valued at $1,500; the DJI Inspire, valued between $2,000 and $3,000; and the Yuneec Tornado, valued at $3,000.3 Similarly, high-grade controllers such as the FrSky ACCST and the DJI Naza-M controller have been successfully exploited. One IT security consultant even hijacked a professional-grade Aerialtronics Altura Zenith UAV, valued between $25,000 and $35,000, used in law enforcement (Best et al., 2020).

All uncrewed aircraft, whether piloted remotely, fully autonomous, or even those using a combination of both, are subject to the Convention on International Civil Aviation (the Chicago Convention). Article 8 of the Chicago Conventions articulates that "no aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of a contracting State without special authorization by that State and under the terms of such authorization. Each contracting State undertakes to ensure that the flight of such aircraft without a pilot in regions open to civil aircraft shall be so controlled as to obviate danger to civil aircraft" (ICAO, 2011).

Figure 1: UAS Vulnerability Assessment Process- (U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency)

UASs, in the hands of adversaries, could present novel avenues for cyberattacks, with UAS themselves serving as "cyber weapons" intended to deliver malicious content or kinetic impacts. UASs swarms carrying explosives in significant numbers can attack U.S. symbols of political power and, through cascading effects take down interdependent systems, like critical elements of the U.S. electric power grid.

- foreign-manufactured UAS: UAS manufactured by foreign adversaries may contain vulnerabilities that allow government and intelligence officials access to sensitive information.
- Software and Hardware vulnerabilities: Certain software and firmware used in UAS operations may pose data privacy risks, resulting in stolen data or unauthorized control of the UAS.
- Peripheral devices: The transfer of data between UAS and connected devices, such as controllers, smartphones, and docking stations, allows for vulnerabilities that may be exploited.

An article in the Harvard Business Review claims that blockchain is 'decades from reaching its full potential' due to the relative novelty and complexity of the technology. However, blockchain has the potential to revolutionize UAS cybersecurity. It can provide a secure and transparent platform for UAS operations, reducing the risk of data breaches and unauthorized access. A study published in October 2017 surveyed supply chain and logistics professionals and found that just 20 percent had implemented any 'blockchain solutions.' According to the professionals surveyed, the primary barriers to the broader use of blockchain included regulatory uncertainty, the need for different parties to agree to and utilize a standard system, and technological maturity. Data security was also a significant concern. It needs to be determined what effect blockchain will have on the cybersecurity of commercially available UAS. However, it is a technology and trend that warrants further scrutiny in the next several decades. Cyberspace has become, as defined in the U.S. National Strategy to Secure Cyberspace- the "nervous system of the state." Our economy and national security depend entirely on technology and IT infrastructure. The functioning of the critical infrastructure depends on the efficiency and security of Cyberspace". (The White House, 2003). UASs are connected to computers and networks, store data, and transmit information. Due to critical information being part of that flow, the UASs are a desirable target for malicious actors. Today, UASs are also constantly growing in use on the battlefield. However, their popularity also increases the risk of destructive cyber-attacks affecting complex networks and systems. Experts indicate that UAS has become more common, accessible, and valuable due to new possibilities, such as increased data collection capabilities and autonomous operations. In this way, UAS can be both a target of a cyber-attack and an effective weapon. New developments in UAS technology, including the introduction of more autonomous control software and the ability to create a swarm of UASs via mobile networks, increase the scope and advancement of potential cyber-attacks.

In Europe, with the amendment of the so-called Basic Regulation (EU) 216/2008, the new Regulation (EU) 2018/1139, for the very first time, directly referred with its provisions to cybersecurity and established that the coordinating role to collaborate with the industry stakeholders on cybersecurity issues will belong to EASA. Based on this, the EASA established two rulemaking proceedings to implement new provisions on cybersecurity. The first one, the Aircraft Cybersecurity (RMT.0648), intends to address cybersecurity provisions through different certification specifications to mitigate cyber threats impacting safety. (EASA, 2019)

3.1 Economic Implications

Globally, the term "critical infrastructure" encompasses the lifelines of modern society, such as water, energy, food processing, and critical manufacturing. However, every industrial facility, regardless of its scale, deserves to know that its processes are secure and safe. With the increasing threats of new technologies and evolving workforce demands, the role of security managers in operational technology (OT) is more crucial than before. It

must have the necessary techniques and materials to defend its facilities and teams, especially against UAS threats.

The global impact of UAS attacks was starkly demonstrated on 14 September 2019, when drones flown alongside cruise missiles hit oil processing facilities at Abqaiq and Khurais in eastern Saudi Arabia. These facilities, which provide 6 percent of the world's oil supply, were targeted. The Houthi movement in Yemen claimed responsibility, while some States deemed the Islamic Republic of Iran responsible. The drones were possibly UAV-Xs powered by German and Chinese engines, as found by the United Nations panel that inspected them (UN et al., 2020). The economic implications of UAS attacks on the Red Sea are far-reaching due to the region's significance in global maritime trade. The Red Sea serves as a crucial conduit for transporting goods between Europe and Asia. The Suez Canal and the Bab el-Mandeb Strait are essential maritime chokepoints. UAS attacks have led to a notable increase in shipping costs, as many shipping companies have chosen to reroute their vessels around the Cape of Good Hope. This detour significantly lengthens voyages, adding up to 12 days to typical journeys, which results in higher fuel consumption, increased crew wages, and elevated vessel chartering costs.

Consequently, shipping costs have risen by as much as 30%, placing a substantial financial burden on the global logistics industry. Additionally, due to the direct costs, the threat of UAS attacks has driven up insurance premiums for maritime operations in the region. War risk premiums have skyrocketed from 0.6% to 2% of the cargo value, reflecting the heightened danger and potential for significant losses. These increased insurance costs further strain shipping companies' financial resources and increase shipping expenses. The disruptions in the flow of maritime traffic also have broader implications for the global supply chain, causing delays and interruptions that can affect the timely delivery of goods worldwide. (Dras, 2024).

The economic impact of UAS attacks extends beyond the shipping industry, as the increased costs and delays can contribute to global inflationary pressures. The higher transportation costs are often passed on to consumers, resulting in elevated prices for goods and services. However, the role in mitigating these impacts is crucial. The UAS attacks have had a humanitarian impact by impeding the flow of essential aid into the region, including food, fuel, and medicine. This exacerbates existing humanitarian crises and leads to further economic and social instability. influence in this area can make a significant difference. Lastly, the environmental impact of longer shipping routes, resulting in increased carbon emissions, adds another layer of complexity to the economic implications of UAS attacks in the Red Sea. For Europe-Asia voyages, a diversion to the Cape of Good Hope increases shipping time by 30 to 50 percent. This has immediate economic impacts and creates medium-term logistics issues for individual shipping firms (CSIS, 2024).

3.2 Geopolitical Implications

Two weeks ago, Russia's nuclear doctrine approved changes to "Under the changes, a large attack on Russia with conventional missiles, UASs, or aircraft could meet the criteria for a nuclear response, as could an attack on Belarus or any critical threat to Russia's sovereignty. Moscow would see any aggression against Russia by a state member of a coalition as aggression from the whole group. According to state-run news agency Tass, the updates expand the number of countries and coalitions and the kinds of military threats subject to a possible nuclear response”. Anonymous claimed to have hacked Russia's unmanned aerial vehicle (UAV) plans in mid-June. (Canadian Centre for Cyber Security, 2022).

In the big-picture questions, many academics regarded UASs as a threat to international security that promotes instability and increases uncertainty in regional balances of power. UASs strike could thus potentially transform global order, argued Senn and Troy and Lushenko et al. A growing security studies literature also drew attention to increasing autonomy in weapon systems enhanced by artificial intelligence, pointing to algorithmic bias, flaws in training data, and receding human control.

The objectives do not have direct military significance (as, for example, in an armed conflict, cyber-attacks on the enemy's command and communication systems) but belong to the category of the state's critical infrastructure. Such attacks may cause threats to international security (global information security), destabilization of critical infrastructure, disruptions in the functioning of public administration, economic losses (inhibition of the development of companies and enterprises), or even personal losses of citizens. The scale of the attack and the losses are essential. Saudi Arabia is an example.

The security concerns related to drones and their dependency on GPS must be addressed. GPS is used for drone navigation, and no encryption is in place, so it is an easy target for attackers. Losing control of drones by a GPS spoofing attack may result in massive harm. For example, it was claimed that in December 2011, Iranian forces

took control over a Lockheed Martin RQ-170 Sentinel drone, which belonged to the United States Air Force. The explanation for taking control of a drone was a potential GPS spoofing attack. (Joo & Tan, 2018).

The EW systems spoof GPS satellite navigation signals. The fake signals can help hijack a UASs, steering it toward an unintended location or even causing it to crash. Spoofing can also affect civilian mobile devices, unintentionally tricking them into displaying incorrect locations or times. This interference can impact map applications or other navigation tools, steering users into wrong turns or confusing situations. (The Record, 2023).

On 19 July 2024, a Houthi UAVs flew for some 16 hours from Yemen over more than 2,600 kilometers to reach Tel Aviv, where it killed one Israeli citizen and injured at least eight others. This incident marked the first time a Houthi UAVs breached Israeli air defenses, let alone caused casualties on Israeli soil. Despite their relative newness to UASs technology, the Houthis have been pioneering UASs warfare. They established large-scale drone production around 2018, leveraging Iranian technology transfers. This attack underscores the growing threat of drones in modern warfare. (Flourish Studio, n.d.).

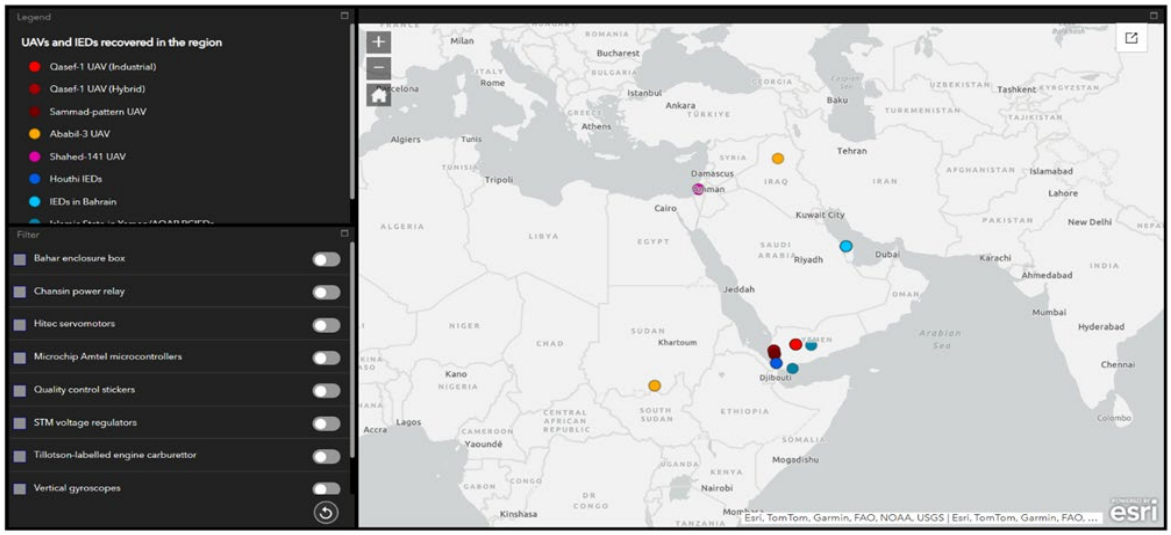

Figure 2: According to the interactive StoryMaps (active UASs cyberspace threat)

In early June 2023, Ukraine launched a counteroffensive to retake lost territory and split Russian forces, requiring the enemy to fight on multiple fronts. After Ukrainian troops made an initial thrust into Donetsk, Russian troops moved into their well-prepared defenses and successfully halted the Ukrainian advance. Since then, the war has devolved into a fight resembling World War I trench warfare rather than the quick victory the Russians expected. This shift in tactics has significant implications for international security, as it suggests that modern warfare is not immune to historical patterns. Much like WWI, both sides continue to conduct reconnaissance, counter-reconnaissance, and artillery strikes. (U.S. Army Training and Doctrine Command, 2024).

4. Discussion and Future Research

Looking ahead to 2025, it's crucial to recognize that Russian cyber operations in Ukraine and beyond are not a one-time event. These activities, including cyber espionage, cyber-attacks, and information operations, are expected to persist. Beyond Ukraine, Russian cyber espionage will likely continue to serve Moscow's global interests. This ongoing threat demands sustained attention and proactive measures. (Google Cloud, 2024). And so long as it remains active, the Israel-Hamas conflict will likely continue to dominate Iranian state-sponsored cyber threat activity, fueling cyber espionage, disruptive and destructive attacks, and information operations. However, this focus will not prevent Iranian threat actors from continuing operations consistent with long-term patterns, targeting government and telecommunications organizations across the Middle East and North Africa or dabbling in cybercrime.

However, the industry is not sitting idle. Several companies have already developed anti-drone equipment to take down UAVs or render them uncontrollable through jamming. Manufacturers have been aware of jamming for many years, and many have developed measures in place in case the control data link is jammed or lost. For example, the DJI Phantom 4 has an on-board computer with a "Failsafe" feature that will cause the drone to

either hover in place, return to a pre-determined home location, or automatically land in the case of a lost connection that may be the result of jamming. (Tang, n.d.).

Policymakers, concerned departments, cybersecurity experts, and other government and law enforcement agencies must consider the importance of their roles and move toward a coherent UAS cyber strategy. This paper will take inventory of categorized UAS platforms, understand the possible consequences, identify mitigation options for UAS-related cyberattacks, and stay abreast of new technological developments that could change the threat space. Focusing on Collaboration among all these stakeholders is crucial for robust UAS security. This step ensures industry safety and security protocol compliance and promotes interagency coordination. To understand mitigation options, DHS must monitor technological development in counter-UAS (cUAS) systems and experiment with emerging attack techniques and technologies. (Best et al., 2020).

Blockchain technology may become widespread in the UAS world, ensuring certain communications are encrypted and increasing the amount of data available to would-be attackers to track developments in UAS technology. This might make the challenges more difficult. Moreover, Experts indicate that the first step to protect against cyber-attacks against UAS should be to create a map of threatened areas and an effective risk-neutralization plan. It is also necessary to establish cooperation with cybersecurity specialists who have the appropriate.

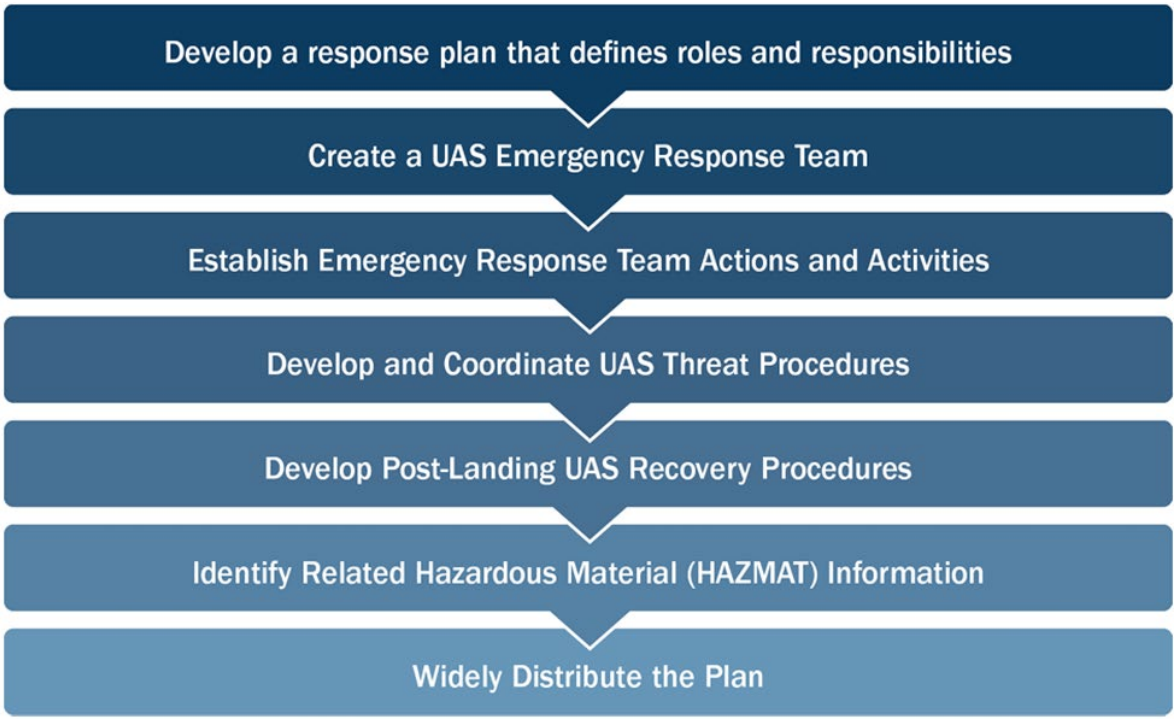

Figure 3: Developing a UAS Incident Response Plan. (U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency)

Experience and knowledge are needed to improve the quality of security. At the state level, the priority is to tighten the relationship between state administration entities and law enforcement agencies to create a common cyber strategy dedicated to UAS. Investing in regular equipment testing in cross-sectoral cooperation (state, private companies, laboratories, research centers) is equally essential, as it enables the creation of universal security and protection protocols that could be implemented on a larger scale. (Pyzynski & Balcerzak, 2021).

Establishing a trusted dialogue (possibly through different working groups or forums) among the UAS manufacturers, operators as well as regulators, or other relevant organizations to know how ensuring the confidentiality, integrity, and availability of systems and data are protected, which will create proper lines of communication between different stakeholders and ensuring there is a suitable level of regulations and standards and recommended practices, complemented by the guidance material, for the UAS that addresses cybersecurity issues at international, regional, and national levels; Establishing proper mechanisms for the information sharing between appropriate stakeholders, define the type of information that should be shared

(e.g., vulnerabilities, cyber threats, lessons learned from previous attacks). Moreover, developing appropriate education, training programs, and tabletop exercises to address cybersecurity challenges such as:

- Read software user agreements and privacy policies to understand where the data is transferred, stored, and potentially shared.
- It is essential to maintain a secure connection with the UASs during flights by using a virtual private network (VPN) or Wi-Fi encryption method.
- un all files through an antivirus program.
- Ensure that UAS devices involved do not access the enterprise network directly.
- Isolating or segmenting networks prevents potential malware or breaches from spreading to the enterprise network.
- Delete collected data from the UAS, including imagery, Global Positioning System (GPS) history, and flight telemetry data after data has been transferred and stored. An internet connection often allows for cloud connectivity as a means of data connectivity and storage.
- Remove and secure portable storage, such as secure digital (SD) cards, from the UAS before storage to prevent unauthorized access.
- Set a pre-determined 'Return to Home' location to minimize GPS-related risks and ensure proper UAS recovery. (CISA, Be air aware).
- Ensure that the devices that download and install UAS software and firmware do not access the manufacturing company's network.
- Properly verify and securely conduct all interactions with UAS vendors and third-party websites. By Taking extra precautions to download software from adequately authenticated and secured websites.

Finally, Zero Trust (ZT) architecture ensures that all network access and transactions across the UAS devices are continuously verified and authenticated, minimizing unauthorized access and shrinking the overall attack surface. (state, private companies, laboratories, research centers) is equally essential, as it enables the creation of universal security and protection protocols that could be implemented on a larger scale. (Pyzynski & Balcerzak, 2021).

5. Conclusion

The emerging enhancements in technology and functionality of the UAS, as well as the constantly growing number of interconnected systems and devices, bring many challenges in terms of cybersecurity. This process allows malicious actors to exploit vulnerabilities and conduct successful cyber-attacks. It should also be noted that different motivations and ways stand behind them. Since the UAS under the international air law regime is considered an aircraft, some provisions of the aviation cybersecurity framework should also apply to the UAS. However, there is already some maturity within the aviation cybersecurity framework, and there is an urgent need for provisions that apply directly to the UAS. This paper explains the rapid development of the UAS industry and emerging threats related to its development.

Moreover, an analysis of potential cyber threats with examples was conducted. The paper addressed the maturity level of the civil aviation cybersecurity framework and followed this with several suggestions that should be considered further.

Today, there is a unique opportunity for the cybersecurity world to create an intricate and secure system for a service that will revolutionize modern transportation. This system will be resilient to jamming, spoofing, DOS attacks, MITM, and other cyber-attacks. Multiple inter-validating navigation systems, symmetric encryption for combined video transmission, secondary control, and navigation data link, and Blockchain-based PKI for key management, will power it.

In the near future warfare, it will be challenging to differentiate between a state UASs strike and a swarm from a terrorist UAVs strike. And swarm as states deliberately Attempt to muddy the waters and create deniability by supplying identical systems to nonstate actors in future UASs wars, the landscape will become very complex. and congested.

Preemptive measures or preemptive war (in military language) must be taken against these security vulnerabilities, which appear to cybersecurity and strategic studies specialists to be vulnerabilities ready for use by criminals and criminal organizations at any time and fully available, especially considering the development of international tensions and the spread of radical organizations. UASs will continue to evolve; shortly, they will dominate numerous commercial and public sector areas and businesses, such as deliveries, crop and livestock

monitoring, border control, defense, surveillance, mapping, and security services. As such, it is not just important, but vital to secure them correctly To obtain the benefits of their use and to prevent them from becoming adversarial weapons in the hands of opportunistic state cyber threat actors.

References

Australian Army Research Centre. (2024). *Drones in modern warfare: Lessons learnt from the war in Ukraine*. Available at: https://researchcentre.army.gov.au/sites/default/files/241022-Occasional-Paper-29-Lessons-Learnt-from-Ukraine_2.pdf [Accessed 31 Jun. 2024].

Best, K. L., Schmid, J., Tierney, S., Awan, J., Beyene, N. M., Holliday, M. A., Khan, R. and Lee, K. (2020). *How to analyze the cyber threat from drones*. RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RR2972.html [Accessed 12 March. 2024].

Burrows, E., Arhirova, H. and Hinnant, L. (2024). 'Operation False Target: How Russia plotted to mix a deadly new weapon among decoy drones in Ukraine'. *Los Angeles Times*, 17 November. Available at: https://www.latimes.com/world-nation/story/2024-11-17/operation-false-target-how-russia-plotted-to-mix-a-deadly-new-weapon-among-decoy-drones-in-ukraine [Accessed 25 May. 2024].

Canadian Centre for Cyber Security. (2022). *Cyber threat activity associated with the Russian invasion of Ukraine (CCCS-2022-01)*. Available at: https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf [Accessed 31 Jul. 2024].

Center for Strategic and International Studies. (2024). *The global economic consequences of attacks on Red Sea shipping lanes*. Available at: https://www.csis.org/analysis/global-economic-consequences-attacks-red-sea-shipping-lanes [Accessed 14 Aug. 2024].

Cybersecurity and Infrastructure Security Agency. (2019). *Be air aware: UAS cybersecurity*. Available at: https://www.cisa.gov/topics/physical-security/be-air-aware/uas-cybersecurity [Accessed 1 Sep. 2024].

Cybersecurity and Infrastructure Security Agency. (2020). *Protecting against the threat of unmanned aircraft systems (UAS)*. Department of Homeland Security, November. Available at: https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf [Accessed 11 Sep. 2024].

Cybersecurity and Infrastructure Security Agency. (2019). *Cybersecurity best practices for operating commercial UASs*. Available at: https://www.cisa.gov/sites/default/files/publications/CISA%20Cybersecurity%20Best%20Practices%20for%20Operating%20Commerical%20UAS%20%28508%29.pdf [Accessed 31 Oct. 2024].

Davies, M. (2024). 'Putin approves changes to Russia's nuclear doctrine'. *BBC News*, 19 November. Available at: https://www.bbc.com [Accessed 11 Sep. 2024].

Dras. (2024). *The Red Sea crisis and impact on maritime economy*. 26 November. Available at: https://dras.in/the-red-sea-crisis-and-impact-on-maritime-economy/ [Accessed 31 Sep. 2024].

Esri. (n.d.). *iTrace [Web map]*. Available at: https://itrace.maps.arcgis.com/apps/webappviewer/index.html?id=a4b79c9758484a619f98c06f122bd62b [Accessed 17 Oct. 2024].

Ertan, A. (2022). *Exploring the security implications of artificial intelligence in military contexts* (Doctoral dissertation). Royal Holloway, University of London. Available at: https://pure.royalholloway.ac.uk/ws/portalfiles/portal/46513266/2022ErtanAPhD.pdf [Accessed 04 Sep. 2024].

European Union Aviation Safety Agency. (2019). *Easy access rules for unmanned aircraft systems*. Available at: https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulations-eu [Accessed 31 Von. 2024].

Federal Bureau of Investigation. (2024). *Cybersecurity guidance: Chinese-manufactured UAS*. Internet Crime Complaint Center, 17 January. Available at: https://www.ic3.gov/CSA/2024/240118.pdf [Accessed 18 Nov. 2024].

Flourish Studio. (n.d.). *Maps*. Available at: https://flourish.studio/visualisations/maps/?utm_source=showcase&utm_campaign=visualisation/18836347 [Accessed 26 Jun. 2024].

Google Cloud. (2024). *Cybersecurity forecast 2025*. 28 November. Available at: https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025/ [Accessed 15 Dec. 2024].

Hutchinson, A. M. (2021). *The effects of colonization and apartheid on the development of South Africa: Namibian influence, impacts on education, and state capture*. Johns Hopkins University.

Iansiti, M. and Lakhani, K. R. (2017). 'The truth about blockchain'. *Harvard Business Review*. Available at: https://hbr.org/2017/01/the-truth-about-blockchain [Accessed 20 Aug. 2024].

International Civil Aviation Organization. (2011). *Unmanned aircraft systems (UAS)*. Available at: https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf [Accessed 22 Aug. 2024].

Joint Air Power Competence Centre. (2021). *Future threats: Military UAS, terrorist drones, and the dangers of the second drone age*. January. Available at: https://www.japcc.org/chapters/c-uas-future-threats-military-uas-terrorist-drones-and-the-dangers-of-the-second-drone-age/ [Accessed 31 Oct. 2024].

Joo, Y.-M. and Tan, T.-B. (2018). 'Smart cities: A new age of digital insecurity'. *Survival*, 60(2).

M. Geoff and E. Steuter. (2017). *Drone Nation: The Political Economy of America's New Way of War*. p. 43.

Pyzynski, M. and Balcerzak, T. (2021). 'Cybersecurity of the unmanned aircraft system (UAS)'. *Journal of Intelligent & Robotic Systems*, 102, p. 35. Available at: https://link.springer.com/content/pdf/10.1007/s10846-021-01399-x.pdf [Accessed 17 Sep. 2024].

SANS Institute. (2024). *Industrial control systems cybersecurity awareness training*. Available at: https://www.sans.org/cyber-security-courses/industrial-control-systems-cybersecurity-awareness/ [Accessed 28 Sep. 2024].

Tang, A. C. B. (n.d.). *A review on cybersecurity vulnerabilities for urban air mobility*. National Aeronautics and Space Administration.

The Record. (2023). 'Ukraine's anti-drone GPS spoofing affects civilian mobile phones'. 1 December. Available at: https://therecord.media/ukraine-anti-drone-gps-spoofing-affects-civilian-mobile-phones [Accessed 24 Dec. 2024].

The White House. (2003). *The national strategy to secure cyberspace*. Available at: https://www.cisa.gov/sites/default/files/publications/national-strategy-to-secure-cyberspace-february-2003_0.pdf [Accessed 15 Dec. 2024].

U.S. Army Training and Doctrine Command. (2024). *Ukrainian unmanned aerial system tactics*. 8 October. Available at: https://oe.tradoc.army.mil/2024/10/08/ukrainian-unmanned-aerial-system-tactics/ [Accessed 16 Sep. 2024].

U.S. Department of State. (2024). *United States international cyberspace and digital policy strategy*. 16 February. Available at: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/ [Accessed 31 Nov. 2024].

United Nations Human Rights Council. (2020). *Use of armed drones for targeted killings (A/HRC/44/38)*. United Nations.