Deloitte.

Together makes progress

Cyber Threats to Unmanned Aerial Vehicles

April 2026

Contents

Introduction

Unmanned Aerial Vehicles (UAVs) have evolved from specialized military reconnaissance platforms into ubiquitous commercial assets transforming agriculture, infrastructure inspection, emergency response, and logistics operations. As UAV adoption accelerates across critical sectors, these systems have become integral to modern business processes.

The integration of artificial intelligence (AI) has fundamentally amplified UAV functionality, enabling autonomous navigation, real-time computer vision analysis, swarm coordination, and edge-based decision-making that operates independent of cloud connectivity. However, this technological convergence has simultaneously expanded the attack surface, exposing UAVs to sophisticated cyber threats including global positioning system (GPS) spoofing, radio frequency (RF) jamming, supply chain compromise, and targeted exploitation by nation-state actors, cybercriminals, and hacktivist groups with diverse strategic and economic motivations.

Unmanned aerial vehicles

The cybersecurity implications of AI-enabled UAV systems extend beyond traditional information technology concerns to encompass operational integrity, physical safety, and geopolitical stability. Further, as UAVs increasingly perform mission-critical functions—from precision agriculture, where it has contributed to a 40% reduction in pesticide application,[1] to emergency response systems locating earthquake survivors—organizations should implement comprehensive security frameworks that protect confidentiality, integrity, and availability while maintaining the low-latency, real-time processing requirements essential to autonomous operations.

This analysis explores some commercial and military applications of AI-enhanced UAVs, catalogs emerging threat vectors and adversary tactics, and proposes security architectures leveraging containerization, Zero Trust principles, hardware roots of trust, and edge computing to safeguard these transformative yet vulnerable systems.

Commercial use cases

UAVs have rapidly expanded across commercial sectors, transforming operations in agriculture, infrastructure, logistics, and emergency services.

Agriculture: Agriculture and precision farming represents one of the largest commercial applications for UAVs. Airborne UAVs equipped with multispectral cameras enable precision agriculture by monitoring crop health, detecting irrigation issues, and identifying pest infestations. A study published in Precision Agriculture found that UAV-based crop monitoring could improve yield predictions by up to 85% compared to traditional ground-based methods.[2] Major agricultural companies have integrated drone technology into their farm management systems, allowing farmers to make data-driven decisions about fertilization, irrigation, and harvest timing.

Infrastructure management: UAVs are also heavily utilized for infrastructure inspection and maintenance, as they have revolutionized infrastructure inspection across energy, telecommunications, and transportation sectors. The Federal Aviation Administration (FAA) reports that infrastructure inspection accounts for nearly 36% of commercial drone operations in the United States. Utility companies use drones to inspect power lines, wind turbines, and solar installations, reducing inspection time from weeks to days while eliminating safety risks to human inspectors.[3]

Emergency services: Emergency services also increasingly rely on UAVs.[4] They have had a growing and increasingly essential role in disaster assessment, search and rescue operations, and firefighting support. During the 2023 Maui wildfires, drones provided real-time thermal imaging that helped firefighters identify hotspots and plan containment strategies, as reported by CNN.[5]

AI presents numerous benefits, albeit current drawbacks of hallucinations and errors alongside emerging questions about accountability in the event of errors or even disasters resulting from AI miscalculations. To take a commercial use case example of deploying AI to manage airports or even air traffic control someday: "AI-powered drones, in particular, shift the traditional liability model—where a human pilot or operator was clearly accountable—to a more complex ecosystem involving AI agents, software developers, and airport managers. Legal doctrines remain ill-equipped to handle such distributed responsibility."[6]

Law enforcement use cases

Law enforcement use cases: Local and federal law enforcement agencies deploy UAVs for aerial surveillance during large public events to monitor for and protect against threats and enhance crowd control management. UAVs are used heavily in search and rescue missions during natural disasters to quickly cover hard to reach terrain and locate missing persons with thermal imaging technology. Traffic accidents and construction zones are captured real time by UAVs leading to more safety and control of our roadways. UAVs and drones are also becoming increasingly invaluable for monitoring armed subjects and high threat scenarios as well as documenting crime scenes, providing real time feedback while maximizing on officer safety.[7]

Threat vectors

Supply chain attacks against hardware and software

From 2022 to August 2024, APT group Earth Ammit conducted multi-stage attacks disrupting Taiwanese and South Korean drone supply chains.[8] First, vulnerabilities on upstream enterprise resource planning (ERP) software providers' web servers were exploited using open-source tools in the VENOM attack to deploy web shells that run open-source remote access tools to persistently steal credentials. These credentials were then used in the TIDRONE attack to sign and distribute malware collecting and compromising UAV control software through the trusted ERP update channel. This campaign highlights the importance of assessing partner software vendors and adopting trustless architectures.

The targets of such attacks extended beyond East Asian countries in 2025. Lazarus Group used fake job postings for defense roles at European UAV firms for social engineering tactics8. Victims downloaded infected PDF "job descriptions" that installed remote access trojans (RATs), allowing attackers to steal proprietary UAV designs, manufacturing data, and intelligence on drones used in conflicts. While primarily direct targeting, this enabled potential supply chain ripple effects by compromising employee systems to access production pipelines.

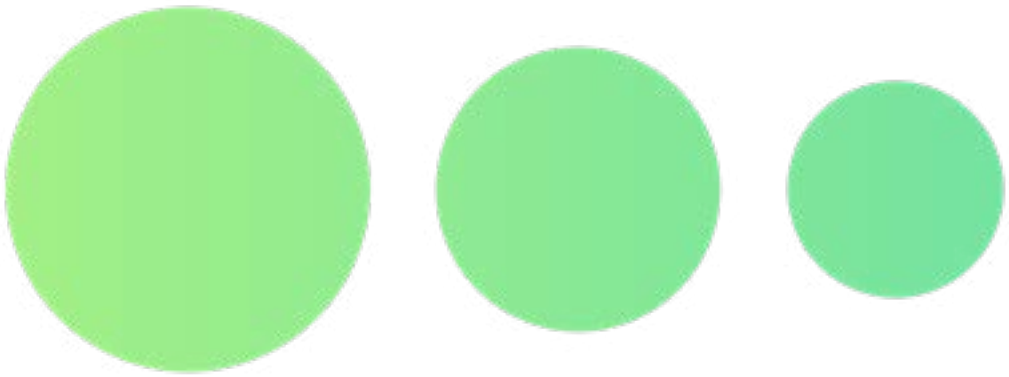
Various ongoing attacks to supply chains were documented in 2025,[9] when third-party hardware chips or firmware updates were tampered with during development, which may have included injecting malware into UAV flight controllers. For instance, vulnerabilities in commercial drone firmware (e.g., Wi-Fi modules) have been exploited to introduce backdoors, as seen in analyses of popular models where supply chain-sourced software libraries enabled unauthorized control.[10] These echo broader risks like the 2011 US drone supply chain theft vulnerabilities, where physical stages (storage) were robbed for components.

Threat vectors for both hardware and software supply chains, including potential impacts and mitigations, are summarized in Table 1.

CATEGORY	THREAT VECTOR	DESCRIPTION	IMPACT	POTENTIAL MITIGATION
Hardware	Compromised electronics	Malicious modifications to processors, sensors, or communication modules during manufacturing or delivery, inserting hardware backdoors.	Remote hijacking leads to operational failures (to the extent of explosions) or data leakage (tracking) during flight.	Trusted foundry sourcing and end-to-end supply chain audits,[11] secure packaging and logistical tracking.[12]
Software	Third-Party injection	Compromised open-source libraries (such as the infamous liblzma backdoor[13] integrated into a UAV's operating system (OS), introducing vulnerabilities and malware.	Flight path manipulation and mission corruption.	Code signing and dependency scanning.
	Firmware update exploitation	Unsecure over-the-air (OTA) updates hijacked to deploy malicious code altering control algorithms.	Unauthorized access or AI model poisoning in autonomous UAVs.[14]	Encrypted updates and integrity checks.[15]
Hybrid	Vendor compromise	Breaching suppliers to propagate attacks downstream such as the ERP backdoors affecting UAV assembly lines.	Widespread fleet compromises across organizations.	Zero Trust vendor assessments.[16]

Table 1: Summary of hardware and software supply chain threat vectors.

These vectors are amplified by UAV reliance on commercial off-the-shelf (COTS) components, geopolitical tensions (e.g., restrictions on suppliers and exports to[17] certain nations), and the integration of AI in drone autonomy, which we explore further in the next subsection. For more guidance on mitigations, resources like OWASP's Drone Security Cheat Sheet[18] outline endpoint-specific defenses.



Foreign manufactured components

Post-pandemic, the attention of UAV cybersecurity shifted from software risks to sheer cyber-physical availability in supply chains.[19] Certain countries control 80–95% of critical UAV components (neodymium magnets, brushless motors, Li-ion cells, carbon fiber, flight-controller chips).[20] Most international supply chains cannot currently replace volume at cost, creating dependence on these select countries.[21] The threat vectors associated with deliberate export halts and embargoes have already been executed since 2024 on graphite, gallium, and lithium cells.[22] Domestic unmanned aircraft system (UAS) manufacturers advise against import bans and tariffs that domestic material/component manufacturers cannot readily scale as it would hinder their growth.[23] However, independent of domestic UAS manufacturer views, components they were promised to import such as battery cells get diverted to the opposition as their manufacturers are also foreign.[24] Domestic UAS system integrators further suffer from opaque sub-tier sourcing (only 17% were able to affirm foundries of their chips).[25,26]

Absent immediate stockpiling and allied co-production, conflicts lasting >90 days could potentially collapse national UAV production and sustainment. Current "Blue UAS" exemptions for imported motors/ batteries could conceivably contribute to a single-point-of-failure UAV functionality risk. The UAV industrial base can overlap with critical infrastructure and elicit funding magnet/motor lines during conflicts (24–36 months to a meaningful scale).

GPS jamming/spoofing and radiofrequency attacks

UAVs are dependent on Global Navigation Satellite Systems (GNSS) for Position, Navigation, and Timing (PNT) data. The command and control (C2) data link manages remote piloting and telemetry transmission.GPS spoofing is transmitting false GPS signals to a drone receiver, which manipulates the drone's perceived PNT data. This is feasible because the civilian GPS is unencrypted and unauthenticated. GPS attacks can be executed using low-cost hardware like Software Defined Radios (SDR). The impact of such attacks can result in hijacking of drones, causing them to deviate from their path, crash, or enter no-fly zones. RF interference/jamming, on the other hand, is the intentional transmission of powerful radio signals on the same frequency as GPS or a drone's C2 link to overload the drone's receiver with noise and blocking the legitimate signals. This causes loss of communication and control, often triggering the drone's failsafe protocols and can lead to erratic flight behavior or crash.[27]

2018, Hong Kong, Hong Kong Drone Light Show, GPS Jamming/Interference (confirmed):

More than 40 drones performing in a professionally organized light show fell from the sky after the GPS signal was jammed.[28]

2024, Korea, GPS Jamming/Spoofing (confirmed):

North Korean GPS jamming caused an ROK S-100 drone crash into the Yellow Sea.[29]

Peripheral devices and controllers

Threat vector groups for UAV peripheral systems

UAV cybersecurity threats targeting peripheral systems fall into four dominant categories. First, control interface attacks exploit vulnerabilities in ground control stations (GCS), remote controllers, and mobile apps. Second, sensor and navigation deception is on the rise. Lastly, firmware and payload compromise remains a powerful vector. In 2021, researchers discovered CVE-2021-34125, a vulnerability in the PX4 autopilot used by the Yuneec Mantis.[30]

Q, which allowed adversaries to extract firmware and sensitive data directly via an exposed command shell, bypassing memory protection on embedded flight systems.[31]

GROUP	DESCRIPTION
Control interface attacks	Exploits targeting ground control stations (GCS), remotes, and apps via hijacking, spoofing, or malware.
Communication link intrusions	Attacks on RF, Wi-Fi, or satellite channels through jamming, interception, or command injection.
Sensor and navigation deception	GPS spoofing, visual adversarial inputs, or light detection and ranging (LiDAR) blinding that affects navigation and autonomy.
Firmware and payload compromise	Malicious code or hardware trojans in onboard systems and connected payloads.

Table 2: Summary of threat vector groups for UAV peripheral systems.

Cross-cutting observations and trends

The recent incidents reflect broader systemic trends shaping UAV cybersecurity. Protocol-level vulnerabilities remain prevalent. For instance, the open source DSMx protocol used in hobbyist drones has been reverse-engineered and hijacked via brute-force key guessing. The convergence of UAVs with consumer electronics continues to erode baseline security. AI-driven autonomy is introducing new vulnerabilities, as demonstrated by academic adversarial attacks against drone vision systems that misclassify visual input, an area expected to grow as more UAVs adopt AI models.[32,33] Another trend is the operational insecurity of ground systems as the UAV-ground communication and app-based control surfaces remain soft targets.[34,35] This is particularly dangerous as off-the-shelf components become pervasive in both commercial and military UAVs.[36] Lastly, electronic warfare in modern conflicts has validated the threat of spoofing and signal deception as strategic tools, with 430,000 reported GPS interference incidents in high-risk zones as of 2024.[37] These patterns suggest UAV security must contend with both opportunistic exploitation and deliberate state-level adversaries acting across the full spectrum of a UAV's peripheral ecosystem.

TREND	INSIGHT
Communication protocol exploits	Repeated vulnerabilities in common telemetry/control protocols (e.g., MAVLink, DSMx).
Attack surface expansion via autonomy	Increased AI and autonomy introduce novel machine learning (ML)-based manipulation and spoofing risks.
Low-security ground systems	GCS and mobile apps are frequent weak links despite hardened airborne platforms.
Third-party risk amplification	Supply chain, software development kits (SDKs), and cloud integrations introduce non-obvious entry points.

Table 3: Summary of threat vector groups for cross-cutting observations and trends.

Threat actors and incidents targeting UAVs

General motivations

Both civilian and military UAVs are attractive targets for threat actors. When any type of threat actor gains unauthorized access to a UAV, they can access and collect sensitive information and prevent the victim organization from accessing this information. This reconnaissance can also enable future attacks, such as physically disruptive attacks on critical infrastructure. Nation state-sponsored APTs are comparatively more likely to target military UAVs to conduct strategic reconnaissance and hijack military supply chain components. Meanwhile, all types of threat actors can harbor economic motivations while targeting military or civilian UAVs, aiming to steal intellectual property (IP), undermine economic competitiveness, engage in economic sabotage, or conduct further cyber reconnaissance.[38] Cybercriminal motivations are primarily for personal financial gain, whereas hacktivist motivations generally align with those of nation-state APTs in their broadly anti-Western victimology.

Nation state-sponsored threat actors

Turla (Secret Blizzard) and Storm-1837:

A pair of related Russian threat actors has shared malware tools to gain access to Ukrainian surveillance drone data. Turla is one of the most advanced Russian state-sponsored threat actors, which include its own advanced toolset, including zero-day exploits. However, its recent involvement with cyberattacks against UAVs stems from its ability to piggyback off other threat actors' infrastructure. In a campaign observed in December 2024, Turla used two custom malware tools (the Tavidig and KazuarV2 backdoors) developed by another Russian APT, Storm1837, that facilitate the deployment of espionage malware that targets Ukrainian surveillance UAVs.[39] With these tools, Turla simultaneously conducts espionage and counterespionage against Ukrainian drones while masking operations and obfuscating attribution.[40] The image below shows each state of the Russian operation against Ukrainian surveillance drones align with those of nation-state APTs in their broadly anti-Western victimology.

Attack chain

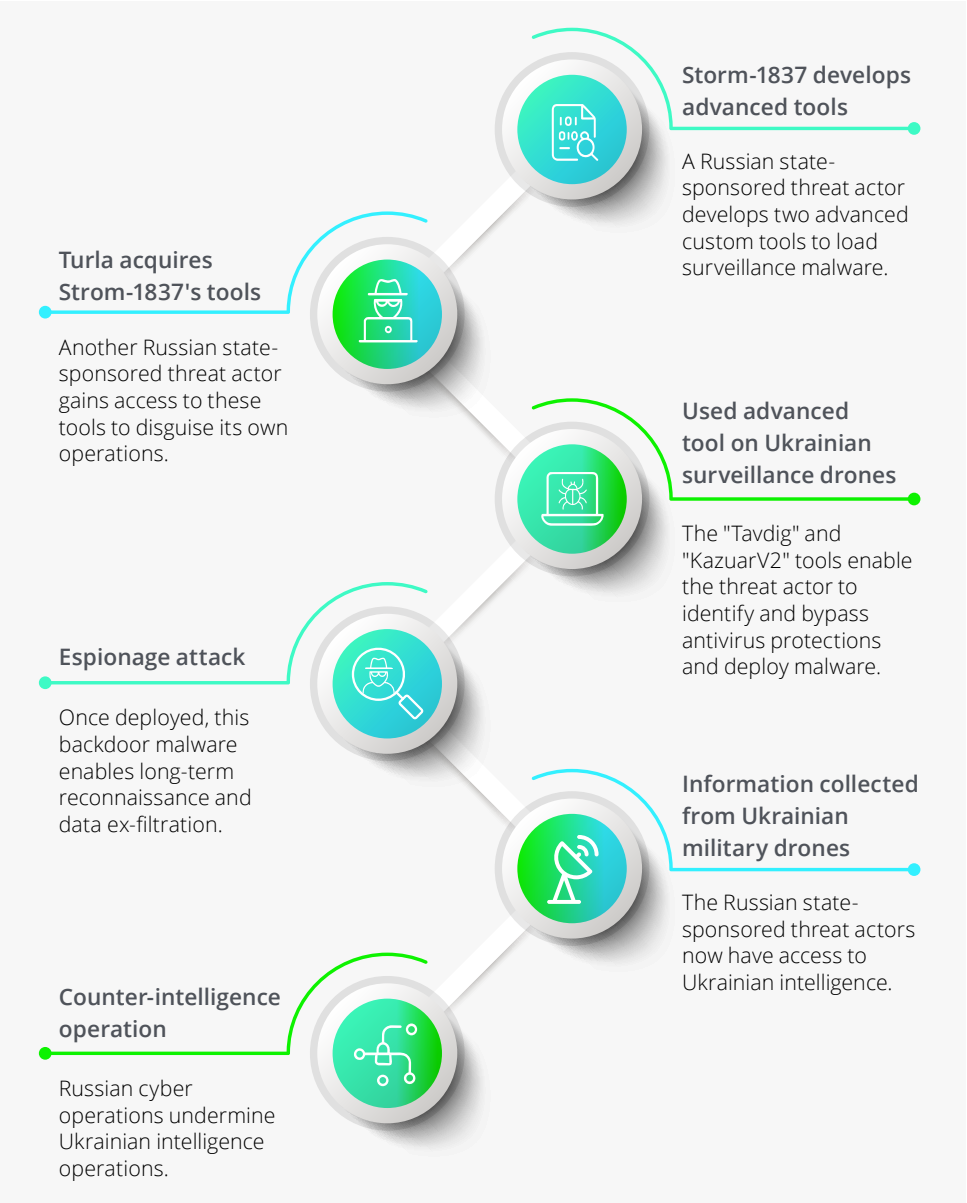


Figure 2: Turla and Storm-1837 attack chain targeting Ukrainian surveillance drones.[41,42]

UNC4895 (CIGAR, RomCom):

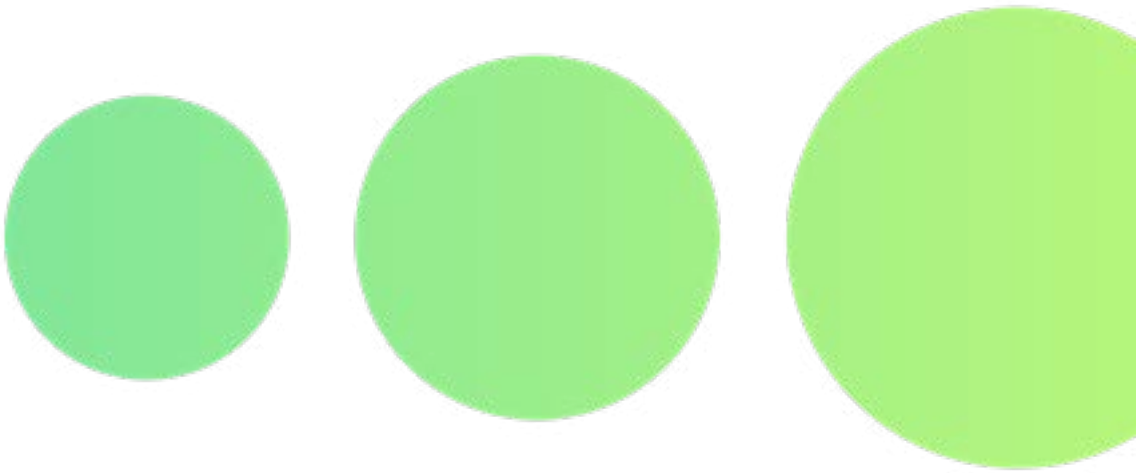
UNC4895 falls into a category of Russian-aligned threat actors that has plausible nation-state or advanced hacktivist connections. UNC4895 is a dual espionage and financially-motivated threat actor that has operated on behalf of Russian geopolitical interests. It has exploited multiple zero-day vulnerabilities to deploy RomCom malware, enabling espionage attacks against Ukraine's DELTA battlefield management and surveillance system.[43] The DELTA system features UAVs, sensor networks, and satellite imagery to assist Ukraine's defensive intelligence, and has been a target of other Russian-aligned hacktivist groups.[44]

Earth Ammit:

Geopolitical conflicts and economic tensions in the South China Sea have led to a high interest in disrupting UAV supply chains. Downstream, UAV manufacturing disruptions have both economic and national security implications. Earth Ammit is an East Asian state-sponsored threat actor that was observed conducting two campaigns in 2024 that targeted a neighboring government and civilian critical infrastructure. The two campaigns, dubbed "VENOM" and "TIDRONE," targeted a broad range of industries via software supply chains.[43] The TIDRONE campaign was most notable for targeting military surveillance infrastructure including drone manufacturers and the UAV software supply chain. In these attacks, Earth Ammit conducted espionage via malicious code injection and privilege escalation while disabling defenses.[44] The threat actor's motivations align with enhancing the East Asian country's economic and military capabilities.

Lazarus Group:

Lazarus Group and its subgroups are North Korean aligned threat actors. Unlike other nation-state APTs, North Korean-aligned threat actors typically conduct financially-driven operations with espionage as secondary. However, recent Lazarus Group campaigns have targeted individuals with access to sensitive government and defense information. Lazarus Group's "Operation Dream Job" is a set of threat campaigns in which the threat actor uses phishing lures—often with the use of Generative AI—described as fake job openings for defense engineers to espionage malware. In this campaign observed in October 2025, Lazarus Group conducted social engineering that prompted victims to sign up for an interview for a fake job offer, after which a malicious file would deploy the ScoringMathTea RAT. This malware was aimed at employees of defense organizations with potential access to drone secrets.[45]



Cybercriminals & hacktivists

Prana Network:

The Prana hacking network is a global hacktivist group of unknown origin that has targeted Asian government organizations. Its Telegram activity overlaps with the hacktivist collectives GhostSec and Anonymous.[46] In February 2024, Prana Network conducted a hack-and-leak operation that revealed stolen data from a nation state-aligned Sahara Thunder UAV production company. The data revealed that the company had been selling military UAV technology to a Russian facility.[47]

Sylhet Gang:

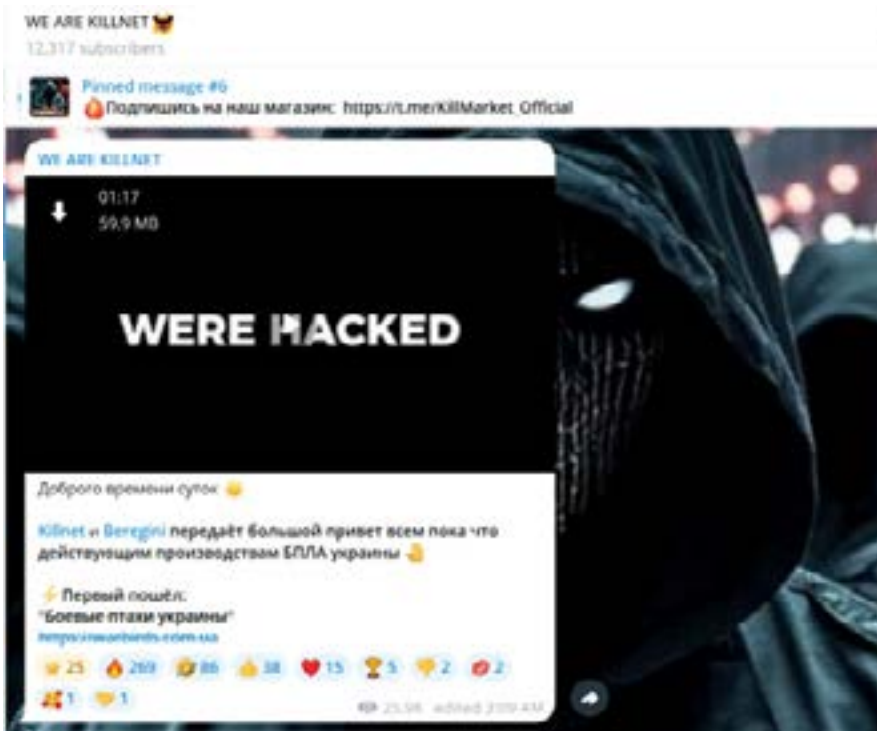
Sylhet Gang is a hacktivist group that aligns with regional political and religious movements. Its country of origin is unknown. The group claimed responsibility for a distributed denial-of-service (DDoS) attack in 2024 against a manufacturer of military UAVs in Asia. Sylhet Gang also advertises data leak capabilities and large-scale DDoS against critical infrastructure, and ransomware, threatening a cyberattack against US organizations.[48]

NoName057(16):

NoName057(16) is a pro-Russian threat actor. Its hacktivist operations mostly support pro-Russian and anti-Ukrainian interests, although sometimes veer into more broadly anti-Western or anti-NATO political interests. Since 2023, NoName has operated the DDoSia project, a collaboration of pro-Russian and Russian-speaking DDoS actors on affiliated Telegram channels. NoName targets the aviation industry as a whole, with early 2024 operations targeting UK-based UAV manufacturers.[49]

Palach Pro and KillNet:

Both Palach Pro and KillNet are pro-Russian hacktivist groups, with DDoS and hack-and-leak capabilities. Palach Pro claimed to have developed an AI-based tool that could detect hidden activity in satellite images, while KillNet claimed to have used this tool to discover a launch point of Ukrainian UAVs in the Crimea region. The hacktivist groups, though officially unaligned with a nation-state.[50] In the images below, KillNet claims responsibility for breaching Ukraine's DELTA drone surveillance program and makes additional claims about Ukrainian drone operations.



Figures 3-4: KillNet claims responsibility to UAV production breach.

Impacts

Operational impacts (remote hijacking, service disruptions)

Cyber threats to UAVs primarily manifest as remote hijacking and service disruptions, exploiting vulnerabilities in communication links and navigation systems. Up to 75% of all drones used by both sides in the Ukrainian theater were downed by jamming.[51] Firmware backdoors in commercial models enable persistent access, leading to 48-hour average downtime per breach and operational halts in sectors like agriculture and logistics.[52]

Safety and privacy (physical harm and espionage)

Government and defense studies warn that hacked drones pose severe safety and privacy threats. A compromised UAS can be weaponized or crash into populated areas55 creating hazards for public safety and critical infrastructure,[56] or used for intelligence collection against critical infrastructure networks.[57] Insider misuse amplifies these risks, as poor access controls or intentional sabotage.

Financial impacts

UAS cyber incidents impose direct costs from asset loss and indirect burdens via data breaches, operational disruptions, and regulatory penalties. Compromised drones can expose sensitive operational data[53] triggering breach response costs that align with global averages exceeding $4.45 million per incident.[54] Additionally, owners of hacked UAVs may face potential fines under aviation and privacy regulations under civil negligence liability of failing to secure the UAS,[55] as well as reputational damage that can erode long-term revenue streams.

The growing role of AI in UAVs

AI has become fundamental to modern UAV operations, transforming drones from remotely piloted aircraft into autonomous systems capable of complex decision-making. The integration of AI enables drones to navigate dynamically, analyze data in real-time, and operate in coordinated swarms, expanding their utility across military, commercial, and humanitarian applications.

AI-powered computer vision systems allow UAVs to navigate complex environments without human intervention. ML algorithms process sensor data from cameras, LiDAR, and radar to detect and avoid obstacles in real-time. According to research published in IEEE Transactions on Robotics, deep learning-based navigation systems have achieved 95% success rates in avoiding dynamic obstacles in urban environments.[58] Commercial AI-driven drones that use visual simultaneous localization and mapping (VSLAM) to navigate autonomously through forests, buildings, and other challenging terrain.[59]

In addition, AI enables UAVs to identify and classify objects with unprecedented accuracy. Convolutional neural networks (CNNs) process aerial imagery to detect specific targets—from counting wildlife populations to identifying infrastructure defects. A study in Remote Sensing demonstrated that AI-enhanced drones achieved 92% accuracy in detecting individual trees and assessing forest health, outperforming traditional satellite imagery analysis.[60]

Furthermore, edge AI computing allows drones to process and analyze data onboard rather than transmitting raw footage to ground stations. This capability is critical for time-sensitive applications. Nature Communications published research showing that AI-equipped agricultural drones can identify crop diseases with 89% accuracy and recommends targeted treatments in real-time, reducing pesticide use by up to 40%.[61] During the 2023 Turkey-Syria earthquake, AI-powered drones analyzed thermal imaging to locate survivors trapped in rubble, prioritizing rescue efforts based on probability assessments.[62]

Secure and resilient architectures for drone operations

Protecting confidentiality, integrity, and availability when traditional security controls result in latency

UAVs require real-time AI processing at the edge for tasks like obstacle detection and decision-making, but traditional cybersecurity creates latency that undermines autonomous capabilities. To protect the confidentiality, integrity, and availability (CIA) of UAV systems and data—especially as they're used for critical business processes—security solutions need to go beyond standard cloud approaches and operate where the data is generated. Edge computing enables sensitive data to stay on-site, minimizing exposure risks during transmission and proving more reliable than cloud-based security in remote or disconnected environments.[63] Securing UAV operations means using layered defenses like security-by-design through containerized applications, Zero Trust frameworks, supply chain verification, and strong encryption, all of which help isolate core processes, enforce strict access and validate authenticity, protecting data from sophisticated cyber threats.

Isolation of processes: Containerization to decentralize workloads and minimize the attack surface

Containerization, which is a software deployment process,[64] using Kubernetes clusters, allows drone operators to securely deploy and rapidly update applications, helping to isolate different drone functions (route planning, package tracking system, inventory management agent, customer notifications) and allow modular updates for quick patching of vulnerabilities without disrupting missions.[65] Containerization supports the protection of CIA through:

- Isolation of applications and processes, limiting blast radius if one is compromised. Even if one application or process is attacked, the attacker is confined within strict boundaries, and rapid recovery is possible.
- Consistent, immutable runtime environments that prevent tampering and make it easy to patch vulnerabilities.
- Minimized attack surface, where each container includes only the essential components.

Zero Trust architecture (ZTA)

ZTA is built on the principles of never trust, always verify, using identity as the core of access decisions and continuously validating users, devices, and context before granting the least-privilege access possible. ZTA combines strong identity and access management (IAM), multi-factor authentication (MFA), device posture checks, endpoint and extended detection and response (EDR/XDR) telemetry, and Zero Trust network access (ZTNA) to provide application-level access rather than broad network access, while microsegmentation and tools like next-generation firewalls (NGFW) enforce granular east-west and north-south traffic controls aligned with Zero Trust policies. In this context, organizations use cloud-native security practices embedded in edge-enabled drone operations (e.g., implement cloud-native security tools, originally designed for cloud environments, directly at the edge, on each drone's onboard computer). The ecosystem of tools that make up ZTA is designed to enable ongoing verification, minimize implicit trust, and reduce lateral movement.

Establish a chain of trust throughout the supply chain

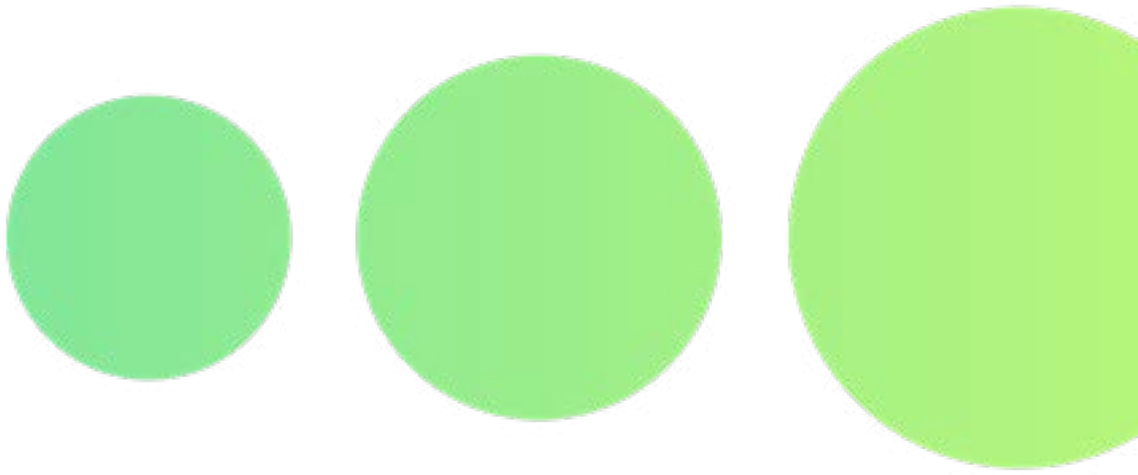
Hardware trust: Root of trust establishes the foundation for a trusted supply chain, providing assurance of a device's origin. Establishing trust within the supply chain starts with establishing root of trust in the devices produced by manufacturers, beginning with the physical architecture designs of the device itself, through shipment and deployment or implementation of the device onto a customer's network. This can be accomplished through Trusted Platform Model (TPM), offering a hardware-based foundation for security. By integrating these trusted hardware elements early in the manufacturing process, both manufacturers and device owners can confidently verify the identity and authenticity of each device throughout its entire lifecycle—helping to prevent tampering, counterfeiting, or unauthorized access within the supply chain.[66]

Secure boot and firmware (software trust): Platform Configuration Registers (PCRs) maintain an audit record of how the platform booted [80]. Essentially, PCR allows security teams to identify how the hardware booted and on what firmware, allowing security teams to understand if it was booted at a well-known and secure state, as prescribed by the root of trust of measurement (RTM) designed by the manufacturer. PCR strengthens software integrity by securely recording and verifying each stage of the system's software and firmware, helping to ensure that only approved, untampered code is executed and providing transparency throughout the device's lifecycle.[67]

Protections during runtime: For added runtime protection in the chain of trust, a Trusted Execution Environment (TEE) keeps sensitive workloads secure even in untrusted settings by isolating code and data from the OS, firmware, and threats, ensuring they stay protected throughout the device's lifecycle. TEEs only run authorized code, verified via signature checks, and safeguard critical operations even if the broader system is compromised.[68]

As it relates to protecting CIA, establishing chain of trust architecture within the supply chain supports:

- Hardware-based or cryptographic anchors (RTM) used to validate software and system integrity at every layer, from boot-up to runtime.
- Chain of trust mechanisms ensure each component (firmware, OS, application) is validated, providing strong protection and prevention against the execution of malware in the environment.
- Ensure only trusted, verified components run on your devices or infrastructure, stopping persistent or low-level (e.g., firmware/rootkit) attacks at the source.



Commercial use case example: Securing drone-operated e-commerce logistics

When e-commerce logistics services use drones for critical tasks, securing operations at the edge enables low-latency, real-time AI decision-making and requires strong protection for both data in transit and at rest. Leveraging the aforementioned security controls, alongside cloud-native protections (e.g., integrating NGFWs and enforcing strict policies at the edge) help prevent data breaches, secure devices, and block threats across networks and applications to help ensure drone operations stay efficient, resilient, and secure.

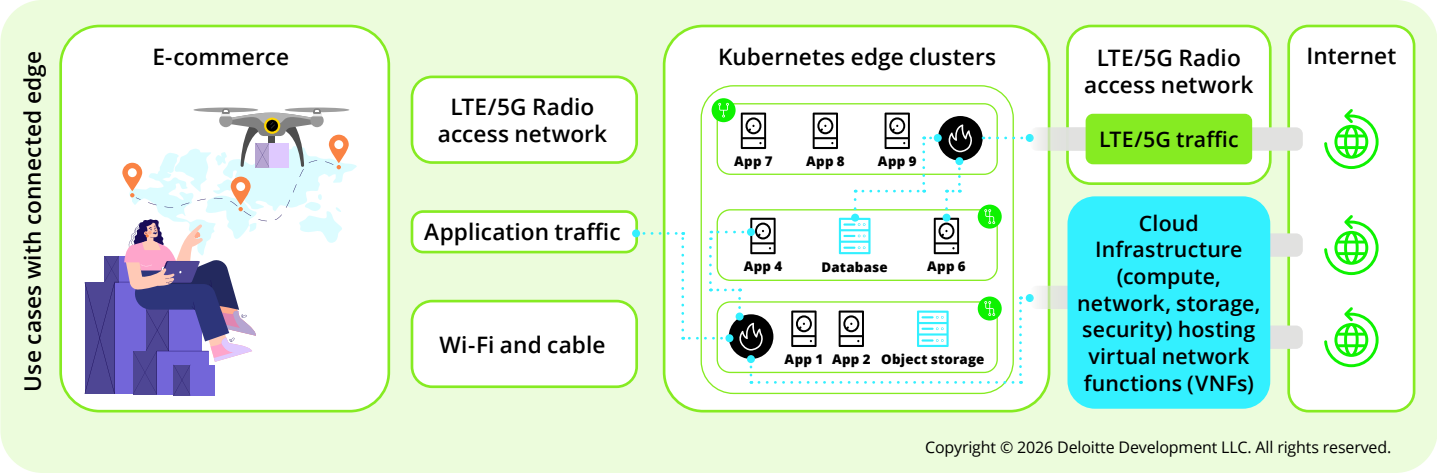


Figure 5: Modern edge infrastructure running Kubernetes clusters (containerization) with respective data pipelines or other connected services, the networking devices, and internet connections.

As we further explore, embracing distributed, immutable, and ephemeral (DIE) architecture will be key to bolstering security, enhancing scalability, and optimizing performance for next-generation business processes where trustless architecture can be better achieved.

Achieving trustless architecture for futuristic resilience

Achieving Trustless architecture – not to be confused with unsecured systems which are therefore untrustworthy – are systems that do not need to trust humans or institutions, can create a foundation for futuristic resilience.

This architecture, known as the DIE Triad, focuses on systems that are distributed, immutable, or ephemeral, ensuring data cannot be altered or persist only briefly. It incorporates security by design. Applying DIE to UAVs or drones means designing fleets, data flows, and control systems so they are resilient by construction: drones and ground/fog/ cloud elements form a distributed swarm using mesh links and consensus so no single controller or vehicle is critical; mission logs, command histories, firmware, and access policies are treated as immutable, recorded on append-only ledgers (often blockchain or directed acyclic graphs (DAG)-based) with signed updates and smart contracts for auditable data sharing; and sensitive assets such as identities, cryptographic keys, compute workloads, and in-memory state are made ephemeral, tied to missions or sessions and rotated or destroyed quickly so captured or compromised drones have minimal long-term value.

Conclusion

The proliferation of AI-enabled UAV systems represents a paradigm shift in commercial operations, delivering measurable operational efficiencies and strategic advantages across agriculture, infrastructure inspection, emergency response, logistics, and defense sectors. However, this technological advancement has fundamentally transformed the threat landscape, as demonstrated by documented campaigns from sophisticated nation-state adversaries and coordinated hacktivist operations. The convergence of autonomous navigation, edge computing, real-time computer vision, and swarm coordination capabilities has created complex attack surfaces that traditional cybersecurity approaches cannot adequately address.

Organizations deploying UAV systems for mission-critical operations need to recognize that securing these platforms requires fundamentally rethinking security architectures to accommodate the unique constraints of autonomous systems operating in contested environments with minimal latency tolerance. Effective protection of UAV operations demands a comprehensive security framework that integrates containerization for workload isolation, Zero Trust architecture for continuous authentication and authorization, hardware-based roots of trust for supply chain integrity, and edge computing capabilities that enable real-time threat detection without compromising operational performance.

As nation-state actors, cybercriminals, and hacktivists continue targeting UAV systems for espionage, economic sabotage, and strategic disruption, organizations must adopt security-by-design principles that embed protection mechanisms throughout the technology stackfrom manufacturing provenance verification through runtime execution monitoring. The strategic and economic value of UAV systems will continue escalating as AI capabilities mature. Ensuring these platforms remain secure, reliable, and trustworthy requires sustained investment in advanced security technologies, and threat intelligence sharing.

References

1 Li, Wen, et al. “A sustainable crop protection through integrated technologies: UAV-based detection, real-time pesticide mixing, and adaptive spraying,” Nature, 13 October 2025. [Online]. Available: https://www.nature. com/articles/s41598-025-19473-x. [Accessed 5 January 2026].

2 Zhang, C., & Kovacs, J. M, "The application of small unmanned aerial systems for precision agriculture." Precision Agriculture, 13 July 2012. [Online.] Available: https://link.springer.com/article/10.1007/s11119-012-9274-5. [Accessed 5 January 2026].

3 Federal Aviation Administration, “UAS by the Numbers,” 2023. Available: https://www.faa.gov/uas [Accessed: 05 December 2025.]

4 Moore, Richard. “Autonomous drones for infrastructure inspection,” SINTEF, 11 September 2023. [Online]. Available: https://adrforum.eu/sites/default/files/2023-11/2023-11-09%20-%2004_ADRF%20 Autonomous%20Drones%20for%20Infrastructure%20Inspection.pdf. [Accessed 5 January 2025].

5 Martinez, L. (2023). "Drone technology in wildfire response." CNN, August 2023. Available: https://www. cnn.com/2025/10/27/world/video/lifesparrow-ai-drone-hong-kong-tech-for-good-spc-hk [Accessed: 05 December 2025.]

6 Roy, David, et. al. "Multi-resolution monitoring of the 2023 Maui wildfires, implications and needs for satellite-based wildfire disaster monitoring," Science of Remote Sensing, Volume 10, December 2024. Available: https://www.sciencedirect.com/science/article/pii/S2666017224000269. [Accessed: 12 December 2025.]

7 Staff, “In Support of Small Unmanned Aircraft Systems in Law Enforcement,” International Association of Chiefs of Police, 1 November 2013. [Online]. Available: https://www.theiacp.org/resources/resolution/expired-in-support-of-small-unmanned-aircraft-systems-in-law-enforcement. [Accessed 5 January 2026].

8 Pierre Lee, Vickie Su, Philip Chen, “Earth Ammit Disrupts Drone Supply Chains Through Coordinated Multi-Wave Attacks in Taiwan,” TrendMicro, 13 March 2025. [Online]. Available: https://www.trendmicro.com/en_us/ research/25/e/earth-ammit.html. [Accessed: 15 December 2025].

9 Kálnai, Peter, et al, “Gotta fly: Lazarus targets the UAV sector,” ESET, 23 October 2025. [Online]. Available: https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/ [Accessed: 02 December 2025].

10 Ioannis Anagnostis, Panayiotis Kotzanikolaou, and Christos Douligeris, “Understanding and Securing the Risks of Uncrewed Aerial Vehicle Services,” 10 March 2025. [Online]. Available: https://ieeexplore.ieee.org/ document/10918966 [Accessed: 04 December 2025].

11 B. Sugg, S. Habicht, R. Dove, and A. Osantowske, “Securing UAS Fleets from Cyber Attacks Final Report,” 2024. Available: https://www.faa.gov/uas/programs_partnerships/BAA/BAA004-CNA-Securing-UAS-Fleets-from-Cyber-Attacks.pdf [Accessed: 04 December 2025].

12 “DMEA - Trusted Access Program Office,” www.acq.osd.mil. https://www.acq.osd.mil/asds/dmea/tapo/trusted-supplier-programs.html [Accessed: 04 December 2025].

13 “IT Security Procedural Guide: Drones/Unmanned Aircraft Systems (UAS) Security CIO-IT Security-20-104.” Available: https://www.gsa.gov/system/files/Drones-Unmanned-Aircraft-Systems-%28UAS%29-Security-%5BCIO-IT-Security-20-104-Rev-2%5D%2003-18-2025.pdf [Accessed: 04 December 2025].

14 “NVD - CVE-2024-3094,” 29 March 2024. https://nvd.nist.gov/vuln/detail/CVE-2024-3094 [Accessed: 04 December 2025].

15 “Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems,” Federal Register, Jan. 03, 2025. https://www.federalregister.gov/ documents/2025/01/03/2024-30209/securing-the-information-and-communications-technology-and-services-supply-chain-unmanned-aircraft [Accessed: 04 December 2025].

16 R. Voughn, “MEMORANDUM TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES FROM.” Accessed: Dec. 15, 2025. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2025/11/M-26-02-Ensuring-Government-Use-of-Secure-Unmanned-Aircraft-Systems-and-Supporting-United-States-Producers.pdf [Accessed: 05 December 2025].

References

17 CISA, "UAS Cybersecurity | CISA," Cybersecurity and Infrastructure Security Agency CISA, 2024. https://www. cisa.gov/topics/physical-security/be-air-aware/uas-cybersecurity [Accessed: 03 December 2025].

18 Suat Cubukcu, "The Houthi Drone Supply Chain - Orion Policy Institute," Orion Policy Institute, Jul. 26, 2025. https://orionpolicy.org/the-houthi-drone-supply-chain/ [Accessed: 03 December 2025].

19 "Drone Security - OWASP Cheat Sheet Series," Owasp.org, 2025. https://cheatsheetseries.owasp.org/cheatsheets/Drone_Security_Cheat_Sheet.html [Accessed: 03 December 2025].

20 B. Vincent, "Pentagon's growing list of 'made in America' drones has a loophole for certain parts made in China," DefenseScoop, Nov. 20, 2025. https://defensescoop.com/2025/11/20/dod-drones-blue-uas-list-chinese-parts-motors/ [Accessed: 03 December 2025].

21 M. Amoah, M. Bazilian, Jahara Matisek, and K. Schweiker, "The Drone Supply Chain War: Identifying the Chokepoints to Making a Drone," Csis.org, 2025. https://www.csis.org/analysis/drone-supply-chain-war-identifying-chokepoints-making-drone [Accessed: 03 December 2025].

22 P. Apps, "Conflict, drones, rare earths drive China supply chain dependence fears," Reuters, Nov. 28, 2025. Available: https://www.reuters.com/markets/commodities/conflict-drones-rare-earths-drive-china-supply-chain-dependence-fears-2025-11-28/ [Accessed: 13 December 2025].

23 "GAO-25-107283, DEFENSE INSUSTRIAL BASE: Actions Needed to Address Risks Posed by Dependence on Foreign Suppliers," Gao.gov, 2025. https://files.gao.gov/reports/GAO-25-107283/index.html [Accessed: 13 December 2025].

24 A. Boston et al., 2025. Accessed: Dec. 15, 2025. [Online]. Available: https://www.technet.org/wp-content/uploads/2025/08/TechNet-Comment-re-BIS-232-Investigation-Drones.pdf [Accessed: 13 December 2025].

25 R. Tollast, "Drones: Decoupling Supply Chains from China," 2025. Accessed: Dec. 15, 2025. [Online]. Available: https://static.rusi.org/rp-drone-supply-chains-china-nov-2025_0.pdf [Accessed: 13 December 2025].

26 "Public Report on the Use of Mature-Node Semiconductors." Accessed: Dec. 15, 2025. [Online]. Available: https://www.bis.gov/media/documents/public-report-use-mature-node-semiconductors-december-2024.pdf [Accessed: 13 December 2025].

27 I. GNSS, "Criminal Investigation Underway in GPS Jamming Incident That Crashed Drones, Caused HK$1M in Damage," Inside GNSS - Global Navigation Satellite Systems Engineering, Policy, and Design, Oct. 31, 2018. https://insidegnss.com/criminal-investigation-underway-in-gps-jamming-incident-that-crashed-drones-caused-hk1m-in-damage/ [Accessed: 10 December 2025].

28 jooheon kim, "North Korean GPS jamming caused an ROK drone crash last year: Lawmaker | NK News," NK News - North Korea News, Sep. 2025. https://www.nknews.org/2025/09/north-korean-gps-jamming-caused-an-rok-drone-crash-last-year-lawmaker/ [Accessed 15 December 2025].

29 "Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle," GPS World, Aug. 01, 2012. https://www.gpsworld.com/drone-hack/ [Accessed: 10 December 2025].

30 T. Turgeon, "GPS Jamming Report: June 2024," GNSS Jamming, Jul. 2024. https://www.gnssjamming.com/post/ gps-jamming-report-june-2024 [Accessed 15 December 2025].

31 "NVD - CVE-2021-34125," Nist.gov, 2021. https://nvd.nist.gov/vuln/detail/CVE-2021-34125 [Accessed 10 December 2025].

32 Abiodun Esther Omolara, Moatsum Alawida, and Oludare Isaac Abiodun, "Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey," Neural Computing and Applications, vol. 35, Aug. 2023, doi: https://doi.org/10.1007/s00521-023-08857-7. [Accessed 05 December 2025].

33 B. Branco, J. S. Silva, and M. Correia, "Cyber Attacks on Commercial Drones: A Review," IEEE Access, pp. 1–1, Jan. 2025, doi: https://doi.org/10.1109/access.2025.3527698. [Accessed 05 December 2025].

References

34 V. L. Stouffer et al., “Reliable, Secure, and Scalable Communications, Navigation, and Surveillance (CNS) Options for Urban Air Mobility (UAM),” Nasa.gov, Aug. 12, 2020. https://ntrs.nasa.gov/citations/20205006661 [Accessed 05 December 2025].

35 Ozlem Ceviz, S. Sen, and Pinar Sadioglu, “A Survey of Security in UAVs and FANETs:Issues, Threats, Analysis of Attacks, and Solutions,” IEEE Communications Surveys & Tutorials, pp. 1–1, Jan. 2024, doi: https://doi. org/10.1109/comst.2024.3515051. [Accessed 05 December 2025].

36 A. Yu, I. Kolotylo, H. A. Hashim, and A. E. E. Eltoukhy, “Electronic Warfare Cyberattacks, Countermeasures and Modern Defensive Strategies of UAV Avionics: A Survey,” IEEE Access, pp. 1–1, 2025, doi: https://doi. org/10.1109/access.2025.3561068. [Accessed 05 December 2025].

37 IATA, “IATA Releases 2024 Safety Report,” Iata.org, 2024. https://www.iata.org/en/pressroom/2025-releases/2025-02-26-01/ [Accessed 05 December 2025].

38 Ribeiro, A. “EPA, WaterISAC caution utilities on drone threats and cyber risks in evolving security landscape.” Industrial Cyber, 18 August 2025. [Online] Available: https://industrialcyber.co/utilities-energy-power-water-waste/epa-waterisac-caution-utilities-on-drone-threats-and-cyber-risks-in-evolving-cybersecurity-landscape/ [Accessed: 25 November 2025].

39 Olyniychuk, D. “Secret Blizzard Attack Detection: The russia-Linked APT Group Targets Ukraine via Amadey Malware to Deploy the Updated Kazuar Backdoor Version.” SOCPrime, 13 December 2025. [Online] Available: https://socprime.com/blog/secret-blizzard-attack-detection/ [Accessed: 10 December 2025].

40 Deloitte internal sources.

41 GTIG Staff, “Cybercrime: A Multifaceted National Security Threat.” Google Threat Intelligence Group, 11 February 2025. [Online] Available: https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat [Accessed: 24 November 2025].

42 CERT-UA, “Cyberattack on DELTA System Users Using RomCom/FateGrab/StealDeal Malware (CERT-UA#5709). 18 December 2022. [Online] Available: https://cert.gov.ua/article/3349703 [Accessed: 27 March 2025].

43 Vijayan, J. “Chinese Actor Hit Taiwanese Drone Makers, Supply Chains.” Dark Reading, 13 May 2025. [Online] Available: https://www.darkreading.com/cyberattacks-data-breaches/chinese-actor-taiwanese-drone-makers-supply-chains [Accessed: 25 November 2025].

44 Lee, P et al. “Earth Ammit Disrupts Drone Supply Chains Through Coordinated Multi-Wave Attacks in Taiwan.” Trend Micro, 13 May 2025. [Online] Available: https://www.trendmicro.com/en_us/research/25/e/earth-ammit.html [Accessed: 25 November 2025].

45 Lakshmanan, R. “North Korean Hackers Lure Defense Engineers With Fake Jobs to Steal Drone Secrets.” The Hacker News, 23 October 2025. [Online] Available: https://thehackernews.com/2025/10/north-korean-hackers-lure-defense.html [Accessed: 25 November 2025].

46 Deloitte internal sources.

47 Staff, “The Rise of Cyber Espionage: UAV and C-UAV Technologies as Targets.” Resecurity, 13 February 2025. [Online] Available: https://www.resecurity.com/blog/article/the-rise-of-cyber-espionage-uav-and-c-uav-technologies-as-targets [Accessed: 27 March 2025].

48 Staff, “The Rise of Cyber Espionage: UAV and C-UAV Technologies as Targets.” Resecurity, 13 February 2025. [Online] Available: https://www.resecurity.com/blog/article/the-rise-of-cyber-espionage-uav-and-c-uav-technologies-as-targets [Accessed: 27 March 2025].

49 Deloitte internal sources.

50 “Game of drones: the production and use of Ukrainian battlefield unmanned aerial vehicles,” OSW Centre for Eastern Studies, Oct. 14, 2025. https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-10-14/game-drones-production-and-use-ukrainian-battlefield-unmanned [Accessed: 29 November 2025].

51 CYBERSECURITY GUIDANCE: CHINESE-MANUFACTURED UAS,” n.d. Available: https://www.cisa.gov/sites/ default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf [Accessed: 29 November 2025].

References

52 IBM, “Cost of a data breach report 2025,” IBM, 2025. https://www.ibm.com/reports/data-breach [Accessed: 29 November 2025].

53 “Normalizing Unmanned Aircraft Systems Beyond Visual Line of Sight Operations,” Federal Register, Aug. 07, 2025. https://www.federalregister.gov/documents/2025/08/07/2025-14992/normalizing-unmanned-aircraft-systems-beyond-visual-line-of-sight-operations#h-106 [Accessed: 29 November 2025].

54 IBM,”Cost of a data breach report 2025,” IBM, 2025. https://www.ibm.com/reports/data-breach [Accessed:

55 “Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems.” Available: https://www.faa.gov/sites/faa.gov/files/uas/resources/c_uas/ Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf [Accessed: 29 November 2025].

56 Department of Homeland Security, “Homeland Threat Assessment,” 2025. Available: https://www.dhs.gov/ sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf [Accessed: 29 November 2025].

57 “Department of Defense Cyber Developmental Test and Evaluation Guidebook,” 2025. Accessed: Dec. 15, 2025. [Online]. Available: https://www.cto.mil/wp-content/uploads/2025/07/Cyber-DTE-Guidebook-V3-June2025.pdf [Accessed: 29 November 2025].

58 McEnroe, Patrick, et al. “FERO: Efficient Deep Reinforcement Learning based UAV Obstacle Avoidance at the Edge.” IEEE, 20 August 2025. [Online]. Available: https://ieeexplore.ieee.org/document/10918966. [Accessed: 15 December 2025].

59 Zewe, Adam, “Engineers enable a drone to determine its position in the dark and indoors,” MIT News, 13 February 2025. [Online]. Available: https://news.mit.edu/2025/engineers-enable-drone-determine-its-position-dark-and-indoors-0213. [Accessed: 15 December 2025].

60 Manase, Andisiwe, et al. “The use of UAV-based systems in monitoring forest health,” Scientific African, June 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2468227625001942. [Accessed: 15 December 2025].

61 Michel, Arthur Holland, “The Future of Autonomous Warfare is Unfolding in Europe,” MIT Technology Review, 06 January 2026. [Online]. Available: https://www.technologyreview.com/2026/01/06/1129737/autonomous-warfare-europe-drones-defense-automated-kill-chains/. [Accessed: 10 January 2026].

62 Gao, Jerry, et al. “Integration of UAV and Remote Sensing Data for Early Diagnosis and Severity Mapping of Diseases in Maize Crop Through Deep Learning and Reinforcement Learning,” Remote Sensing, 4 August 2025. [Online]. Available: https://www.mdpi.com/2072-4292/17/20/3427. [Accessed: 10 January 2026].

63 Ozturkcan, Selcen, “Technology and Disaster Relief: The Türkiye-Syria Earthquake Case Study,” Innovation - Research and Development for Human, Economic and Institutional Growth. [Online]. Available: https://www. intechopen.com/books/12857. [Accessed: 10 January 2026].

64 Staff, “Real-Time Drone Data Processing with Edge Computing,” 30 June 2025. [Online]. Available: https://anvil. so/post/real-time-drone-data-processing-with-edge-computing [Accessed: 8 December 2025].

65 Cody Queen, “Containerization Explained: Benefits, Use Cases, and How It Works,” 9 December 2024. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/containerization/#:~:text [Accessed: 07 December 2025].

66 Staff, “Managing Updates and Patching in a Secure Kubernetes Cluster: When Ignoring CVEs Is No Longer an Option (Part 9),” 29 April 2025. [Online]. Available: https://blog.alphabravo.io/managing-updates-and-patching-in-a-secure-kubernetes-cluster-when-ignoring-cves-is-no-longer-an-option-p/ [Accessed: 07 December 2025].

67 Staff, “Trusted Supply Chain and Remote Provisioning with the Trusted Platform Module,” RSA Conference 2018.

68 Staff, “Introduction to Trusted Execution Environments,” May 2018. [Online]. Available: https://globalplatform. org/wp-content/uploads/2018/05/Introduction-to-Trusted-Execution-Environment 15May2018.pdf [Accessed: 07 December 2025].

About the authors

Shawn Cozzolino
Senior Solution Delivery Manager, Deloitte & Touche LLP
scozzolino@deloitte.com

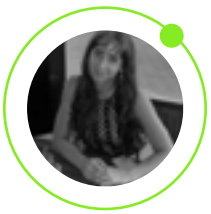
Shawn Cozzolino is a security and cyber operations leader with over 20 years of experience spanning military, federal, and global commercial environments. He currently serves as a leader in Global Managed Cyber Threat Intelligence services at Deloitte.

David An, Ph.D.
Solution Delivery Manager, Deloitte & Touche LLP
davidan3@deloitte.com

David has expertise in cyber threat intelligence--researching and writing reports about nation-state advanced persistent threats and cybercriminal activity, and briefing corporate clients.

Emily Notariano
Senior Solution Delivery Lead, Deloitte & Touche LLP
enotariano@deloitte.com

Emily has over 10 years of experience across military intelligence and cyber threat intelligence, with her military intelligence work focused on threats to aircraft and her cyber threat intelligence work focused on threats to IT/OT/IoT networks supporting critical infrastructure.



Helen Burns
Solution Delivery Lead, Deloitte & Touche LLP
hburns@deloitte.com

Helen leads the Deloitte CTI strategic threat intelligence team, providing expertise on cyberthreats from Russia and Eurasia as well as threat actor use of generative AI.

Laxima Niure Kandel, Ph.D
Assistant Professor of Computer Sciences, Embry-Riddle Aeronautical University
niurekal@erau.edu

Laxima has expertise in RF fingerprinting, GPS Spoofing and AI-Assisted Cybersecurity.

Dr. M. Ilhan Akbas
Associate Professor, Embry-Riddle Aeronautical University
akbasm@erau.edu

Dr. M. Ilhan Akbas leads the FICS Research Group at ERAU, focusing on AI/ML-enabled robust autonomy, safety-critical cyber-physical systems validation, advanced multi-agent simulation and digital-twin frameworks.

Berker Peköz, Ph.D.
Assistant Professor of Electrical Engineering and Computer Sciences, Embry-Riddle Aeronautical University
pekozb@erau.edu

Dr. Peköz specializes in AI-driven edge and infrastructure compute systems that enhance the security and resilience of communications, sensing, and navigation for non-terrestrial connected autonomous platforms.

Deloitte.