Unmanned Aircraft Systems (UAS): Evolving Risks to Large-Scale Public Gatherings

Cyber-Risks Supplemental

May 2026

Overview

Unmanned Aircraft Systems (UAS), or drones, should be treated not only as potential physical security threats, but also as mobile cyber-access platforms, which can be exploited by threat actors targeting large-scale events. By providing an aerial vantage point, drones can bypass fences, gates, guards, access-control points, and other ground-based security measures to position cyber tools near wireless networks, rooftop equipment, upper-floor offices, stadium operations centers, broadcast infrastructure, or other sensitive systems. The CIS whitepaper Unmanned Aircraft Systems (UAS): Evolving Risks to Large-Scale Public Gatherings identifies cyber-enabled UAS operations as a distinct threat vector, noting that drones can carry Wi-Fi exploitation tools, radio-frequency (RF) jamming equipment, and rogue access points near protected infrastructure, bypassing the physical separation that many cybersecurity architectures assume.

This supplemental whitepaper further examines drones as potential platforms for proximity-based cyber intrusion, electronic disruption, and data collection, while identifying associated vulnerabilities and layered mitigation considerations for security planners, especially those focused on large-scale gatherings and special events. Addressing these risks also requires a collective defense approach, in which government, law enforcement, emergency management agencies, private sector operators, and venue stakeholders share information, align capabilities, and coordinate response to detect and mitigate UAS-enabled cyber threats.[1]

Context

Traditional cybersecurity planning often assumes adversaries will gain network access remotely, through phishing, exposed services, compromised credentials, insider access, or physical entry. However, a drone equipped with lightweight computing hardware, such as a Raspberry Pi,[*] software-defined radio, Wi-Fi Pineapple,[†] cellular modem, or rogue access point, can place a threat actor's tools within wireless range of networks and devices without the threat actor ever entering the facility.[2, 3] In 2020, the research organization RAND assessed the cybersecurity implications of UAS use and noted drones should be considered as both cyber targets and cyber-enabled weapons. Commercial UAS can introduce cybersecurity risks through vulnerabilities in software, firmware, communications, data storage, and data transfer mechanisms.[4, 5]

Core Threat Pathways

Drones introduce novel cyber intrusion pathways by enabling adversaries to extend wireless exploitation, network reconnaissance, disruption, and data collection activities into areas beyond the reach of traditional remote attacks.[6] These pathways may also function as part of a broader cyber-physical attack chain, where reconnaissance, access, disruption, and data collection activities are conducted in sequence or in combination.[7] Key cyber threat pathways include:

[*] Raspberry Pi: A portable single-board computer capable of running wireless analysis, network-monitoring, and penetration-testing tools commonly used in cybersecurity research and experimentation.
[†] Wi-Fi Pineapple: A portable wireless penetration-testing platform capable of conducting rogue access point, Evil Twin, credential interception, and wireless traffic analysis activities during authorized cybersecurity testing.

Reconnaissance and Collection

- **Wireless reconnaissance and signal interception.** Drones can be used to collect Wi-Fi, Bluetooth, Radio-frequency identification (RFID), telemetry, or other radio-frequency signals from rooftops, parking areas, public rights-of-way, or upper-level windows.[8, 9, 10] This may allow adversaries to map wireless coverage, identify weakly protected access points, capture metadata, detect Internet of Things (IoT) devices, or identify networks associated with security cameras, ticketing systems, broadcast operations, building automation, or public-safety communications.[11, 12]
- **Cellular and network exploitation.** Venues increasingly rely on private LTE/5G (including Citizens Broadband Radio Service (CBRS)) networks to support ticketing, operations, and security communications.[13] Drones may enable proximity-based interception, rogue base station activity, or targeted disruption against these systems, expanding the attack surface beyond traditional Wi-Fi networks.[14, 15]
- **Credential harvesting and proximity-based access.** Because many enterprise wireless environments still rely on weak configurations, legacy devices, shared credentials, Media Access Control (MAC) filtering, or poorly segmented guest and vendor networks, proximity matters.[16] A drone can bring the attacker's equipment close enough to exploit wireless weaknesses that would otherwise be unreachable from outside the property. This is especially relevant for venues, broadcasters, public-safety command posts, hospitals, utilities, and critical infrastructure sites with complex, temporary, or vendor-managed networks.[17]
- **Rogue cellular and mobile-device interception threats.** Researchers have warned that drones could plausibly serve as airborne platforms for rogue cellular equipment, sometimes referred to as International Mobile Subscriber Identity (IMSI) catchers, that mimic legitimate cell towers to collect identifying information or communications data from nearby mobile devices.[18, 19, 20]
- **Visual surveillance and optical data exfiltration.** Drones equipped with high-resolution cameras can support collection against sensitive spaces, including windows, rooftop equipment, screens, badges, whiteboards, server rooms, or exposed hardware indicators.[21, 22, 23] Research has demonstrated that data could be exfiltrated from an air-gapped system‡ by using malware to control a hard-drive light-emitting diode (LED) and capturing the light pulses with a camera-equipped drone positioned outside a window.[24, 25, 26, 27]

Wireless Exploitation, Spoofing, and Disruption

- **Rogue wireless networks and traffic interception.** Drones equipped with wireless attack platforms can broadcast fraudulent networks that mimic trusted Wi-Fi access points (often referred to as "Evil Twin" attacks) or operate as rogue access points positioned near targeted users or systems. If a device connects, adversaries may intercept communications, harvest credentials, manipulate traffic, or conduct man-in-the-middle (MitM) activity to gain further access to internal networks or resources.[28, 29, 30] In 2022, security researchers reported a drone-enabled attack against a financial firm in which one drone carried a modified Wi-Fi Pineapple and another carried a Raspberry Pi, batteries, a mini laptop, a 4G modem, and Wi-Fi equipment; investigators assessed that credentials and Wi-Fi access had been targeted.[31]
- **RF interference and wireless disruption.** Drones can carry tools that disrupt communications through frequency jamming, de-authentication attacks, or interference targeting wireless security cameras, access-control systems, public Wi-Fi, or operational communications.[32, 33, 34] The Federal Aviation Administration (FAA) Global Navigation Satellite System (GNSS) Interference Resource Guide highlights Global Positioning System (GPS)/GNSS jamming and spoofing as an aviation safety issue.[35]

‡ **Air-gapped system:** A system intentionally separated from unsecured or external networks, including the public internet, to prevent remote compromise or unauthorized data transfer.

- **GPS/GNSS interference affecting navigation and timing systems.** A UAS may be used as a delivery platform for localized GPS spoofing or jamming equipment, potentially affecting nearby drones, vehicles, timing-dependent systems, or navigation tools. Spoofing is especially concerning because it does not merely deny service; it can feed false position, navigation, or timing data to receivers.[36, 37] The FAA has identified GPS/GNSS jamming and spoofing as a growing aviation safety concern and notes that the interference threat environment continues to evolve.[38]
- **Remote ID spoofing and data integrity risks.** Remote ID systems, while foundational for UAS identification and tracking, introduce potential cyber risks if signals are spoofed, manipulated, or disabled.[39, 40] Adversaries may exploit these weaknesses to mask identity, generate false tracks, or degrade trust in detection systems, complicating attribution and response, including generating multiple false signals to obscure real UAS activity or overwhelm detection systems.[41, 42]

Payload Delivery and Network Pivoting

- **Compromise of IoT and operational technology systems:** Drones may also facilitate the compromise of exposed IoT and operational technology systems, including cameras, building management systems (BMS), industrial control systems, and wireless access control devices, particularly where these systems rely on wireless connectivity or are accessible from external vantage points.[43, 44]
- **Malicious payload delivery.** A drone may physically deliver a cyber payload by dropping USB devices, small implants, rogue sensors, or network hardware onto rooftops, balconies, courtyards, loading docks, or restricted exterior areas.[45, 46] The cyber impact may be delayed if a device is later collected, connected to a network, or used to stage wireless access, enabling persistent access, follow-on cyber operations, or delayed exploitation without requiring additional drone activity.[47, 48, 49]

Compromise of UAS and Counter-UAS Ecosystems

- **Compromise of UAS systems.** A drone itself can also become the target. Adversaries may exploit vulnerabilities in drone software, firmware, data links, ground control stations, cloud services, cloud-based platforms and Software as a Service (SaaS) dependencies, docking stations, or supply chains.[50, 51, 52, 53, 54] In 2024, Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) guidance warned Chinese-manufactured UAS can create pathways for data egress, collection of sensitive imagery and facility layouts, firmware-based risk, and network-access exposure.[55] These risks extend beyond the aircraft itself to the supporting infrastructure and services that enable UAS operations, including firmware-update mechanisms, cloud-based management platforms, telemetry systems, remote-management tools, and data-storage services.[56] Compromise of these systems could enable unauthorized access, data theft, operational disruption, surveillance, or manipulation of UAS and counter-UAS capabilities at scale.[57, 58]
- **Counter-UAS degradation.** Adversaries may also modify firmware or system configurations to increase signal strength, bypass geofencing, disable identification features, or degrade counter-UAS effectiveness.[59] Commercial drones are more vulnerable to cyber compromise. Many rely on unencrypted GNSS signals, such as GPS, with limited authentication, making them susceptible to spoofing and jamming.[60] Command-and-control and telemetry links may also be weakly protected, increasing the risk of interception or takeover.[61] By contrast, military and government systems use encrypted communications, anti-spoofing protections, and hardened navigation designed for contested environments.[62]

Risk Implications and Mitigation Priorities

These vulnerabilities are amplified during major events because temporary networks, broadcast systems, ticketing operations, contractor devices, public Wi-Fi, media compounds, command posts, and vendor-managed systems often converge in dense RF environments.[63, 64, 65] The CIS whitepaper Unmanned Aircraft Systems (UAS): Evolving Risks to Large-Scale Public Gatherings assesses that cyber activity may serve as a precursor to UAS-enabled operations and that large-scale events create exploitable gaps where multiple vendors, platforms, and networks converge.[66] These risks also extend to authorized or "friendly" drone operations, where inadequate security controls, unmanaged vendor systems, or improper data handling may increase the risk of data exposure or network compromise.[67]

Addressing drone-enabled cyber risk requires a layered approach that integrates cybersecurity, physical security, and airspace awareness measures. These measures should be grounded in maintaining domain awareness across both the airspace and cyber environment, ensuring a baseline level of airspace awareness through layered threat detection and mitigation capabilities, and implementing the CIS Critical Security Controls® (CIS Controls) and CIS Benchmarks® as a baseline for asset inventory, secure configuration, access control, logging, network monitoring, service-provider management, continuous vulnerability and patch management, and incident response. Priority areas for risk reduction include:

Network and Wireless Security Controls

- **Signal hardening and segmentation.** Organizations should reduce wireless leakage beyond the facility perimeter, use Wi-Fi Protected Access 3 (WPA3) or the strongest available encryption, disable legacy protocols, rotate credentials, segment guest/vendor/IoT networks, and monitor for rogue access points, Evil Twin activity, anomalous SSIDs, and de-authentication attempts.[68, 69]
- **Encryption and authentication hardening.** Organizations should strengthen encryption and authentication protocols across wireless networks and UAS communications to help prevent interception, spoofing, unauthorized access, and command-and-control compromise.[70] Priority measures include robust encryption, mutual authentication, secure credential management, and hardening or replacing legacy protocols that may create exploitable gaps. CISA guidance further recommends strong encryption, secure Service Set Identifiers (SSIDs), Transport Layer Security (TLS), and separation of control, telemetry, payload, and video channels to reduce the risk of interception, spoofing, or unauthorized access within UAS communications architectures.[71]
- **Wireless intrusion detection and RF monitoring.** Cyber teams should integrate wireless intrusion detection, spectrum monitoring, and RF anomaly detection into event-security operations.[72] This should include procedures for identifying unexpected access points, unauthorized Bluetooth/RFID scanning, suspicious Wi-Fi probes, and anomalous signal strength patterns.[73] Establishing a baseline RF environment and alerting on deviations (e.g., new SSIDs, signal spikes, or protocol anomalies) can improve detection of drone-enabled cyber activity. This supports domain awareness by establishing what "normal" looks like across the RF environment before event operations begin.
- **UAS detection integration.** Drone detection should be linked to cyber monitoring. If a drone is detected near a network closet, broadcast compound, command post, rooftop antenna, ticketing office, or security operations center, cyber teams should immediately review wireless logs, authentication attempts, wireless de-authentication activity, rogue SSIDs, and suspicious credential activity. [74, 75]

Physical, Operational, and Incident Response Measures

- **Rooftop and vertical-plane monitoring.** Security plans should treat rooftops, upper-level windows, balconies, parking structures, adjacent buildings, and HVAC areas as cyber-relevant exposure points; not only physical-security concerns.[76]
- **Exercise cyber-physical scenarios.** Tabletop exercises should include scenarios where a drone is detected near a venue, followed by rogue SSID detection, credential harvesting, camera disruption, GPS interference, or suspicious authentication attempts.[77] This helps bridge the gap between physical security, cybersecurity, law enforcement, emergency management, and venue operations.[78] These exercises should also validate implementation of relevant CIS Controls, including audit logging, network monitoring, access control, service-provider management, and incident response.

UAS Ecosystem and Counter-UAS Security

- **Secure authorized UAS operations.** Authorized public safety, media, or vendor drones should be treated as IoT endpoints.[79], [80] CISA recommends secure software and firmware handling, encrypted communications, protected mobile devices, secure data transfer, Multifactor Authentication (MFA), and separation from enterprise networks.[81]
- **Supply-chain controls.** Organizations should evaluate drone procurement, data storage, firmware update control, cloud connectivity, docking stations, and vendor access.[82, 83] CISA and FBI specifically warn that UAS are information and communications technology (ITC) devices with multiple connection points that can be exploited to compromise sensitive information.[84]
- **Counter-UAS system hardening and resilience.** Counter-UAS detection and response systems should be treated as critical cyber infrastructure.[85] Compromise of detection layers, sensor inputs, or management systems can degrade situational awareness and undermine downstream response decisions.[86, 87] Priority measures include:
    - Network segmentation**:** Isolate counter-UAS systems from venue IT, ticketing, and public networks.
    - Firmware and software integrity monitoring**:** Validate updates and monitor for unauthorized changes.
    - Supply chain assurance**:** Align procurement and deployment with CISA Secure by Design principles.[88]
    - Access control and authentication**:** Restrict management interfaces and enforce strong authentication.
    - Anomaly detection**:** Monitor sensor feeds, telemetry, and management consoles for irregular patterns or data inconsistencies.
    - Redundancy and cross-cueing**:** Use multiple detection modalities to reduce single points of failure.

Outlook

UAS blur the traditional separation between physical and cyber risk. By enabling adversaries to position cyber tools directly adjacent to protected environments, drones can bypass many assumptions underlying perimeter security and network defense architectures.[89] Effective mitigation requires treating drone activity as a cyber-physical indicator, integrating UAS detection with network monitoring, hardening wireless, securing authorized drone ecosystems, and ensuring that cyber, physical security, and public-safety teams operate from a shared common operating picture. [90]

Resources

- CIS An Examination of AI-Enabled Threats to Event and Stadium Security
- CIS Benchmarks
- CIS Critical Security Controls
- CIS The Evolving Role of Generative Artificial Intelligence in the Cyber Threat Landscape
- CIS Unmanned Aircraft Systems (UAS): Evolving Risks to Large-Scale Public Gatherings
- CISA Cybersecurity Best Practices for Operating Commercial UAS
- CISA Secure by Design
- CISA Securing the Internet of Things (IoT)
- CISA Stadium Spotlight: Connected Devices and Integrated Security Considerations
- CISA Unmanned Aircraft System Detection Technology Guidance
- DOJ/SLATT Trends in Unmanned Aerial Vehicles (UAVs) and Their Implications for Law Enforcement
- GSA IT Security Procedural Guide: Drones/Unmanned Aircraft Systems (UAS) Security
- Canadian Centre for Cyber Security Cyber Security Considerations for Drone Use

This whitepaper was developed by the Center for Internet Security (CIS) with review and input from DroneSec, DRONERESPONDERS, Aerisq Solutions, the National Fusion Center Association (NFCA) Cyber Intelligence Network (CIN), and the National Real Time Crime Center Association (NRTCCA).

For additional support or information regarding services, please contact CIS.

References

[1] https://www.cisecurity.org/topics/collective-cyber-defense
[2] https://www.raspberrypi.com/documentation/computers/getting-started.html
[3] https://docs.hak5.org/wifi-pineapple-pager/pineapple-functions/introduction/
[4] https://www.rand.org/pubs/research_reports/RR2972.html
[5] https://www.cisa.gov/resources-tools/resources/secure-your-drone-privacy-and-data-protection-guidance
[6] https://tntmax.com/how-drones-are-becoming-a-cybersecurity-threat/
[7] https://dronesec.com/resources/d82bc040-422e-11f1-9281-49
[8] https://www.rand.org/pubs/research_reports/RR2972.html
[9] https://www.cisa.gov/sites/default/files/publications/CISA%20Cybersecurity%20Best%20Practices%20for%20Operating%20Commerical%20UAS%20%28508%29.pdf
[10] https://www.ijcna.org/Manuscripts/IJCNA-2023-O-46.pdf
[11] https://csrc.nist.gov/pubs/sp/800/153/final
[12] https://www.cisa.gov/resources-tools/resources/stadium-spotlight-connected-devices-and-integrated-security-considerations
[13] https://www.digi.com/blog/post/what-are-cbrs-and-private-lte-and-use-cases
[14] https://tecknexus.com/document/securing-private-5g-lte-cbrs-cellular-networks-whitepaper/
[15] https://ongoalliance.org/wp-content/uploads/2023/06/OnGo-Private-Network-Security-Short-White-Paper.pdf
[16] https://csrc.nist.gov/pubs/sp/800/153/final
[17] https://www.cisa.gov/resources-tools/resources/stadium-spotlight-connected-devices-and-integrated-security-considerations
[18] https://arxiv.org/abs/1702.04434
[19] https://arxiv.org/abs/2405.00793
[20] https://www.wired.com/story/dcs-stingray-dhs-surveillance/
[21] https://www.rand.org/pubs/research_reports/RR2972.html
[22] https://www.mitre.org/sites/default/files/2021-11/pr-18-3852-small-uas-characterizing-threat.pdf
[23] https://info.mitre-engenuity.org/hubfs/Open_Generation/Open%20Gen%20Reports/Open_Generation_Overview_of_Security_of_Uncrewed_UAS_Jan2023.pdf
[24] https://cyber.bgu.ac.il/cameras-can-steal-data-computer-hard-drive-led-lights/
[25] https://arxiv.org/abs/1411.0237
[26] https://arxiv.org/abs/1706.05915
[27] https://www.sciencedaily.com/releases/2015/07/150728123634.htm
[28] https://www.sciencedirect.com/science/article/pii/S2950629824000092
[29] https://docs.hak5.org/wifi-pineapple-enterprise/ui-overview/pineap/
[30] https://www.researchgate.net/publication/331607404_Drone_Hacking_with_Raspberry-Pi_3_and_WiFi_Pineapple_Security_and_Privacy_Threats_for_the_Internet-of-Things
[31] https://www.theregister.com/2022/10/12/drone-roof-attack/
[32] https://www.rand.org/pubs/research_reports/RR2972.html
[33] https://www.mdpi.com/2079-9292/15/2/317
[34] https://www.mdpi.com/1424-8220/24/17/5529
[35] https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afx/afs/afs400/afs410/GNSS
[36] https://www.cisa.gov/sites/default/files/2023-02/CISA-Insights_GPS-Interference_508.pdf
[37] https://www.mdpi.com/1424-8220/24/18/6156
[38] https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afx/afs/afs400/afs410/GNSS
[39] https://www.nozominetworks.com/resources/spoofing-drone-locations-by-manipulating-remote-id-protocols-and-communications
[40] https://www.researchgate.net/publication/364632163_Is_the_Remote_ID_a_Threat_to_the_Drone%27s_Location_Privacy_on_the_Internet_of_Drones
[41] https://decentcybersecurity.eu/guarding-the-digital-skies-cybersecurity-threats-to-drone-identification-networks/
[42] https://dronesec.com/resources/dec1a4f0-dddb-11ef-8c74-ef
[43] https://csrc.nist.gov/pubs/ir/8259/a/final
[44] https://csrc.nist.gov/pubs/ir/8228/final
[45] https://www.threatlocker.com/blog/usb-rubber-ducky-attacks-explained-keystroke-injection-evasion-and-defense
[46] https://docs.hak5.org/hak5-usb-rubber-ducky/usb-rubber-ducky-by-hak5/
[47] https://www.mitre.org/sites/default/files/2021-11/pr-18-3852-small-uas-characterizing-threat.pdf
[48] https://www.rand.org/pubs/research_reports/RR2972.html
[49] https://dronesec.com/resources/dec1a4f0-dddb-11ef-8c74-ef
[50] https://www.asisonline.org/security-management-magazine/articles/2023/05/uncrewed-aerial-systems/security-implications-drones/
[51] https://www.asisonline.org/security-management-magazine/articles/2023/05/uncrewed-aerial-systems/weaponized-drones/
[52] https://www.asisonline.org/security-management-magazine/articles/2023/05/uncrewed-aerial-systems/the-diversification-of-the-drone-market/
[53] https://www.mdpi.com/2504-446X/7/7/430
[54] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Drohnen/drone_cyber_threats_defence.pdf
[55] https://www.fbi.gov/file-repository/cyber-alerts/cybersecurity-guidance-chinese-manufactured-uas.pdf
[56] https://www.darkreading.com/vulnerabilities-threats/cyber-espionage-group-aviation-firms-steal-map-data
[57] https://spectrum.ieee.org/commercial-drones-and-gps-spoofers-a-bad-mix
[58] https://owasp.org/www-project-top-10-drone-security-risks/
[59] https://dronesec.com/resources/dec1a4f0-dddb-11ef-8c74-ef
[60] https://www.usenix.org/system/files/sec22_slides-sathaye.pdf
[61] https://usa.kaspersky.com/resource-center/threats/can-drones-be-hacked
[62] https://pmc.ncbi.nlm.nih.gov/articles/PMC8114815/
[63] https://icentralau.com.au/canberra/wp-content/uploads/2025/12/Drone-Enabled-Cybersecurity-Threats-to-Australias-Critical-Infrastructure.pdf
[64] https://www.gsa.gov/system/files?file=Drones-Unmanned-Aircraft-Systems-%28UAS%29-Security-%5BCIO-IT-Security-20-104-Rev-3%5D.pdf
[65] https://www.cisa.gov/sites/default/files/2024-03/Unauthorized%20Drone%20Activity%20Over%20Sporting%20Venues.pdf
[66] https://www.cisa.gov/resources-tools/resources/unmanned-aircraft-system-detection-technology-guidance

[67] https://training.dronesec.com/
[68] https://csrc.nist.gov/pubs/sp/800/153/final
[69] https://www.publicpower.org/system/files/documents/Counter_Unmanned_Aircraft_Systems_Briefing_Presentation.pdf
[70] https://www.researchgate.net/publication/387867253_The_Cybersecurity_Risks_Threatening_Drones_Innovative_Solutions_in_the_Digital_Age
[71] https://www.cisa.gov/resources-tools/resources/unmanned-aircraft-system-detection-technology-guidance
[72] https://www.cisa.gov/resources-tools/resources/unmanned-aircraft-system-detection-technology-guidance
[73] https://www.forbes.com/sites/kolawolesamueladebayo/2026/01/15/the-cyber-factor-why-counter-drone-systems-cant-rely-on-ai-alone/
[74] https://www.rand.org/pubs/research_reports/RR2972.html
[75] https://www.frontiersin.org/journals/communications-and-networks/articles/10.3389/frcmn.2025.1661928/pdf
[76] https://www.gsa.gov/system/files?file=Drones-Unmanned-Aircraft-Systems-%28UAS%29-Security-%5BCIO-IT-Security-20-104-Rev-3%5D.pdf
[77] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf
[78] https://www.rand.org/pubs/research_reports/RR2972.html
[79] https://www.cisa.gov/sites/default/files/publications/CISA%20Cybersecurity%20Best%20Practices%20for%20Operating%20Commerical%20UAS%200%28508%29.pdf
[80] https://www.cyber.gc.ca/en/guidance/cyber-security-considerations-drone-use-itsap00143
[81] https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf
[82] https://www.auvsi.org/wp-content/uploads/2025/07/UAS-Procurement-Guid o-2024.pdf
[83] https://www.gsa.gov/system/files?file=Drones-Unmanned-Aircraft-Systems-%28UAS%29-Security-%5BCIO-IT-Security-20-104-Rev-3%5D.pdf
[84] https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf
[85] https://www.cisa.gov/resources-tools/resources/unmanned-aircraft-system-detection-technology-guidance
[86] https://www.mitre.org/sites/default/files/2021-11/pr-18-3852-small-uas-characterizing-threat.pdf
[87] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf
[88] https://www.cisa.gov/securebydesign
[89] https://capacityglobal.com/news/new-research-warns-drones-could-launch-devastating-cyber-attacks-on-critical-infrastructure/
[90] https://www.lawfaremedia.org/article/drone-threats-are-evolving--data-retention-rules-are-not