Final Paper: UAS Cybersecurity in U.S. Border Operations

AYOKUNUMI OGUNSINA[1]
[1]*College of Aviation, Embry-Riddle Aeronautical University, Uncrewed & Auto Systems Cybersecurity*

I. INTRODUCTION

The United States shares nearly 7,500 miles of land border with Mexico and Canada, as well as rivers, lakes and coastal waters along both borders. Mexico is a region that has long been at the center of political, humanitarian, and security concerns with the US and the shared border between both countries is almost 2,000 miles. The US border security is tasked with preventing illegal immigration, human trafficking, and the movement of illicit drugs and contraband into the country. These challenges are compounded by the rugged terrain, limited manpower and most especially the various evolving methods employed by the criminal organizations. (U.S. Department of Homeland Security, 2025).

During the first Trump administration between 2017 and 2021, the border security became a central policy issue. The administration implemented a series of measures aimed at discouraging illegal immigration and strengthening the southern border. While the efforts reduced some categories of illegal border crossings and contributed to drug seizures, they also sparked debates over human rights, immigration policies and the effectiveness of physical barriers when compared to high tech solutions and humanitarian approaches.

Uncrewed Aerial Systems (UAS), commonly referred to as drones have become an important tool and serves as a force multiplier for both law enforcement and first responders. Drones can provide federal law enforcement with faster response times and a tactical advantage, to include surveillance, reconnaissance, remote tracking, aid delivery, and intelligence collection. The Department of Homeland Security integrated UAS into its border security missions as far back as 2005 (Homeland Security News, 2025).

With the Department of Homeland Security increasingly relying on UAS platforms like the MQ-9 Reaper for border surveillance, these systems have become central to national security operations. Their effectiveness depends not only on their technical capabilities but also on the resilience of their cyber infrastructure. This paper investigates the key cybersecurity vulnerabilities in the Command, Control and Communication (C3) link and the Global Navigation Satellite System (GNSS)/Global Positioning System (GPS) sensor which are two of the most exploited components of the UAS systems. The study also proposes countermeasures and discusses broader operational and legal implications associated with UAS surveillance activities.

CIA Triad

In cybersecurity, particularly in the context of uncrewed aircraft systems, the Confidentiality, Integrity, and Availability (CIA) triad refers to the three fundamental principles that guide the protection of data and systems. The CIA triad is a widely recognized framework in information security that provides a comprehensive method for understanding the different dimensions of risk (Jones et al, 2025).

Confidentiality: this ensures that sensitive information is accessible only to authorized users and is protected from unauthorized access. Confidentiality protects sensitive mission data including video feeds and GPS coordinates from interception.

Integrity: this ensures that data is accurate, authentic, and has not been altered or tampered with during storage or transmission. Prompt attacks can corrupt this by generating biased, misleading, or harmful responses, thereby undermining the reliability of a system's responses (Jones et al, 2025). Integrity ensures that commands, telemetry, and sensor outputs are trustworthy and unaltered.

Availability: this ensures that data and systems are accessible when needed, especially during critical operations. Malicious prompts can degrade the

model's performance or cause it to produce nonsensical or unresponsive outputs, effectively disrupting the system's operations (Jones et al, 2025). Availability ensures that UAS components like the navigation and communication systems functions continuously throughout a mission.

Together, the CIA triad helps define the goals of cybersecurity for UAS operations, by ensuring that systems are secure, trustworthy, and mission ready at all times.

Description of the Uncrewed System in Focus

For security reasons, the Department of Homeland security does not publicly disclose the specific drone models it uses; however, UAS such as the Predator B, also known as the MQ-9 Reaper are believed to have been utilized for surveillance and reconnaissance missions (Yahoo! News, 2025).

The General Atomics MQ-9 Reaper is a remotely controlled UAS. It is the successor of the MQ-1 Predator. (K. Hartmann et al). This UAS is designed to operate in challenging environments such as deserts, mountains, and forests, during extreme temperatures while carrying out remote missions including those conducted Beyond Visual Line of Sight (BVLOS).

The MQ-9 Reaper has payloads such as sensors such as GNSS/GPS sensor and camera sensors which support high-resolution surveillance and precise navigation, they also attract cybersecurity attacks especially in environments where signal spoofing and interception are prevalent.

The payload capabilities of the MQ-9 Reaper are:

1. Electro-optical and infrared (EO/IR) sensor
2. Real time video transmission modules
3. Communication relays
4. GNSS/GPS modules for navigation and geolocation
5. Mobile Ground Control Station (GCS)
6. SeaVue marine search Radar
7. Vehicle and Dismount Exploitation Radar (VADER) sensor/Ground moving target indicator

Cyberthreats to the MQ-9 Reaper Components

Two of the most vulnerable components of the MQ-9 Reaper we will be looking at are the Command, Control and Communication (C3) link and the Global Navigation Satellite System/Global Positioning System (GNSS/GPS) sensor.

C3 Link

The C3 link in a UAS refers to the data and signal pathways that enable a drone to interact with its GCS and operators. It is a crucial subsystem that ensures safe and effective operation of the drone during all phases of a mission. The information passed between the GCS and the UAS must be managed to ensure that communication happens reliably and efficiently (Barnhart et al, 2021).

Due to its critical role, the C3 link is a major target for cyber threats. The risks and vulnerabilities of the C3 link are:

1. Jamming C3 Link
2. Network Intrusion
3. Malicious Code Injection
4. Physical Tampering
5. Eavesdropping

Jamming C3 Link

UAS use wireless radio links to communicate with the GCS and to communicate surveillance and reconnaissance data. A jammer transmits a high-energy random noise signal to increase interference with the objective of increasing the bit error rate to unacceptable levels (Bharat et al, 2019).

CIA Triad Impact: Availability

The primary goal of jamming is to deny availability of the C3 link by disrupting communication.

Mitigation Strategy: Frequency Hopping Spread Spectrum (FHSS)

FHSS a technique that repeatedly switches the carrier frequency over a wide range, making it difficult for a jammer to interfere with the communication consistently. This method increases the resilience of the UAS C3 link by reducing the window during which the jammer can affect the signal.

Network Intrusion

Network intrusion involves hacking drone control channels to intercept data or insert malicious commands, leading to data theft, surveillance, payload hijacking, or weaponization (Amr et al, 2024). A. network intrusion occurs when a malicious actor breaches the link to monitor and manipulate the operations of the UAS.

CIA Triad Impact: Integrity & Availability
The integrity is compromised since the commands or mission parameters may be altered. Availability is potentially affected if the attacker blocks access or causes the system to fail.

Mitigation Strategy: Intrusion Detection Systems (IDS)
An IDS monitors a network or system for malicious activities or policy violations (Ibrahim et al, 2023). Deploying an IDS enables the real-time monitoring of data traffic between the GCS and the UAS. IDS can detect unusual communication patterns, unauthorized command injection, or spoofed commands, triggering alerts or automated responses such as blocking the source IP or switching to autonomous flight mode.

Malicious Code Injection
Malicious code injection on the C3 link refers to the cyberattack in which the criminal actor inserts unauthorized code into the communication channel between the UAS and its GCS. The goal of the attack is to disrupt or take control of the UAS during flight.

CIA Triad Impact: Confidentiality, Integrity & Availability
The integrity is severely compromised when false or unauthorized commands are executed. The confidentiality may be at risk if the injected code enables data exfiltration and the availability can also be disrupted if the code causes crash, flight termination or communication loss.

Mitigation Strategy: Code Signing
Code signing involves digitally signing software and firmware to verify their authenticity and integrity, ensuring that they haven't been tampered with and that they originate from a trusted source. This ensures that only authenticated and verified software or firmware is executed on both the UAS and the GCS. When the system receives a code or a command, it checks the digital signature to verify authenticity and integrity. If the code has been altered or originates from an untrusted source, the system will reject it.

Physical Tampering
Physical tampering involves unauthorized access to the drone's hardware, potentially compromising the integrity of its C3 link. Such attacks can disable secure communication with the GCS or interfere with command execution.

CIA Triad Impact: Integrity & Availability
The integrity is at risk if the hardware modifications can alter system behavior or control the system and availability is also impacted if the modifications can disable communication hardware or block control signals.

Mitigation Strategy: Tamper Resistance and Tamper Detection Mechanisms
Tamper resistance is the ability to resist unauthorized access attempts, and it is mostly used at the level of the device housing while Tamper detection is the ability of the system to detect tampering. The goal of tamper detection mechanisms is to distinguish authorized use of the device from unauthorized use (Vidaković et al, 2023)

Tamper resistant hardware involves the use of specialized casings that prevents or detect the unauthorized physical access, and these systems are designed to resist physical probing and direct hardware manipulation.

Eavesdropping
Eavesdropping in the context of UAS refers to the unauthorized interception and monitoring of data transmitted over the C3 link between the UAS and its GCS. This type of cyber threat allows the attacker to silently observe the exchange of commands and payload data without alerting the system or operators.

CIA Triad Impact: Confidentiality
Confidentiality of the system is compromised since the sensitive data is exposed to unauthorized observers.

Mitigation Strategy: End-to-End Encryption
Encryption techniques offer effective methods to prevent confidentiality threats; however, experts must employ a strong method to prevent an attacker from easily decoding encrypted data. Policy-based and cryptography-based techniques are effective mitigation methods against integrity threats. Moreover, the data must be stored in encrypted form. Furthermore, if required, the data must be transmitted to the command center through an encrypted communication protocol (Bharat et al, 2019).

C3 Link Summary
All five threats pose critical risks to the C3 link but target different aspects of the CIA triad. Jamming and physical tampering primarily threatens availability;

eavesdropping undermines the confidentiality while network intrusion and malicious code injection are targeted by all three aspects.

GNSS/GPS Sensor

The GNSS/GPS sensor is a critical navigation component in a UAS that allows the drone to determine its precise geographic position and maintain accurate flight paths. Potentially, the following are the types of cyberattack on the UAS:

1. Global Navigation Satellite System (GNSS) spoofing
2. Denial-of-service (DoS)
3. Signal Jamming
4. Password-cracking attacks
5. Injecting malware

GNSS Spoofing

In a GNSS spoofing attack, actual GNSS signals are simulated, and fake signals are transmitted to create false location knowledge. Manufacturers program GNSS receivers to use the strongest signal to enable the receiver to acquire a more accurate position. Consequently, spoofing signals must be stronger than real signals in a successful attack, prompting the GNSS receiver to accept spoofed GNSS signals instead of real GNSS signals. As a result, the receiver is unable to detect its current (and accurate) position (Humphreys et al. 2008; Parkinson et al. 2017).

CIA Triad Impact: Availability

The drone uses false location data which alters the mission accuracy and navigation

Mitigation Strategy: Defenses Based on Drift Monitoring

Drift monitoring is a GNSS spoofing detection technique that involves observing and analyzing the natural behavior of a receiver's position and clock over time to identify anomalies that could indicate a spoofing attack.

It looks for unusual changes in the receiver position or clock fix. If the spoofer causes the receiver clock error to change to rapidly, then the victim receiver can detect that the rate of clock drift is larger than is reasonable for its class of oscillation (Psiaki et al, 2016).

Denial of Service

The DoS is an effective cyberattack method against networks. In this case, the malicious actor transmits a high volume of null data packages to the network. The useless data packages consume network resources. The victim's network is unable to reply to the excessive requests received and eventually breaks down (David and Thomas 2019).

Distributed denial-of-service (DDoS), a variation of DoS, is harder to detect in terms of malicious traffic than a DoS attack because the attacker uses "zombie computers" during such an attack. The term "zombie computer" refers to a computer that has been infected with malware before the attack. The attacker triggers the unaware users' zombie computers to send malicious data packages to the victim's network (Gasti et al. 2013).

As a consequence of a possible DoS or DDoS attack to primitive sensors, in particular, an unmanned vehicle may be theoretically forced to travel at too low a speed (Parkinson et al. 2017).

CIA Triad Impact: Availability

The drone may not be able to access GNSS services or process location data therefore affecting its availability.

Mitigation Strategy: Intrusion Detection Systems (IDS)

An IDS monitors network traffic in real time and detects patterns characteristic of DoS/DDoS attacks such as unusual traffic volume spikes, repeated requests from specific IP addresses and redundant packets. By identifying the anomalies, the IDS can trigger alerts, isolate suspicious traffic, or automatically reroute communications through more secure channels.

Signal Jamming

Signal jamming is one of the most crucial problems of wireless communication protocols. This type of attack causes a disruption of services by blocking radio frequencies. Various devices and services may be affected negatively by jamming, including Bluetooth-enabled devices, wireless networks, GNSS services, and mobile phones. Jamming can be conducted legally or illegally. The jamming device, called a jammer, transmits the signal at the same frequency as the target system or device. Adequate power allows the jamming signal to override the genuine signal. As a result of this attack, the receiver is unable to receive data from the real transmitter (Kesavulu et al. 2013).

Conducting a GNSS jamming attack on an unmanned vehicle is simpler than GNSS spoofing (Parkinson et al. 2017). Moreover, GNSS jamming is less dangerous than GNSS spoofing because the target receiver may detect the abnormal situation and warn an unmanned vehicle's operator (Humphreys et al. 2008). Nevertheless, the vehicle or the operator will be unable to determine the current location using the GNSS, thereby losing its navigation capability.

CIA Triad Impact: Availability
The drone loses access to GPS data thereby disabling the navigation and geolocation.

Mitigation Strategy: Use of Anti-Jam Antennas
Anti-Jam antenna uses beamforming or null steering techniques to suppress signals coming from the direction of the jammer while continuing to receive signals from the GNSS satellites. This strategy protects the availability of GNSS services, allowing the UAS to sustain its navigation capabilities even in hostile environments.

A null in the received antenna pattern can be formed once the interference signal has been detected, and the power of the interference is reduced while maintaining the power of the actual GPS signal (Burbank et al, 2024).

Password-cracking attacks
A password is required to access maintenance interfaces of the system, in general. The correct password may be uncovered by the use of several password-cracking methods, such as a dictionary attack, rainbow table attack, and brute force attack (Parkinson et al. 2017). Once they have cracked the password, the attackers can modify the operational parameters, negatively impacting the efficiency and reliability of the affected system.

A dictionary attack employs a list of words used individually or in combination to crack the victim's password. In comparison, a brute force attack is similar to a dictionary attack, except it may employ non-dictionary words with alphanumeric combinations. Although using this method to crack a password may take be a time-consuming process, the password can be identified eventually if the victim has not taken the requisite precautions. The rainbow table attack is also similar to a dictionary-based attack. This attack method features a list of pre-computed hashes created from potential passwords, including a given algorithm (Parkinson et al. 2017).

CIA Triad Impact: Confidentiality & Integrity
The confidentiality is at risk if access may expose sensitive configuration data and integrity is also impacted if the modification of the GNSS settings or routing data is altered.

Mitigation Strategy: Use of Strong Password Policies and Multi-Factor Authentication (MFA)
To counter password cracking attacks on UAS, it is strongly advised to combine a strong password policy with multi-factor authentication for the best result.

Effective password policy should require:
a. Minimum of 12-16 characters
b. A mix of upper- and lower-case letters, numbers and symbols
c. Regular password expiration and rotation
d. Use of password managers

MFA adds an additional layer of defense by requiring not just a password but a second form of authentication such as a one-time code, biometric verification or use of physical security token. Even if the password has been successfully cracked, MFA prevents unauthorized access without the second factor.

Injecting malware
Malware is harmful software designed to run on a specific operating system, such as Mac OS, Windows, or UNIX. Different types of malwares employed for different purposes are available under various names, including virus, worm, spyware, adware, trojan, bot, rootkit, keylogger, and ransomware. A malware program may damage the files in a computer, monitor the victim's activities, or constitute a backdoor for further attacks. Moreover, malware may be used for cyber warfare. For instance, "Stuxnet" malware was allegedly specifically coded against an Iranian nuclear facility by U.S. and Israeli intelligence services (Bettany and Halsey 2017).

Malware can infect control systems, especially unmanned automobiles having passengers, which may be infected through the onboard diagnostic port, embedded web browsers, media players, and removable ports (Parkinson et al. 2017).

CIA Triad Impact: Confidentiality, Integrity & Availability

The confidentiality may be breached when the malware can log the GNSS data or surveillance information and the integrity is compromised when the malware may alter navigation or sensor outputs while the availability is compromised when the GNSS may be disabled, or the systems may crash due to the injection of the malware.

Mitigation Strategy: Antivirus

To effectively mitigate the risk of malware injection into UAS, particularly through control interfaces or onboard systems, the use of antivirus is necessary.

Software based threats are mitigated by adopting antivirus and IDS solutions. The operator should update the operating system and verify the legitimacy of the code running on it. Software countermeasures include classical security approaches such as encryption techniques and IDSs compared to hardware solutions, which rely on embedding security services into hardware modules and software-based attestation approaches. In addition, firewall implementations on the GCS can block sending malicious traffic to the UAVs and an antivirus and IDSs can monitor the network traffic and secure UAVs against malicious activities (Tychola et al, 2025).

GNSS/GPS Sensor Summary

All five threats pose critical risks to the GNSS/GPS sensor but target different aspects of the CIA triad. Spoofing presents the highest risk to integrity, jamming, DoS, and malware injection are the most dangerous to availability while malware injection and password-cracking attacks are critical risks to confidentiality.

II. LEGAL AND ETHICAL IMPLICATIONS

The integration of UAS like MQ-9 Reaper into border surveillance raises several legal and ethical questions. First, the continuous collection of imagery and metadata, especially over private property or populated areas can infringe upon individuals' privacy rights. UAS surveillance data, if improperly secured may also be misused, violating confidentiality principles. There is also concern over accountability in the event of a data breach or misuse of the information gathered.

III. CONCLUSION

The deployment of UAS like the MQ-9 Reaper in the U.S. border surveillance offers unmatched operational capabilities. However, the growing reliance on such platforms also exposes critical vulnerabilities, particularly in the C3 and GNSS components. This paper evaluated a range of cybersecurity threats from GNSS spoofing and C3 link jamming to malware injection and password cracking through the lens of the CIA triad.

While individual mitigation strategies are important, securing the MQ-9 Reaper's critical systems demands a multilayered approach that integrates detection, protection and recovery.

Detection mechanisms are essential to recognize intrusions and abnormal behaviors in real time. This includes the deployment of IDS cross the C3 network, drift monitoring techniques for spoofing detection and behavioral analytics to uncover unauthorized access or system tampering.

Protection measures provide proactive defense against known vulnerabilities. These include end-to-end encryption for C3 data flows, antijamming and signal authentication technologies for GNSS receivers and MFA for access to GCS and maintenance interfaces.

Recovery strategies ensure operational continuity in the face of successful attacks. These include redundant navigation systems to substitute for GNSS, automatic failover protocols like return to base commands during C3 failure and data restoration mechanisms for rapid recovery.

By combining the detection, protection and recovery strategies, operators can increase the detectability of attacks, ensuring the MQ-9 Reaper remains effective even in hostile environments. Future work should explore AI assisted threat detection and quantum resilient encryption to prepare for the evolving cyber landscape confronting uncrewed systems.

REFERENCES

[1] Amr Adel, and Tony Jan (2024, July 13). Watch the Skies : A Study on Drone Attack Vectors, Forensic Approaches, and Persisting Security Challenges. *Cybersecurity in the IoT*

https://doi.org/10.3390/fi16070250

[2] Aybars Oruc (2022, January 4) Drone Systems and Applications: Potential cyber threats, vulnerabilities, and protections of unmanned vehicles https://doi.org/10.1139/juvs-2021-0022

[3] Barnhart, R. Kurt, Douglass M. Marshall, and Eric J. Shappee (2021) *Introduction to Unmanned Aircraft Systems.* Third edition CRC Press

[4] Bettany, A., and Halsey, M. 2017. What is malware? *In* Windows virus and malware troubleshooting. *Edited by* A. Bettany and M. Halsey. Apress. pp. 1–8.

[5] Bharat B Madan., Manoj Banik, and Doina Bein (2019). Securing unmanned autonomous systems from cyber threats. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 2019-04, Vol. 16(2) 119-136* https://doi.org/10.1177/1548512916628335

[6] Burbank, J., Greene, T., & Kaabouch, N. (2024). Detecting and Mitigating Attacks on GPS Devices. *Sensors*, *24*(17), 5529. https://doi.org/10.3390/s24175529

[7] David J. and Thomas C. 2019. Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic. Comput. Secur. 82: 284–295. https://doi.org/10.1016/j.cose.2019.01.002

[8] Gasti, P., Tsudik, G., Uzun, E., and Zhang, L. 2013. DoS and DDoS in named data networking. *In* 2013 22nd International Conference on Computer Communication and Networks (ICCCN), Nassau, Bahamas, IEEE, 30 July–2 August 2013. pp. 1–7. https://ieeexplore.ieee.org/document/6614127

[9] General Atomics: MQ-9 Unmanned Aircraft System https://www.cbp.gov/sites/default/files/2025-04/250429%20FY24%20AMO_10_General%20Atomics%20MQ-9%20Unmanned%20Aircraft%20System.pdf

[10] Homeland Security News (2025) https://homeland.house.gov/2025/04/01/real-time-situational-awareness-chairmen-guest-strong-open-subcommittee-hearing-on-drones-in-the-homeland-security-mission/#:~:text=Since%202005%2C%20the%20Department%20of,agent%20safety%20on%20the%20ground

[11] Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W., and Kintner, P.M. 2008. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *In* Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA, 16–19 September 2008. pp. 2314–2325.

[12] Ibrahim Hayatu Hassan, Abdullahi Mohammed, Mansur Aliyu Masama, Chapter 6 - Metaheuristic algorithms in network intrusion detection, Editor(s): Seyedali Mirjalili, Amir H. Gandomi, Comprehensive Metaheuristics, Academic Press, 2023, Pages 95-129, ISBN 9780323917810, https://doi.org/10.1016/B978-0-323-91781-0.00006-5.

[13] Jones, N., Whaiduzzaman, M., Jan, T., Adel, A., Alazab, A., & Alkreisat, A. (2025). A CIA Triad-Based Taxonomy of Prompt Attacks on Large Language Models. *Future Internet, 17*(3), 113-. https://doi.org/10.3390/fi17030113

[14] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber-attacks - An approach to the risk assessment," 2013 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, Estonia, 2013, pp. 1-23. https://ccdcoe.org/uploads/2018/10/26_d3r2s2_hartmann.pdf

[15] Kesavulu O.S.C and Harini P. 2013. Enhanced packet delivery techniques using crypto-logic riddle on jamming attacks for wireless communication medium. Int. J. Latest Trends Eng. Technol. 2(4): 469–478.

[16] M. L. Psiaki and T. E. Humphreys. June 2016 "GNSS Spoofing and Detection," in *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258-1270. https://doi.org/10.1109/JPROC.2016.2526658

[17] Parkinson S., Ward P., Wilson K., and Miller J. 2017. Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans. Intell. Transp. Syst. 18(11): 2898–2915. https://ieeexplore.ieee.org/document/7872388

[18] Thili, F., Fourati, L. C., Ayed, S., Ouni, B., (2022). Investigation on Vulnerabilities, Threats and Attacks Prohibiting UAVs Charging and Depleting UAVs Batteries: Assessments & Countermeasures. Ad Hoc Networks, Volume 129, 2022. 102805, ISSN 1570-8705

https://doi.org/10.1016/j.adhoc.2022.102805

[19] Tychola, K. A., & Rantos, K. (2025). Cyberthreats and Security Measures in Drone-Assisted Agriculture. Electronics, 14(1), 149. https://doi.org/10.3390/electronics14010149

[20] U.S. Department of Homeland Security: Border Security (2025) https://www.dhs.gov/topics/border-security

[21] Vidaković, M., & Vinko, D. (2023). Hardware-Based Methods for Electronic Device Protection against Invasive and Non-Invasive Attacks. Electronics, 12(21), 4507. https://doi.org/10.3390/electronics12214507

[22] Yahoo! News (2025, June 12): Department of Homeland Security Predator B Drones Are Orbiting Over Los Angeles https://www.yahoo.com/news/department-homeland-security-predator-b-235904615.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAAJL5Zkld0OYClo6J9vJbpJISLbxso5uMKou-pYZ1icQchshSrKSVnWuQds3Yk_IDN2Wi6HKuClGqZvq6b50GtXOv3123TlGK21myncK2Naw59O2_x485WIZTsJmyf_T2UwEzXURJ-SLRNl_zfnQf7_5kv-LrXCQM6mcj54SNH23

[23] Yuan, X., Xingshuo, H., Gelei, D., Jiwei, L., Yang, L., & Tianwei Z. (2023, August 1). SoK: Rethinking Sensor Spoofing Attacks against Robotic Vehicles from a Systematic View. 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P). Nanyang Technological University Library. https://tianweiz07.github.io/Papers/23-eurosp.pdf