FORMULATING A COMPREHENSIVE CYBERSECURITY FRAMEWORK FOR UNCREWED AERIAL VEHICLES

Anice Kiarra Thompson
Troy University
Troy, AL, 36081
athompson186850@troy.edu

Dev D. Patel
Embry-Riddle Aeronautical University
Daytona Beach, FL, 32114
pateld47@my.erau.edu

M. Ilhan Akbas
Embry-Riddle Aeronautical University
Daytona Beach, FL, 32114
akbasm@erau.edu

Abstract—This paper presents a cybersecurity testing strategy specifically designed for uncrewed aerial vehicles (UAVs) that is both efficient and comprehensive compared to existing testing methods, along with initiating attack methodologies such as, GPS Spoofing and Denial-of-Service (DoS) on a UAV model to test the effectiveness of our cybersecurity framework. UAVs provide several benefits in today's world. But they are susceptible to many different cybersecurity threats. The goal of the paper is to create a cybersecurity framework catered towards UAVs for users to follow. As widely credited and known for covering all major aspects of cybersecurity, we use NIST (National Institute of Science and Technology) as the leading framework and enhanced each of the five core functions of NIST to fit the exact needs of UAV cybersecurity. This was done through the addition of several other elements from different frameworks such as MITRE ATT&CK, ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission) 27001 and CIS (Center for Internet Security). To demonstrate the criticality of a cybersecurity testing strategy, we used an agent-based simulation environment and represented the effects of a cyber-attack on a UAV if safety implementations are manipulated and not secure enough. Representations of a normal UAS operation were given along with additional visuals demonstrating how these attacks can alter the operation of a UAV system's response times, resulting in an increase in the likelihood of risk and collision.

Keywords— Uncrewed Aerial Vehicles (UAVs), NIST (National Institute of Science and Technology), MITRE ATT&CK, ISO/IEC 27001 (International Organization for Standardization and the International Electrotechnical Commission), CIS (Center for Internet Security).

I. Introduction

Uncrewed aerial vehicles (UAVs) have been used since the late 1950s. They carry out missions and tasks without operators being physically onboard the aircraft. UAVs can be used in several different types of applications such as in aerial photography to capture images for a company. The military also uses UAVs to perform critical operations. Such as initiating cyber-attacks, performing intelligence and reconnaissance missions, and search and rescue missions. These UAVs can obtain highly advanced LiDAR Sensors and provide a high level of precision when navigating to provide aid to those in need of it or gain additional information from an adversary. Despite these positives, there are some major challenges in the operation of UAV systems. Unfortunately, UAVs fall victim to numerous cyber-attacks. It is necessary to implement safety measures to prevent further attacks and breaches from happening. For this paper's purpose, the safety measures include creating a cybersecurity framework for UAV users. Currently, there are many cybersecurity frameworks, however, none of these frameworks are made specifically for UAV users and many of the frameworks are made for companies and organizations to maintain their major systems. Hence, through our research, we developed and answered the following research question: “Can a risk-based cybersecurity testing strategy specifically designed for uncrewed aerial vehicles be developed that is both efficient and comprehensive compared to existing testing methods?” To answer the research question, this paper presents a framework to be used with UAVs by combining aspects of pre-existing cybersecurity frameworks and strategies. To create our model, we explored several cybersecurity standards and identified the required components from each for the needs of UAV security before, during, and after a cyber-attack. We combined aspects of some of the different standard frameworks we researched to create one framework. After deciding on our main framework, the National Institute of Standards and Technology (NIST) [1] cybersecurity framework, we utilized portions of three other frameworks we researched to enhance the five core functions of NIST (Identify, Protect, Detect, Respond, and Recover) that is needed to be strengthened for use with UAVs. These three frameworks include MITRE ATT&CK [2], ISO/IEC 27001 [3], and CIS Controls 8 and 17 [4]. In-depth analysis of supporting research papers and explanations on why and how the chosen frameworks will support our goal are also provided. To stress the importance of cybersecurity on UAVs, we also created a model representing a manned aircraft, a helicopter, and a UAV flying and intersecting in their paths. This model gives an overview of normal UAV behavior and shows the UAV properly avoiding the helicopter when it is within a certain distance of the UAV. It also later shows the risks that can occur should a UAV face a cyber-attack during this moment. This model's purpose is to convey that UAVs can cause many problems if their security is not up to par.

II. Related Works

Cybersecurity standards are critical for the deployment of cyber physical systems. The research paper by Webb and Hume [5] proves the effectiveness of using NIST as a leading framework. West Texas A&M University adopted this framework, enabling the implementation of additional IoT measures to be carried out on their campus such as the creation of smart-connected parking and transportation, and the deployment of a network to aid faculty and staff on research related projects. The reason for selection of the NIST CSF (Cybersecurity Framework) in this project includes the simplification of terminology and language, cost effectiveness, utilization of components in COBIT and ISO frameworks, and the worldwide recognition of being a credible and reliable standard to use. Additional recommendations and modifications were also given to each function in NIST to further enhance the existing framework and tailor it to fit the project's needs similar to how we propose ours. The paper by Greer [6] explores the efficiency of using the MITRE Attack framework in developing strategies to address vulnerabilities in UAV systems pertaining specifically to S&R (Surveillance and Reconnaissance) operations. Towards the paper's end, it shares a scenario created to highlight the performance of this framework in mitigating attacks. This paper discusses choosing 2 attack matrix types from the MITRE Attack framework, Enterprise and ICS (Industrial Control Systems). The enterprise matrix covers applications made in operating systems such as Windows, MacOS, Linux, and various other cloud environments. This paper additionally gives scenarios that test the performance of the MITRE Attack framework such as GPS Spoofing attacks. Building onto this paper, and testing it in a 3D simulated environment, would enhance the efficiency of using the MITRE ATT&CK Framework in other UAV cybersecurity related projects such as our own cybersecurity framework. The study by Choudhary et al. [7] describes an Intrusion Detection System that includes aspects of our proposed cybersecurity framework. The detection and response functions of the NIST framework correspond to the incident response aspect of the Intrusion Detection System. The ISO/IEC 27001 framework logs and monitors incidents using intrusion detection and provides structured incident response plans. MITRE consists of various intrusion detection techniques to identify suspicious behaviors in a system. Finally, CIS Control 8 focuses on managing audit logs and can be used to alert when an attack or suspicious activity is detected, which is an important part of Intrusion Detection Systems. This paper supports that our framework, which consists of a combination of 5 different incident response frameworks, will effectively detect, respond, and fight against cyberattacks. The research paper by Balderstone et al. [8] proposes a framework for incident response and recovery. The framework proposed by the writers consists of a combination of several pre-existing frameworks, including some of the frameworks we have incorporated into our proposed framework. They use the NIST framework, ISO/IEC 27001 framework, and CIS Controls (though we utilize CIS Controls v8 in our framework which was launched after the publication of their paper). Their proposed framework has 4 stages, the planning phase, preparation phase, mid-incident phase, and post-incident phase. These 4 phases closely resemble the 5 phases of our proposed framework. The planning phase and preparation phase of their framework resemble the enhanced identify and protect functions of our framework, where we manage our assets, create risk assessment, monitor our systems, and report suspicious activity. The mid-incident phase correlates with our response function where we use ISO/IEC 27001 to complete an incident response form and the post-incident phase corresponds with our recover function where we use CIS Control 17 to perform post-incident analysis, document lessons learned and improve our incident response for future incidents.

III. Proposed Framework

A. *Overview*

For this study, the NIST (National Institute of science and Technology) framework proves to be most effective. Consisting of five core functions: Identify, Protect, Detect, Respond, and Recover, this framework covers all main aspects of cybersecurity today. The choice in this standard exists in the designs range of flexibility and customizability to fit the needs of any project. Further enhancements were implemented into this standard including the addition of elements in various frameworks such as, MITRE ATT&CK, ISO/IEC, and CIS (Center for Internet Security).

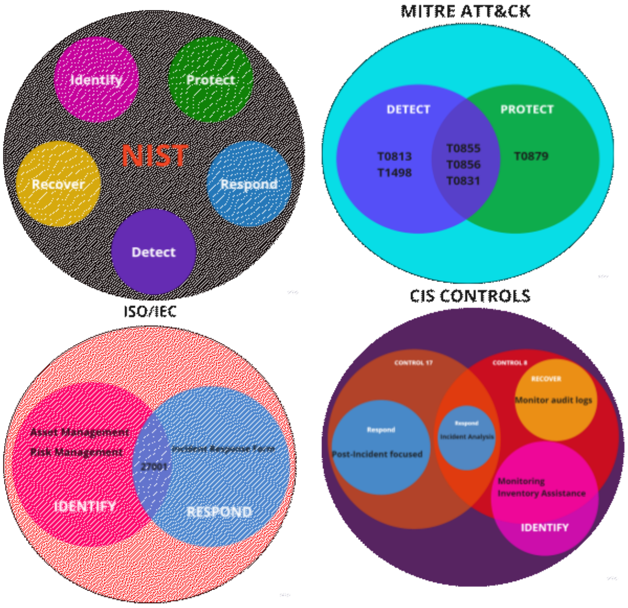

Figure 1 Visual Representations for the Proposed Framework

<u>Why MITRE ATT&CK?</u> MITRE ATT&CK provides detailed explanations as to what type of tactics are used in cybersecurity, and how they can be implemented by an adversary to do harm in the real world. It shares different assets that can be targeted in an attack and any mitigation and detection methods to use to fight against the attack. This can be demonstrated by a Water Breach attack in 2000 which will be discussed in more detail later. MITRE lists several targeted assets during the attack, including a Control Server, Data gateway, Human-Machine interference, Programmable logic controller, and Intelligent Electronic Device. This can be useful in our research project by enhancing several aspects of the leading NIST framework. For example, in asset management, we can consider the inventory of assets and find ways to protect them. In response phases of NIST, these elements prove to be helpful in finding ways to detect and mitigate the attacks we plan to execute. This is useful because it can allow us to think like an adversary into how they would target assets. Such as using Network analysis tools to detect any strange activity and ways to filter activity preventing any unauthorized inputs and commands from being made. This framework covers all the main aspects of cybersecurity today encompassing a robust range of several tactics and techniques used by adversaries to aid in any research project

B. *Implementation of MITRE ATT&CK Framework* MITRE ATT&CK is a knowledge-based system structured in matrices, describing the various actions an adversary might take when operating under a network system. We decided to use three tactic ID numbers which relate to the two different cyber-attacks we plan to initiate, GPS (Global Positioning System) Spoofing and DoS (Denial of Service) attacks. T0856 – Spoof Reporting message, T0855 Unauthorized Command Message, and T1498 – Network Denial of Service.

T0856 Spoofing & T0855 Unauthorized Command Message

In UAVs, spoofing and unauthorized command messaging is done when an adversary transmits false signals that mimic real ones or enters a series of inputs leading a drone down an unprojected flight path. This is potentially dangerous in many different cases. For instance, let's say you wanted to capture cinematic photography of homes in a community or a plot of land right by an airport. After conducting pre-flight checklists and preparation, you conduct a mission. But whenever you fly the UAV, you notice it not following your commands from the ground control station. It goes off in a totally different trajectory away from you and towards the airport. Now you can understand how dangerous this might be. Doing such an attack can lead to potential crashes, damaging property, causing safety hazards, and even worse, causing severe injury or even death. A real-life case study similar to this can include the Maroochy Water Breach in 2000. In this study, an adversary manipulated the controls of a local government's wastewater system to disrupt and release 800,000 liters of sewage into the community. This is why stressing the importance of implementing safety measures in UAVS is a critical problem to address. And the need to start developing ways for the system to become resilient to cyber-attacks through robust defensive mechanisms is imperative. Safety measures can be done using a Machine learning algorithm, Neural network, and seeking the guidance of a cybersecurity framework.

Why this methodology is effective:

We agreed to follow the MITRE ATT&CK framework because it allows for ways for individuals to understand how these attacks are done and the need to protect systems. We specifically used the spoofing and unauthorized command message tactics from MITRE because it provides documentation on how TTPS (Tactics, Techniques, and Procedures) are used by adversaries to carry out attacks. For example, first, analyzing several ways adversaries can make attacks, then finding vulnerabilities in the system that can help us in developing detection methods and mitigation strategies. Such as conducting data signal encryption or using any anti spoofing technology. Incorporating these TTPS in our project can also allow us to create very realistic simulations to test similar attacks. This in turn can help us test the resilience of the security systems in drones and look to develop ways to protect the system in the future.

T1498 Denial of Service

This attack is done by exhausting a system's bandwidth capacity by directing tons of network traffic towards the system. This can delay response times in input commands or even worse, lose total control in a temporary shutdown of the system. This can also cause major damage to property and injury as well. Here is another example going back to the cinematic photography scenario of the drone. In the event of the drone taking pictures of a home, if a DoS attack were initiated and the drone was set to move forward to get a picture of the house, a delay could be made in movements of the drone, making it fly closer to the house increasing chances of hitting it. A more serious situation could be the drone needing to avoid a helicopter flying in the air. Instead of flying the drone away from the helicopter, a DoS attack can cause delays in time responses, making the drone crash into the helicopter instead of avoiding it.

Why this tactic is effective:

This element is useful because it provides information and insights into different DoS attacks such as resource exhaustion and network flooding. Understanding these vectors can help in finding vulnerabilities in the system. MITRE ATT&CK also suggests several ways to detect and mitigate potential DoS attacks. Such as continuously monitoring network data, checking for any suspicious activity like anomalies in data.

Additional Tools to use for the MITRE ATT&CK Framework:

Additional tools that we used to enhance our framework include the following from MITRE:

T0813 – Denial of Control – This is when an adversary blocks all input from the operator. This can be particularly useful for this research project because it allows us to cover various scenarios of how these attacks can be made and accounted for. An example of this can be demonstrated from a case study "The Dallas County Siren Incident" in 2017. What occurred was that the operators of the Dallas office of Emergency Management (OEM), were unable to disable the fire alarms that were hacked into. The attack was done using a Dual-Tone-Multi-Frequency (DTMF) signal from a radio. After investigating, it became clear that one or more computer systems used for controlling the sirens were compromised. Denial of Control was also demonstrated through the Maroochy Water Breach incident that was discussed above. The adversary temporarily shut down a network system preventing any investigators from issuing any controls. (Blocking any inputs and commands from an operator.) (This tactic can help us in detecting anomalies in data)

T0879 – Damage to property – This is any action intended to cause damage and destruction to property. Used in GPS Spoofing and Denial of Service attacks, the adversary is planning to do harm, and that could lead to potential consequences such as damage to any buildings, land, or any other property. This can be supported by the Maroochy Water Breach incident. An adversary accessing control systems to release 800,000 liters (about 211337.6 gal) of raw sewage into the city solely just to cause and wreak havoc.

T0831 – Manipulation of Control – This tactic focuses on an adversary gaining control over a system alone. This can allow us to find additional ways to address multiple attack vectors of several attacks including Spoofing and DoS attacks. And can allow us to find several of the most popular mitigation tools and techniques to address these issues. Some examples can include implementing a tool to analyze network traffic and set up alerts to take notice of a potential DoS attack such as a Watchdog timer. Another can be to ensure communication authenticity between two systems. Allow it to where the system does not allow any external control without prior permission.

C. *Implementation of ISO/IEC 27001***:**

One of the most widely known frameworks today, ISO/IEC 27001 uses a systematic approach to manage sensitive information ensuring it remains secure. Information is shared in a series of clauses and annexes.

We decided to take elements from clause 6 sections 1 and 2 for risk management and annex A8 for asset management from this framework to enhance the identify and response functions of the NIST framework. The NIST framework on its own does not include additional asset and risk management aspects, So, after concluding, we decided adding these elements could be used to further strengthen our approach to improving UAV security. We want to prove additional ways to demonstrate strategies and verify the framework's effectiveness as well. (Using a more enhanced version of the NIST response function tailors it to fit the exact needs of our project.)

In relation to our project potential assets and inventory could include, the data gathered that was implemented in the Simulation, the 3D simulated world itself, the drone used, and any sort of building/objects we plan on using when demonstrating a particular scenario. Then we would need to rank each asset on a scale from most important to least important, allowing us to make room for discussion as to what the most important asset is and why, as well as coming up with the best possible approach as to what best defensive strategies are to address security issues. For the response function of the NIST framework, we plan on strengthening it by implementing an incident response form. Based off Clause 6 and Annex A.16, here is a proposed incident response form we propose to execute from ISO/IEC 27001:

- **Name of the Incident (Or ID #):**
- **Date and Time of Incident:**
- **Reported by: [Name]**
- **Description of Incident:**
- **List of systems that were affected:**
- **What were the initial steps taken:**
- **Eradication:** (Identifying the root cause of an attack.)
- **Recovery:** (Testing, verifying, and monitoring systems.)
- **Lessons Learned:**
- **Perform post-incident analysis:** (Reviewing incident response plan and analyzing the effectiveness of the response.)

This form is used due to its high credibility to maintain a set of safe cybersecurity practices. Offering a more structured approach. It also covers major critical aspects of cybersecurity. The form is to be completed during the response period of the NIST framework.

D. *Implementation Of CIS 17:*

The CIS (Center for Internet Security) is another framework that discusses taking safe practices and implementing effective security measures. This framework is structured into 18 different CIS controls which expand on a prioritized set of actions to take to mitigate threats. Benchmarks are also included discussing attacks that can be done and mitigated using several operating systems, network devices, servers, cloud providers, applications, and mobile devices. CIS Control 17 is included in our framework due to its robust support for post-incident analysis. Section 17.8 focuses on conducting post-incident reviews. While that is something mentioned in the ISO/IEC 27001 incident report, it does not give much in-depth explanation. CIS 17.8 gives a detailed explanation to users of what their post-incident analysis should consist of. For instance, some of the questions users should be answering include:

- Exactly what happened?
- What caused it?
- How did the personnel responsible respond?
- How long did the response take?
- Was the response procedure adequate?
- What could have been done better?
- Was the information in the incident report sufficient?
- What could have been done differently?
- What measures can prevent such incidents in the future?

Users of our framework now have specific questions they can answer and even build off when conducting post-incident analysis. This control supports the response and recovery functions of the NIST framework. It is a part of the response documentation created using the ISO/IEC 27001 framework, but it also aids in the recovery function as knowing information such as “what caused the attack” can help with recovering systems affected by the attack.

E. *Implementation Of CIS 8:*

CIS Control 8 is another control we plan to implement in our proposed framework. It can aid in enhancing multiple functions in NIST. Control 8 focuses on the management of audit logs, which is something not included in the core 5 NIST functions but is something we feel is an important part of incident management. Due to this, it can help monitor for attacks, detect them when they occur, and give a sense of when the attack happened and where it occurred in the system when documenting the incident once it’s over.

Essentially, adding Control 8 to our framework can provide a lot of useful information more than one of the core NIST functions. It provides visibility in the logging of all assets and accurate inventory in an audit form. For the response function, monitoring logs can aid in incident analysis as logs can indicate when and where an attack originated. They are also useful in the recovery function as they can show where systems were in their efficiency right before the attack and give developers ideas of what systems are expected to do when they are being brought back online. Viewing logs right before an attack can essentially save progress rather than developers having to potentially recover systems from scratch.

IV. Experimentation and Results

After the completion of the framework, it was decided to test and demonstrate a simulation of a UAV and a helicopter head-on encounter. The UAV encounters are simulated by a multi-agent simulation, developed in the Julia Programming Language using the Agents.jl package. This simulation enhances the use of our framework by following proper guidelines in maintaining safe cybersecurity practices. The initial state of the simulation is shown below in Figure 2:

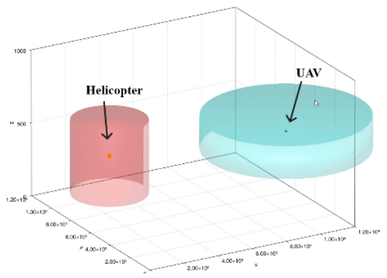

Figure 2 Initial State of Simulation

The dots in the center of each cylinder represent the aircraft itself. The surrounding shaded areas represent the space for flight violation if the other aircraft enters that space. What we aim to present is how GPS Spoofing and DoS attacks can be demonstrated in a simulation. The image above is what the simulation shows at the start of the scenario. Fig. 3 is a visual displaying the middle of the scenario:

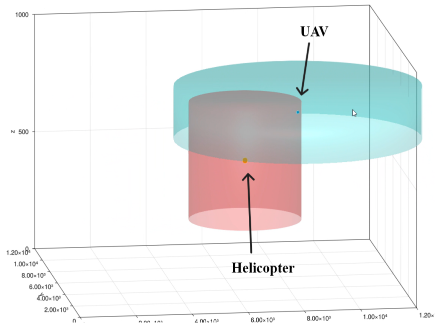

Figure 3 Middle State of Simulation

The helicopter approaches the UAV, and the UAV works to avoid the helicopter's movements. As the helicopter continues its path, the UAV moves to avoid it once it is within a certain distance. Fig. 4 shows the visual representation of location and position of each object at the end of the scenario.

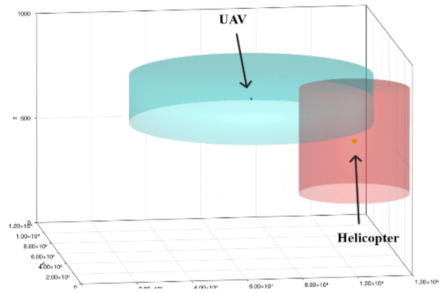

Figure 4 Final State of Simulation

These images show an effective representation of a drone avoiding a helicopter's movements during normal operations. But if a cyberattack were to be executed such as a GPS Spoofing or DoS attack, this would cause delays in the response time of the drone system increasing the likelihood of it crashing into the helicopter.

First, we have the example before of initial positioning in Fig. 5:

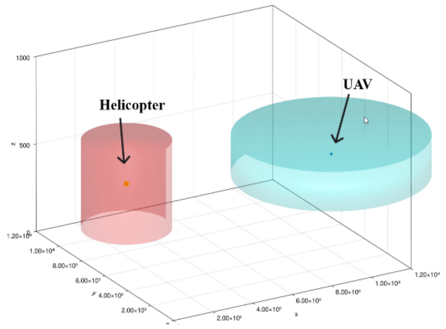

Figure 5 Initial State of Simulation

As shown in Figure 6, we can see the positioning of the UAV and helicopter after the execution of a DoS or Spoofing attack:

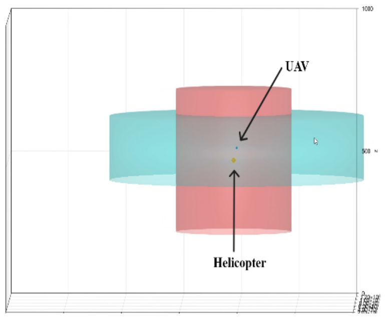

Figure 6 Representation of a Cyberattack in the Simulation

Unlike before, the UAV gets extremely close to the helicopter before it begins to correct itself and move away. In a real-life scenario, a last second correction like this may not be enough to prevent a crash, or the UAV may not be able to correct itself in time.

VI. Conclusion and Future Work

This paper presents a cybersecurity framework catered towards cyber testing of UAVs. Specifically, our framework addresses GPS Spoofing and DoS attacks. Due to UAVs being used pervasively in many domains, it is vital that their security increases with their popularity, as well. We provide a framework that can be a steppingstone to future frameworks and research on the cybersecurity of UAVs. Aside from creating a cybersecurity framework for UAVs, we also provided a simulated example of the hazardous situations UAVs could be in should someone with malicious intent gain control over a UAV during a dangerous situation. In a real-life scenario, should this ever happen to a UAV user, the framework we provide can be used to aid. Our framework is intended to be used before, during, and after a cyber-attack with the intent of allowing users of the framework to learn from attacks that may happen, and better prepare for future attacks.

The future work includes extending the simulation model, demonstrating more attack methodologies, incorporating a Machine Learning algorithm and developing a Neural Network to use as a defensive strategy against cyber-attacks. Hence, creating a model that learns to differentiate between real and synthetic data will be the goal for this project in the near future.

Acknowledgment

This material is based upon work supported by the National Science Foundation (NSF) award CNS-2244515. This research was conducted through the NSF REU program enabling students to conduct intensive research to develop a project focusing on UAVs in the cybersecurity realm.

References

[1] Pascoe, C. , Quinn, S. and Scarfone, K. (2024), The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Papers (CSWP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.CSWP.29, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=957258

[2] ISO/IEC. "ISO/IEC 27001:2022." ISO.org

[3] Strom, Blake E., Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas. "Mitre att&ck: Design and philosophy." In Technical report. The MITRE Corporation, 2018.

[4] CIS Controls TM V8, pp. 76, 2021.

[5] Webb, James, and Dustin Hume. "Campus IoT collaboration and governance using the NIST cybersecurity framework." *Living in the Internet of Things: Cybersecurity of the IoT-2018*. IET, 2018.

[6] Greer IV, Jeffrey. "MITRE Attack framework adaptation in UAV (Unmanned Aerial Vehicles) usage during surveillance and reconnaissance missions." (2024).

[7] G. Choudhary, V. Sharma, I. You, K. Yim, I. -R. Chen and J. -H. Cho, "Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 2018, pp. 560-565, doi: 10.1109/IWCMC.2018.8450305.

[8] Staves, A., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2020, May). A Framework to Support ICS Cyber Incident Response and Recovery

[9] Asiedu, Samuel. "Risk driven models & security framework for drone operation in GNSS-denied environments." (2023).

[10] Fas-Millán, M.-Á., Soro, F., Jung, O., & Shaaban, A. (2023). Cybersecurity analysis in the UAV domain: The practical approach of the Labyrinth project. In *GoodIT '23: Proceedings of the 2023 ACM Conference on Information Technology for Social Good* 10.1145/3582515.3609566

[11] Shinde, Nivedita, and Priti Kulkarni. "Cyber Incident Response and Planning: A Flexible Approach." *Journal of Network and Computer Applications*, 5 Nov. 2021, https://doi.org/10.1016/S1361-3723(21)00009-9.

[12] Visconti, Paolo & De, Fernando & Pintado, Prieta & Telli, Khaled & Kraa, O. & Himeur, Yassine & Ouamane, Abdelmalik & Boumehraz, Mohamed & Atalla, Shadi & Mansoor, Wathiq. (2023). A Comprehensive Review of Recent Research Trends on Unmanned Aerial Vehicles (UAVs). Systems. 11. 400. 10.3390/systems11080400.