Drone Tracker Project Proposal

Meredith Nye, Abe Perkins, Sterling Sloan, Aaron Stewart, JieJun Stowell, Austin Williams
Electrical and Computer Engineering Department
Tennessee Technological University
Cookeville, TN
mrnye42@tntech.edu, asperkins42@tntech.edu, sbsloan42@tntech.edu,
ajstewart42@tntech.edu, jjstowell42@tntech.edu, agwilliams43@tntech.edu

I. Introduction

Drones have grown exceedingly popular in recent years due to both their novelty and capabilities. In the year 2020 alone, commercial drone sales increased by over 21 percent [1]. Unfortunately, not all drone users prioritize the safety and privacy of others while flying their drones, so to combat a rise in unsafe drone activities, the Federal Aviation Administration (FAA) created a regulation in 2023 requiring drones to emit a remote identification signal [2]. Utilizing this regulation, this team proposes a drone tracking device that will notify the Tennessee Technological University (TTU) Police if an unauthorized drone enters the contiguous campus.

This drone tracking device will help the TTU police keep the campus safe from any unauthorized drones that threaten to compromise the safety and well-being of TTU students or staff by not following the operating requirements enforced by the FAA [3]. This device will also help alleviate some of the stress placed on the campus police department when responding to a drone-related crime by providing valuable information to a dispatcher in real-time.

The drone tracking device will be able to capture and store all of the data from the remote ID signals, take a picture of the drone using the obtained location during flight, and then report the information captured by the device to campus police. This information will be presented on a website, identifying the drone ID (remote ID-compliant serial number), drone location and altitude, drone velocity, control station location, control station elevation, time mark, and emergency status [3]. The website will then take the recorded data and create a flight path for each of the flight sessions reported. When a drone is detected during flight, the drone tracking device will check to see if TTU has authorized access. If permission is denied, then a warning notification will be sent to the TTU campus police department, and live information regarding the flight can be viewed on the website

This proposal aspires to offer a solution to the problem presented above. Throughout the rest of this proposal, the team will detail a broad implementation of a particular solution to this problem, specifically one in which drones are detected using radio frequency sensors to intercept the remote ID signal. The team hopes that upon completing this project, they will have made the TTU campus safer.

II. Formulating the Problem

At TTU, many students pilot drones around campus. Often, students will pilot drones irresponsibly, putting bystanders on campus at risk. There is currently no drone detection system on campus to assist in the protection of students against drones. The most useful tool for protecting students against drones is the ability to quickly locate the drone and its control station. The team's challenge is to create a system that will accurately map the drone's travel path as well as store the data of the detected drones currently in flight. The following section will detail any prior knowledge the team believes the reader should know to understand how the team plans to go about solving this problem.

A. Background Information

Every month, the FAA receives hundreds of reports from a variety of sources, including pilots and law enforcement, detailing unauthorized flights of UAS (unmanned aircraft systems) [2]. These reports detail specific instances where people's lives were potentially put in harm's way due to the incompetence of a drone operator. Action should be taken to make certain that innocent civilian lives are not recklessly endangered. This project aims to create a broad system that will detect consumer drones emitting the remote ID signal, as specified by the FAA. This project will implement a radio frequency (RF) sensor(s) on the TTU campus that is designed to pick up the remote ID signal broadcast by registered drones. The information encoded in the remote ID signal will then be broken down into its constituent parts and transmitted to a database where it can be monitored by a governing body, in this instance, the TTU campus police department.

In everyday life, signals are present all around us. They can be something as complex as a WiFi signal that a cell phone joins or something as simple as music notes coming from a guitar. According to the Merriam-Webster dictionary, a signal is "a detectable physical quantity or impulse (such as a voltage, current, or magnetic field strength) by which messages or information can be transmitted" [4]. A radio frequency signal is one such signal that is used to transmit data, specifically in the 20 kHz to 300 GHz range. Different sources will sometimes list conflicting bounds for the radio frequency spectrum. For the purpose of this project, the team asks the reader to interpret radio waves as any wave with a higher frequency than audible sound but still lower than infrared radiation. These signals are far beyond the human detection range, so they are often used to transmit data between electrical devices. One such family of devices that use this range are drones, which emit their remote ID signal in this frequency band (along with multiple other signals.) One of the main ideas of the project is that the team hopes to be able to intercept and decode this signal using signal processing and analysis techniques to gather useful information.

Another large portion of this project relies on the team breaking down the information stored in these signals and converting it into something that makes sense to the campus police department. The data sent over these signals is stored in a "packet" format. These packets are organized in a standardized way such that once you know how the information is stored, you can simply pick them apart and recover the data you will need. Completion of this project is reliant on the team being able to decipher these packets and turn them into valuable information.

One more large chunk of this project is the programming aspect of it. The team, being made up of senior electrical and computer engineering students, has plenty of experience with coding. This project, however, relies on multiple programs to run simultaneously while also feeding data to each other, which is on a much larger scale than any of us have ever worked. The data from the sensor must be able to be deconstructed and organized in a way that the website and potential camera system can access it in real-time, meaning that the code must be as optimal as possible to reduce execution time, the amount of time it takes for a program to execute its instructions. This can largely be dependent on what processor the system runs on, as a faster processor will reduce the time it takes for programs to execute.

B. Specifications and Constraints

1) Specifications: This project has many different stakeholders with different specifications that will need to be addressed. The team's primary stakeholders consist of TTU campus police, Dr. Jefferey Austen, Mr. Jesse Roberts, and TTU students.

- a The campus police have specified that the database be accessed through a website and that the range of the system can reach off-campus pilots. The website is requested for ease of access and to avoid the use of phones, as the system could be constrained by the usage of a mobile app.
- b Dr. Austen is constraining the tracking system only to detect drones that are emitting the remote ID signal. Drones that are not emitting this signal will go undetected and, therefore, will be considered out of scope.
- c Professor Jesse Roberts is requesting that a control system be put in place to take a picture of the drone as well. This is a solution that may be implemented into the design in the future.
- d The system is being created to help campus police defend against drones that are not authorized to be on campus. This will help keep students safe from irresponsible drone flying.

2) Standards: In this project, the team aims to adhere to standards and rulings set by many governing bodies of the United States of America, as well as the State of Tennessee and TTU. The following standards must be followed at all times in order to remain compliant with the law.

Standards regarding Unmanned Aerial Systems [referred to in this section as "Drones"]:

- FAA 14 CFR Part 107 - This standard regulates the operation of Drones in U.S Airspace, ensuring that pilots operate their drones in a safe manner. Safety standards include limiting maximum altitude to 400 feet (122 meters), prohibiting drones from flying directly over a non-participating human being, and limiting accessible airspace for pilots to fly in without express permission [3].
- FAA 14 CFR Part 89 - This standard pertains to the Remote Identification of Drones operating in U.S Airspace. In sections 89.305 and 89.315, the standard details the minimum element requirements of the Remote ID transponder's broadcast and how often pilots are required to broadcast it. [5].
- FCC 47 CFR Part 15 - This standard pertains to electrical and electronic devices that emit or absorb radio frequencies within the 9 kHz to 3,000 GHz range. This standard limits power and exposure levels to prevent interference and endangerment to living beings [6].
- IEEE 802.11 - Regulates implementation standards for WIFI Networks, Local Area Networks, and MAC Address protocols. Also defines frequency bands and collision-avoidance protocols for wireless transmissions [7].

Standards regarding circuit design:

- NEC 310.15 - Specifies wire sizing, wire ampacity, and constraints for voltages up to 2000 volts [8].
- IEC 60364-1 - Specifies design, installation, and verification of electrical systems to ensure the safety of living beings and properties near it. This standard pertains to shock, over-current, fault, power interruption, and interference protections [9].

Standards regarding data retention at TTU:

- TTU Policy 403 - Defines procedures and standards for the usage of cameras on campus, along with surveillance periods and incident reporting procedures [10].
- TTU Policy 856 - Defines standards and requirements for data security and handling. This policy defines four levels of data security, their encryption requirements, and disposal procedures of the data [11].

3) Shall Statements:

1) The system shall detect and track remote ID emitting drones for the contiguous Tennessee Technological University campus.
2) The system shall record and store all data recovered from the Remote ID signal.

3) The system shall notify campus police in real-time upon detection of a drone in flight.
4) The data shall be displayed in real-time and in a concise manner to a secure constructed website to campus police dispatchers.
5) The system shall allow campus police to authorize drones for permitted flights in a specified time frame.
6) The system shall increase the alert's urgency if a drone is detected in a private geological region.

4) Externalities: With this drone project adding another layer of surveillance to the campus, there will be multiple impacts on the campus as a whole.

- Public Safety will be improved as a whole by being able to track and handle non-authorized public drone traffic on campus, as there have been many reports of drones flying above and too close to human spectators at events. Additional concerns being addressed refer to privacy issues with drones, many of which have cameras and are potentially able to illegally observe students in private settings.
- Social Factors may include many law-abiding drone pilots feeling as though their freedom to use their drones may be impacted as a result of this project's successful implementation.
- Environmental impacts may include a very minor uptick in power allocation from the University due to the usage of main-line power for the team's sensor array(s).
- Economic factors include a potential minor increase in financial expenditure due to needing to maintain a web server, website, and physical hardware resulting from this project. The department responsible for this upkeep will be decided at a future date.

C. Existing Solutions

Despite many solutions existing for smaller subsystems of this project, research shows that only one solution envelopes the entire scope; however, at the time of this project proposal, it is out of production. Other solutions on the market that exist but do not fully encompass the scope of the project are described below:

1) Radars are already used to detect drones. However, due to size, it can be hard for the radar to distinguish a drone from a bird. There are efforts to combat this with a product called a micro-doppler radar. This device can detect the different movement speeds inside moving objects and was created by the company Robin Radar Systems [12].
2) There are also apps, such as Drone Scanner, that can be used, but these apps have limitations that may be placed on the phone, such as only being able to read a Bluetooth signal in the case of Apple phones. Other issues with these apps are paid subscriptions and a lack of labeling specific drones as authorized or prohibited [13].
3) Aerial Armor is another app that specializes in drone tracking. This app accomplishes creating a database, real-time mapping, and reading the remote ID signal. However, this app requires a paid subscription service and is only meant to be used by security professionals [14].

D. Summarizing the Problem

The usage of unmanned aircraft systems on the contiguous campus is not permitted according to TTU policies, with some exceptions made in special cases. However, the campus police still get complaints of drones causing security, safety, and privacy issues. For example, drones are often reported over University athletic events. This is a clear safety issue for the student-athletes, and campus police are often notified to resolve the issue. Without a system to track the drone and its operator, the officers are not able to stop the problem. With the implementation of a drone tracking system, dispatchers would be able to notify the officers of the unauthorized drone and easily relay the necessary information, such as the pilot's location, so the issue could be resolved. Drones can also cause serious concerns about privacy on campus. Drones can be used in stalking or harassment cases, the most obvious situation being a drone filming into a window in on-campus housing. While this behavior could be reported currently, it would be very difficult for the pilot to be located, and a drone tracking system would make it very easy to disrupt and stop these illegal activities.

The objective for this project will be very complex. The team will need to create multiple systems consisting of hardware and software working in harmony with one another to achieve the objective. If a single subsystem did not work as proposed and designed, it would be very detrimental to the system's functionality, possibly rendering the system nonfunctional. It is also essential to ensure each system will integrate with the others seamlessly. Not taking this into consideration during the design process could make the system inoperable. As previously mentioned in the existing solutions section, the project's scope is not fully covered by any solution in current production without a paid subscription or a very large setup fee. This may be due to the 2023 regulation by the FAA requiring drones above 250 grams to emit a Remote ID signal [2]. Since drones will be required to follow this standard, more companies will likely employ this method to track drones in the future.

III. Solving the Problem

The following sections will address potential solutions for resolving the shall statements. These sections will also cover how the team will aim to achieve these solutions, identify and address unknowns, the process for evaluation of success, and the broader moral scope.

A. Solutions

The team's solution to the proposed problem will require the functionality of various systems composed of both software and hardware. These proposed systems are listed below.

- Power

- Sensor
- Network
- Website
- Optional: Protection
- Optional: Camera

The power system will involve designing, building, and testing circuits to provide power to the project's hardware, including the sensor itself and the optional camera system. Safety is the paramount concern for this system, and it will be important to comply with the electric standards listed in the standards section, ensuring the system is completely grounded and includes surge protection devices.

The sensor will detect and decode the information from a drone's remote ID transmitter as it passes overhead. For this system, the accuracy and precision of decoded information will be the paramount concern, as this information is used by other systems.

The network will use a data storage system to save the decoded information in a database so that it can be used by the following subsystems. At the time of the proposal, it was unclear whether the team desired to use a local or cloud storage option for data storage.

A website for displaying the stored data in various formats (Remote ID, flight pattern on a map) will only be accessible to TTU police, and the police will be able to set authorization for drones to be operated on campus. A good implementation of this website would allow dispatchers to view all flights of a specified drone via serial number to observe repeat activity and other quality-of-life features.

An optional system with an emphasis on the protection of the system and the longevity of the project would be extremely useful. This system would involve designing and implementing casings for security, weather-proofing, and accessibility for the project's hardware. A user manual would also be created to ensure longevity by providing clear maintenance or error resolution steps. Deciding proper locations to reduce tampering and interference will also be essential.

Implementing a camera is an optional system that could add useful functionality to the project. One way this may be implemented is with a centralized camera that will rotate to find the drone in the sky upon reception of the remote ID signal. Another way this subsystem could be implemented is with an array of cameras positioned around campus, and whichever camera is closest to the detected drone will take a picture.

B. Identifying and Addressing Unknowns

1) When multiple drones are operating in an area, one may be sending off the remote ID signal using Bluetooth, while the others may be sending off the signal using a different protocol. The team will need to determine how the device will process the input without data interference.
2) The placement of the sensor is an important unknown that will have to be addressed. The team is under the impression that placing a sensor inside a building will weaken the sensor's ability to detect drones. However, some sensors are bad at sensing beneath them, so putting them up high is a poor choice. Thus eliminating the option of placing the sensor outside on the roof. If the team places it outside on the ground, then students and other externalities are a danger to the system. The contiguous campus needs to be covered, so the radius covered also needs to be taken into account when deciding where the sensor will go.

The first unknown can be tested by experimenting on the system by flying multiple drones in the sensing area to test the system's ability to detect multiple drones simultaneously. The team could then test the system by flying two drones emitting their remote ID signals simultaneously through Bluetooth and a different protocol respectively. The team could also experiment with varying sensor placements. The most important factors to consider would be the system's safety, packet interference, and accuracy of results.

The team could also use simulation for the system's testing. The team could send various signals to the sensor that simulate a drone flying on campus. The team also may be able to run simulations to find a good location for the sensor's location. However, practical experiments will most likely be more prominent for this project.

If the team is not able to detect multiple drones simultaneously, the system's functionality would be limited compared to the initial idea for the project. Functionality would also be limited if an ideal sensor location is not found. If the unknowns are not properly addressed, the quality of the team's results will suffer.

C. Evaluating Success

The main metric for success will be derived from the shall statements that the team is constrained to complete. To test that the system works all across campus, the team will need to fly drones throughout and monitor the data to see if it is accurate to what drone is being flown and where the location is. The team will need to break the campus up into different sections and test each section thoroughly by flying the drone around for an extended amount of time to verify data collection and ensure there is no strain on the system. By breaking the campus into sections, the team will be able to test the ability of the system to differentiate higher-priority areas from lower ones. These places may include dorm room windows and sports stadiums during sporting events where large crowds will attend. During the team's testing regimen, the team will need to fly drones that are both permitted by the detection system and drones that are not permitted by the detection system. This will allow us to make sure that the information reported to the campus police department is not erroneous. To test the range of the sensor, the drone will need to be moved in and out of the expected range. The team will also need to verify that buildings are not an obstacle for the sensor and will have to pilot the drone close to buildings to make sure the sensor still picks up the desired signal. The team will need to fly the drone in and out of high-priority areas to make sure that the sensor can properly detect what areas need more protection than others and relay that information to the police. These tests are all needed to verify that the shall statements are adequately accomplished as promised by the team and requested by the stakeholders. The team cannot properly test the functionality of the system without piloting a drone, and the system needs to be tested in various areas of campus to confirm that there are no blind spots. Various areas also must be tested to verify the ability to differentiate between areas of campus.

D. Ethical Considerations and Responsibilities

Ethical considerations involved in taking on a drone tracking project are limited as the project has a small scope focused solely on prohibiting illegal drone behaviors. However, even in projects that are designed to promote safety and welfare, it is important to consider every possibility. In the case of this project, either the success or failure of the system could lead to issues. If the system is highly successful, drone users that feel stifled by the extra security may try and retaliate. The users may go to extra lengths to avoid the tracking system and in turn increase illegal drone usage overall. If the system is not successful or gives faulty information to the authorities, the team may be held responsible for faulty arrests or wasting the time and efforts of authorities. These scenarios are broader implications the project may have, and they prove that the team has a responsibility to work diligently to produce a good product, and to be honest with stakeholders about the final product.

IV. Resources

The drone tracking device will require the following parts that allow the drone device to receive, transmit, and manipulate data. The main components are as follows: a power supply, antenna, RF transceiver, microcontroller, camera module, and memory module. The following section will go into detail on the team's expected cost of each of these components and how the team plans to use them in the project to accomplish the task.

A. Physical Resources and Budget

Some software is listed below that might be used to help the design the device: KiCad for PCB design, AutoCad for 3D modeling (designing the chassis and case for the device), Python/C/C++ for programming how data is sent/received and encoded/decoded over the network and where data will be stored, and HTML software for a website design. A 3D printer for printing the prototype of the case and the chassis.
An omnidirectional antenna that enables the sensor to support 360-degree detection, and a camera module with a rotor system for capturing pictures of the drone or two wide lens camera modules for 360-degree capture. Microcontrollers used to operate the different components in the device will also be necessary. Memory modules for temporary storage of the received data before sending it off to a database in case the RF Transceiver (network processor) can't transfer data fast enough. Below are some common components found inside an RF sensor:

- A multilayer diplexer that will separate the received signal into a low and high band output.
- A bandpass filter to reject frequency outside of the 2400-2483.5 and 5030-5091 GHz ranges.
- An attenuator for noise reduction and to prevent signal distortion (any undesired change to the waveform of the signals).
- An amplifier that will boost the weak signal while maintaining the signal's integrity.
- A mixer might be necessary for demodulation and will depend on how the remote ID data is packaged.
- An analog-to-digital converter (ADC) so the RF signal can be processed by the microprocessor.

A licensed drone with a remote ID transmitter will be used to test the system. The drone will be flown at varying speeds and distances relative to the sensor, and the collected data will be compared to the information given by the drone's controller for accuracy and precision.

The figure below shows the major components of the device; the estimated total cost should be $707.20 or below.

	Qty.	Low (USD)	High (USD)
Antenna	1	13.95	79.95
RF Transceiver	1	9.81	31.57
MicroController	1-2	2.77	168.06
Camera Module	1-2	50	189
Extra Memory Module	1-2	22.43	48.62
Circuit Boards	1	N/A	200
Power Supply	1	N/A	50
Wire Supplies	1	N/A	20
Extra unknown components	N/A	N/A	100
		Total:	707.2

Table 1. Proposal Budget

B. Personnel

Skills that the team members currently possess are listed below:

- Meredith Nye: Assembly, LTSpice, MATLAB, C++, Soldering, RStudio
- Abe Perkins: Python, C/C++, Assembly, VHDL
- Sterling Sloan: Electronics Design, Signal Processing, KiCad, LTSpice
- Aaron Stewart: Auto-CAD Electrical, Arduino/C++, 3D Modeling and Printing, LTSpice
- JieJun Stowell: Assembly, VHDL, Python, C/C++
- Austin Williams: Power, LT Spice, MATLAB, Arduino, 3D Modeling

The skills necessary to complete the project will include coding capabilities, skills associated with signal acquisition, the ability to design circuitry, 3-D printing capabilities, skills associated with power supply and management, skills associated with networking, and, tentatively, the ability to design mechanical systems depending on whether a camera subsystem is added into the project scope. The skills listed initially that each team member already possesses accumulate to cover a wide range of the skills needed to complete the project. However, some gaps remain, so each team member will need to do research and learn new skills during this project. It may be necessary because of the large portion of the project scope dedicated to software for all of the team members to be more capable of coding or analyzing code. Additionally, completion of the project will require many personnel to learn more about the remote ID signal emitted by the drones and the particular network constraints of the TTU campus. Another glaring weak point in the team is a lack of database management knowledge. A concerted effort must be made by members of the team to obtain this knowledge and implement it for the project to be successful. These gaps will be closed as needed by the appropriate team members. Much of the learning regarding background information and specifications will be touched on during research for this proposal. Coding skills will be obtained either from more experienced team members or from online resources at the time when they are needed. If it becomes clear during the design process that any more in-depth knowledge is required, the appropriate measures will be taken immediately to ensure that the team continues to be capable of meeting project standards. the team will likely need to study various resources such as textbooks and reputable online sources. Electrical and Computer Engineering department professors will also be great resources to answer questions about the project or help the group find good resources, should they be willing to assist.

C. Timeline

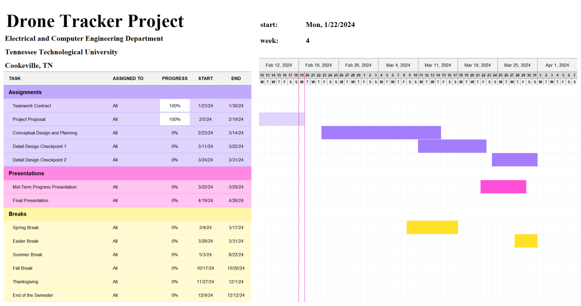

Fig. 1. Condensed Project Gantt Chart

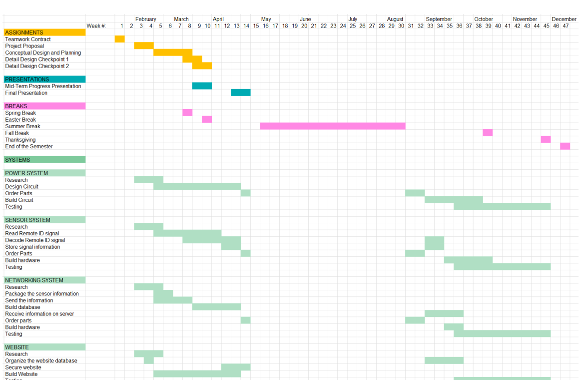

Fig. 2. Full Project Gantt Chart

V. Conclusion

In an effort to increase campus security against all non-permitted aerial drone systems, the team has proposed a Drone Tracking System. Using one or more sensors, we will detect any drone using the FAA-required remote ID transmitter and use its telemetry data to track and store its flight path while within campus airspace. This system will increase safety, allow student-registered drone flights, and promote responsible use. With these parameters, the team believes that a cost-effective and efficient solution can be developed.

References

[1] "2022 drone market forecasts: Optimism but uncertainty over demand for complex services," Unmanned Airspace, Available: https://www.unmannedairspace.info/uncategorized/2022-drone-market-forecasts-more-optimism-but-uncertainties-remain-over-demand-for-complex-services/ [Accessed Feb. 15, 2024].

[2] "Remote identification of drones," Federal Aviation Administration, Available: https://www.faa.gov/uas/getting_started/remote_id [Accessed Feb. 15, 2024].

[3] "Part 107- unmanned aircraft systems," Title 14- Aeronautics and Space, Code of Federal Regulations, Available: https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-107 [Accessed Feb. 15, 2024].

[4] "Signal," Merriam-Webster Dictionary, Available: https://www.merriam-webster.com/dictionary/signal [Accessed Feb. 18, 2024].

[5] "Part 89- minimum message elements broadcast by standard remote identification unmanned aircraft," Title 14- Aeronautics and Space, Code of Federal Regulations, Available: https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-89/subpart-D/section-89.305 [Accessed Feb. 15, 2024].

[6] "Part 15- radio frequency devices," Title 47- Telecommunication, Code of Federal Regulations, Available: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15 [Accessed Feb. 19, 2024].

[7] "Ieee 802.11-2020: Collision avoidance in wireless networks," American National Standards Institute, Available: https://blog.ansi.org/ieee-802-11-collision-avoidance-wireless-networks/ [Accessed Feb. 19, 2024].

[8] "310.15 ampacities for conductors rated 0–2000 volts," International Code Council, Available: https://codes.iccsafe.org/s/ISEP2018/national-electrical-code-nec-solar-provisions/ISEP2018-NEC-Sec310.15 [Accessed Feb. 19, 2024].

[9] *IEC 60364-1 Low-voltage electrical installations*, 5th ed. International Electrotechnical Commission, 2005.

[10] "403 safety and security camera acceptable use," Tennessee Technological University, Available: https://tntech.navexone.com/content/dotNet/documents/ [Accessed Feb. 19, 2024].

[11] "856 data security and handling policy," Tennessee Technological University, Available: https://tntech.navexone.com/content/dotNet/documents/ [Accessed Feb. 19, 2024].

[12] "Uas sightings report," Federal Aviation Administration, Available: https://www.faa.gov/uas/resources/public_records/uas_sightings_report [Accessed Feb. 16, 2024].

[13] "Dronetag releases drone scanner app to track nearby drone flights using remote id data," Unmanned Airspace, Available: https://www.unmannedairspace.info/latest-news-and-information/dronetag-releases-drone-scanner-app-to-track-nearby-drone-flights-using-remote-id-data/ [Accessed Feb. 16, 2024].

[14] "Proprietary drone detection software," Aerial Armor, Available: https://www.aerialarmor.com/drone-detection-software [Accessed Feb. 16, 2024].