Journal of Intelligent & Robotic Systems (2021) 103:69
https://doi.org/10.1007/s10846-021-01524-w

REGULAR PAPER

Defining the Tradespace for Passively Defending Against Rogue Drones

Mary L. Cummings[1] · Hala Nassar[2] · Vishwa Alaparthy[1]

Received: 28 July 2021 / Accepted: 23 October 2021

Abstract
While increasingly popular, small unmanned aerial vehicles, aka drones, are often flown illegally over outdoor public gatherings or public facilities like prisons, threatening the safety of those nearby. There is a clear need to address interloping drones in public spaces from a sociotechnical perspective, including understanding the tradespace of variables. Through surveys, interviews, technology and infrastructure design, and experimentation, we developed a tradespace model of those variables that managers and designers of high-risk settings like public spaces and prisons need to consider in their development or renovation. These include cost considerations, both capital and infrastructure, as well as technology design elements of range and false alarm rates potentially exacerbated by convolutional neural networks (aka, deep learning). Results also highlight that environmental design elements can provide a possible low-tech solution in the design of obstructions that either eliminate or complicate a drone pilot's line of sight. This effort demonstrates that managers and designers of high-risk settings like public spaces and prisons will have to balance sometimes competing objectives to obtain the best possible outcomes for public safety.

Keywords Unmanned aerial vehicle · Unmanned aerial systems · Drone · Acoustic · Alert · Warning · Defense

MSC Code 68T40

1 Introduction

Small unmanned aerial vehicles, otherwise known as drones or unmanned aerials systems (UAS), are expected to produce a global commercial market value in excess of US$43 billion by 2025 [1]. While this growth brings new economic opportunities, it has also opened the door to illegal uses of drones. These have ranged from minor in the use of drones to watch outdoor concerts to major with the use of drones to drop weapons and cell phones into prison yards. Even in the most benign of circumstances, flying drones in possibly crowded venues poses many risks.

Drones flown illegally over outdoor public gatherings threaten the safety of the public as well as operations of those legitimate aircraft that support such events. Novice pilots of drones operating illegally in these settings increase the risk of either a crash into another legitimate drone or loss of control of the drone due to inexperience, potentially resulting in a crash with people or property. Incidents have already occurred involving drones at music events [2, 3], sporting events [4], street markets [5], and even at the White House [6]. Moreover, the use of drones to drop contraband into prisons is increasing with potential grave consequences [7].

Given the rise of such issues, it has become critical for managers and designers of high-risk settings like public spaces and prisons to consider how drones could become a problem in such environments. Unlike major facilities such as airports with large budgets to develop defensive capabilities, these smaller venues have very limited budgets and staff to dedicate to protection.

Because of this increasing threat of drones in the public domain, there has been increasing research in counter-UAS. The bulk of these efforts focus on the use of expensive radio frequency (RF), radar, and electro-optical systems for detection, with one government report listing the cost to be more than $100,000 for 63 % of commercially-available systems

✉ Mary L. Cummings
m.cummings@duke.edu

[1] Electrical and Computer Engineering, Duke University, Durham, NC, USA

[2] Landscape Architecture, Clemson University, Clemson, SC, USA

Published online: 20 November 2021

[8]. Cost, including infrastructure costs, has been cited as a major detriment in the installation of counter-drone technologies, as well as the ill-defined legal landscape of using any active energy-emitting devices [9].

To address these problems, we developed a multidisciplinary collaboration to examine what interventions could be designed to support such high-risk venues in inhibiting pranksters and malicious users, including identifying cost-effective technologies with low operational overhead. To this end, this paper integrates results from previous lower-level drone experiments [10, 11] with new human performance results, design elements and feedback from both drone operators and the public to develop a tradespace model for managers and designers of high-risk settings like public spaces and prisons who want to develop solutions for defending against rogue drones.

Risk perceptions of both drone pilots and the general public were used to design prototype deterrence and detection technology solutions and landscape architecture design solutions that could fill the need for deterring rogue drone operations. We then highlight how such solutions should be flexible and adaptable across different environments, and conclude with a discussion of the tradespace that emerged from this research effort.

2 Background Information

2.1 Detecting Drones

There exist numerous proposed approaches to the detection of unmanned aerial vehicles (UAVs), including the detection of drone radio frequency signals and acoustic signals, as well as the use of camera vision and RADAR systems [12]. There are two main aspects in dealing with drones that could be illegally operating in and around areas of high risk: (1) Deploying countermeasures to prevent and deter illegal activity, and (2) Detecting rogue drones that exist within the airspace of interest. These two approaches are inextricably linked to how drones function, their capabilities, and the properties of the venue and surrounding environment, which are explored more in the following section.

Current methods to deter and stop illegal drone operations, also known as counter-UAS can generally be divided into three main categories: (1) Regulations and standards, (2) Active controls, and (3) Passive mitigations [13]. Regulations and standards focus on the long-term ability of national and local governments as well as industry and professional organizations to set rules and guidelines around the operation of drones in order to promote deterrence of unwanted drones. Examples include the Federal Aviation Administration (FAA) mandate for registration and labeling of drones [14] or manufacturer policies for including software that forces drones to adhere to safe flying practices, such as geo-fencing.

Geo-fences are invisible barriers that define boundaries in the onboard software, within which the drone cannot fly. While such regulations and standards can be useful long-term strategies for stopping some accidental drone incursions, they can easily be ignored by custom drone builders with prankster or malicious intent. Indeed, in the previously-mentioned survey of drone operators, 73 % said they had some knowledge of how to build and program drones, and the Internet hosts many websites instructing people how to disable such restrictions.

Active drone countermeasures are those that attempt to interfere with the function of a drone in real time in order to physically stop it from continuing flight. Such active countermeasures fall under three main categories: electronic (including jamming, hacking, and spoofing), kinetic (such as guns or mobile nets), and energy (such as lasers and electromagnetic pulse). Active countermeasures carry the possibility that a drone could be brought down in an uncontrolled manner, so are closely regulated by government agencies like the Federal Aviation Administration or Department of Homeland Security and may be illegal [15]. However, detecting a drone with RADAR is expensive and ineffective in detecting small drones [8], and visibility can significantly limit optical sensing techniques [9]. In addition, such active countermeasures carry significant expense not only in the acquisition of the system, but also the need to train, both initially and in refresher courses, operators who require a relatively high degree of expertise [16].

Passive countermeasures are those that do not target a specific drone, but instead attempt to diffuse the threat by other means. Examples include building infrastructure to block the views of the onboard drone cameras or through the use of camouflage like nets, which has long been a military staple of passive defense from aerial threats. Passive mitigations are advantageous in that they do not require expensive technology or training, do not increase the risk of causing a drone to fall out of the sky, and can be flexible to accommodate the various environments. However, passive countermeasures like nets may be infeasible in areas like botanical gardens that place high value on aesthetic appeal, and such interventions may also carry more costs than organizations are willing to spend.

Some companies have designed multi-faceted detection solutions that incorporate combined detection approaches but it is generally agreed that there is no current solution that can detect all drones with perfect accuracy [12, 17]. Moreover, such approaches only increase the complexity and cost of owning and operating these systems, which is substantial [18]. In this effort, we explored the use of such passive countermeasures through applications of landscape architecture survey and design methods to determine if and how such techniques could be effectively leveraged.

2.2 Understanding the Problem

While managers of high-risk spaces see rogue drones as a liability source, we wanted to get a sense of to what degree and why the general public views small, commercially-available drones as sources of risk (as opposed to military drones). Threats to privacy from commercially-operated drones have been a consistent significant concern for the general public [19, 20]. Safety has been a lesser concern with only 38 % of respondents in a 2013 survey concerned about safety [20], with nearly identical numbers in a 2019 study [19].

To determine how those opinions from people who frequent a small outdoor venue like botanical gardens compared to the earlier general public opinions, we conducted a survey of 145 people at the Sarah P. Duke Gardens in March of 2018 at approximately midday. A little more than half of respondents were female (51 %), with 55 % in the 21-40 yr. age group and 20 % in the 41-60 yr. group. Garden visitors were largely educated (76 % were college graduates) and 88 % reported that they were familiar with drones.

If respondents saw a drone while visiting the Gardens, 24 % reported they would definitely be concerned, while 35 % reported that they might be. Unlike previous studies where privacy was the major concern, this group reported their most significant concern in seeing a drone flying around the Gardens would be not knowing the intent of the pilot (50 %). The possible invasion of privacy was their second highest concern (39 %). In contrast, a 2019 study reported that 71 % of people were concerned about their privacy [19]. For the most part, this group of visitors reported that they would likely do nothing if they saw a drone flying around during their visit (55 %), while 24 % reported that they would move away from the drone. In general, it appears that this group of visitors generally see drones in the environment as more disruptive than as a threat to their safety.

These results are interesting in that while managers of the Gardens see rogue drones as a safety threat, their visitors may be somewhat ambivalent. This group of visitors was not particularly concerned with potentially unsafe drones or privacy violations. When asked whether such environments should be designed to deter rogue drones, only 40 % agreed. These visitors overwhelmingly placed aesthetics as their most important attribute of the Gardens (91 %), with safety, curiously, as their second (89 %). Privacy was the lowest ranked attribute with only 42 % of respondents reporting this as an important value.

While these results are informative in terms of how potential visitors to places like botanical gardens view drones from a safety and privacy perspective, understanding how drone pilots view such issues complements these insights. To this end, a group of 41 commercially-certified drone pilots were surveyed at a drone trade conference, also in 2018. One interviewer asked 22 questions, and recorded answers on a tablet which were either multiple-choice (e.g., In which types of areas do you prefer to use your drone? ("Please tell me all that apply")or ranked data on a Likert scale (e.g., Please state your level of agreement with the following statement: Drones are safe to use in public spaces.)

This group also was well-educated (76 % had a college degree or more) with 66 % in the 21-40 yr. age group and 27 % in the 41-60 yr. group. This sample was predominantly male (88 %), the majority of whom flew either weekly (46 %) or daily (22 %). Most (80 %) preferred line-of-sight control within a mile of their physical location, and 90 % said battery was their most important system concern.

When asked where they preferred to fly, 68 % reported flying in an open field and the goal of 66 % of respondents was to take videos and pictures of areas, objects and people of interest. Indeed, 27 % said they like to use their drones to observe social events, festivals, and games, which aligns with venue managers' concerns for public safety. The surveyed drone pilots overwhelmingly (71 %) felt that flights in public spaces were safe (Fig. 1), but interestingly, 68 % agreed that the public could be harmed by such operations.

Perhaps the most striking aspect of Fig. 1 is that while two-thirds of drone pilots recognize the danger to the public when they elect to fly in these settings, only one-third of the public (38 %) understands these risks. This difference in risk perception where pilots see more risk than does the public has also been noted in another study [21]. Such differences suggest that there are increased safety risks to the public given that the pilots have the expertise to recognize the danger, but the surveyed visitors' perceptions of risk are not calibrated to reality. These results, which are admittedly based on a small sample, further underscore that managers of outdoor venues have reason to be concerned for public safety and that it could be beneficial to them to deter conducting illegal drone operations in their areas.

2.3 The Need for a Tradespace Framework

In the development of systems with multiple stakeholders and multiple competing objectives, tradespace frameworks are

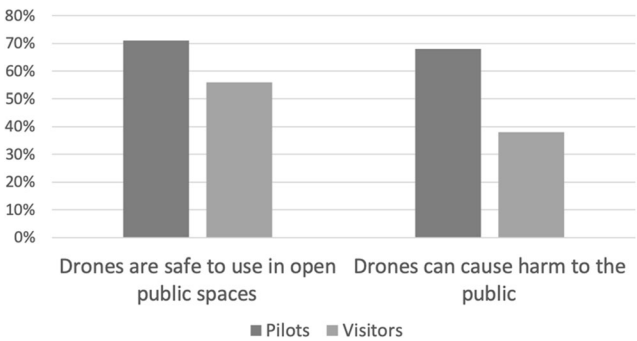


Fig. 1 Drone pilot and botanical garden visitor views on safety of drones flying in public spaces

critical in helping decision makers understand the key attributes that need to be considered, particularly when evaluating alternatives [22]. While there have been a few efforts formally examining the tradespace of unmanned aerial vehicle design, they have focused primarily on military systems [23], or low-level details like the optimal wingspans and engine types [24]. To date, there has been no published research developing or analyzing the tradespace for defending against possible drone incursions, especially those in civilian settings where costs and labor are especially limited.

To develop such a tradespace, we used our knowledge gained through stakeholder interviews to develop a low-cost, easy-to-use drone detection system and then experimented with this system to determine the critical performance elements, as well as how such systems could or should be installed in representative settings. The next section discusses the initial design as well as those iterations required to achieve basic functionality.

3 System Design

Interviews with local outdoor venue managers as well as prison officials revealed that such agencies would only like to spend approximately $1,000 on such a system, with little-to-no cost for monitoring and operations. Given this small budget, we initially elected to focus on acoustic detection systems, which are not only relatively cheaper but also could be more widely adapted to different settings.

Acoustic detection is a passive sensing approach to drone detection which involves analyzing patterns of wave energy produced by an oscillating body through distinguishing pressure fluctuations between two signals [25]. Acoustic detection is advantageous since signals are typically omnidirectional, and greater coverage is easier to achieve with a smaller sensor footprint as compared to other modalities. Analyzing sound pressure levels and spectral peak frequencies over time can detect aerial vehicles [25, 26]. Such approaches include pattern-matching through some kind of machine learning approach, which requires that a drone's acoustic signature must be known a priori to train the algorithm.

Our initial approach leveraged a discriminative statistical machine learning technique called Support Vector Machines (SVM) for classification. An SVM is a lightweight, stable and computationally inexpensive alternative for neural networks [27]. To build an SVM, we needed data from drones actually flying in order to extract features. To this end, we built a library[1] of more than 10,000 drone sounds from DJI Phantom4, DJI Inspire2 and 3DR Iris drones flying at various known ranges using a microphone connected to a low-cost ($55) micro-computer (a Raspberry Pi). Then we used Mel-frequency cepstral coefficients (MFCCs), spectrogram, chromagram, spectral contrast and tonal centroids (tonnetz) as features.

With an 80 % accuracy rate in controlled settings against three different drones, the initial results were encouraging. However, in follow-on live flight tests, the accuracy dropped to about 60 % accuracy at a range of 50-60 m. There were also a high number of false alarms when the system was exposed to lawn equipment, life leaf blowers, and weed eaters [10]. This made it clear that our approach was not robust enough for actual deployment.

In the second iteration of the design, we expanded the dataset to include many more instances of lawn equipment as well as more drone sound signatures. Instead of an SVM, we used a convolutional neural net (CNN) with a six-convolution layer approach with a reduction in the number of features used as in the SVM. Only MFCCs were used as features in the CNN algorithm. More details about this approach can be found in [11], but in similar test scenarios to that of the SVM, the CNN's accuracy ranged from 92 % for sounds 30 m away but dropped to 76 % at 60 m. In comparison, human detection accuracy rate at these same ranges was consistently ~92 % [11]. While an improvement over the SVM, false alarms were still a problem with an average of 72 false alarms a day over a 17-day period.

The high false alarm rate did not substantially improve when we switched from an SVM to a CNN classification approach and added more training data. This indicated that we needed a new approach to mitigating false alarms. To that end, we elected to add a radio frequency (RF) detector ($158) to the system to detect the 2.4 GHz and 5.8 GHz frequency range, which is the range used by small drones to transmit video. Most operators illegally flying drones (but not all) use the onboard camera for navigation and precise payload placement (like contraband). Thus, we developed a fused sensing approach such that the system would passively detect an RF signal and then alert officials. In the small chance that an operator did not use video, the acoustic sensor, provided a second layer of defense, as illustrated in Fig. 2.

One caveat to this fused approach is that there are likely other sources of RF in an environment around local outdoor venues or prisons. Thus, system filters must be updated whenever a new, approved RF signal source is installed, such as a new wi-fi router. In addition, false alarms can still occur with the second, acoustic layer of defense. However, as will be discussed in the Threat Communication section, there are ways to continually improve the system to reduce false alarms.

The resulting system, called the Fused Acoustic RF System (FARS) was constructed and installed at the Koka Booth Amphitheater in Cary, NC (Fig. 3) to determine its effectiveness both in detecting drones and mitigating false alarms. In

[1] https://sites.duke.edu/prisdatabase/.

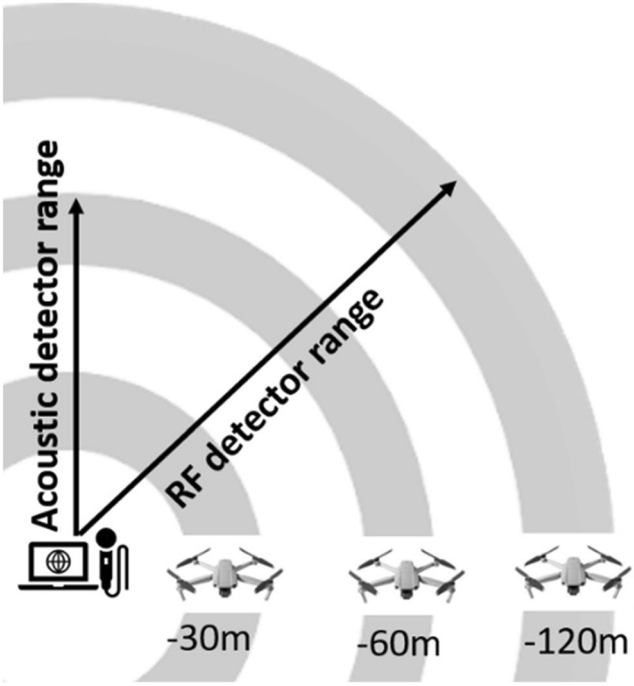


Fig. 2 RF and acoustic sensor ranges

Fig. 3, FARS is the black box in the left-center and blends in with the rest of the lighting infrastructure.

Unfortunately, only 17 days after the initial installation, a hurricane hit the local area, causing the system to fail due to a faulty power adapter. One important lesson learned in this first phase was that high winds could cause false alarms for the acoustic system, so the CNN had to be retrained to reject these sounds. Once these issues were fixed, the system was installed and left running for 154 days until the end of the project with no further system failures. During this period of operation, there were 0 % false alarms with the RF detector, and an average of 18.7 acoustic alert false alarms per day. The total cost of the final sensing unit was $400 (not including solar power and monthly cell service and data charges).

Fig. 3 The Fused Acoustic RF System (FARS) installed at the Koka Booth Amphitheater

While detection is a critical element in defending against rogue drones, alerting relevant officials that potential threats are nearby is also very important. To this end, the next section details the mobile alerting system that accompanies the sensors.

3.1 Threat Communication

Both the public venue and prison stakeholders agreed that money would not be available for continuous service and operational contracts. Thus, we needed to develop an alerting system for the sensing system that was both low in cost but also relatively easily accessible with minimal maintenance needs. Due to the ubiquitous nature of mobile phones and the relatively low cost of developing associated applications, we determined that a smartphone-based app(lication) was the best candidate for communicating a nearby threat detected by FARS to either venue managers or prison officials in a cost-effective manner.

Figure 4a illustrates the resulting application, called the Mobile Alerting Interface (MAI), which can operate on both Android and Apple phones. MAI is connected to a remote server that received notifications from the fused sensing system by a cellular module. It is designed to promote maximum situation awareness (SA), which is the comprehension of events in an environment with regard to time and space. There are three levels of SA: (1) Perceiving a critical situation, (2) Understanding key elements and events within this situation, and (3) Projecting the situation into the future to predict how the situation will unfold [28]. So, in terms of rogue drone detection for high risk areas, FARS needs to communicate with users in such a way to allow them to quickly perceive, understand and develop plans for possible mitigation.

While more detail about MAI's design and evaluation can be found in [29], as seen In Fig. 4a, the primary display that leverages native maps indicates where the threat was likely detected and which sensor detected the target, which allows users to perceive and understand what is happening. The additional critical element is the confidence interval that accompanies any alert, which is critical in calibrating user trust and especially important in the presence of fused sensor data [30]. The confidence estimate, either medium or high confidence, is based on the number of 'drone detected' predictions in a 10 s audio clip (a total of five samples).

In addition to the confidence interval which helps users understand the likelihood of an actual threat, if an alert is triggered by the acoustic detection system, users can also play back the sound file that caused the alert (Fig. 4b). This real time feedback is critical since the probability of a false alert based on acoustic sensing is non-trivial, and allows users to

Fig. 4 The Mobile Alerting Interface (MAI), **a**) Home screen with a (M)edium confidence detection and **b**) Sound file presented to user

act as an additional sensor to screen the signal. If it is suspicious, then management can investigate in a timely fashion. If not, the app allows the user to immediately label the sound, which humans are very adept at doing [11]. This feedback is archived through the History function and could be used in future updates to the system, which is addressed further in the discussion section.

Potential users both in prison facilities and outdoor public venues were very receptive to MAI, even though there could potentially be multiple false alarms in a relatively short period [29]. Users reported that even if 1 in 5 alerts was a false alarm, they would consider such a system to be extremely effective. Moreover, they did not complain about requests for data labelling. To the contrary, users appreciated having input to the system and liked the teaming aspect.

Technology that appears to be augmenting humans as opposed to replacing them is often seen in a more favorable light [31], so this is likely an important design consideration in environments where technology may be distrusted. One caveat to this is that our partners were never tasked to assist with labeling more than a few weeks at a time, so a longer-term study is needed to determine if and when users become frustrated with data labelling in addition to other duties.

3.2 Camouflaging the Detector

While MAI and FARS address the detection piece of defending against rogue drones, one aspect of this technology piece is that, as seen in Fig. 3, FARS nested inside a black box is not particularly aesthetically pleasing. It blended in with other supporting lights and cords at the Koka Booth amphitheater but other partners like the Sarah P. Duke Gardens who place high value on visual aesthetics balk at installing such devices that may take away from the desired experience.

The physical form of such a device can even be a problem in places like prisons that may not seem to place a high value on visual aesthetics. The prison staff warned us that if we installed any device in a tree or on a pole that looked like a surveillance device, it would be shot down, especially if placed near the edge of the prison's property, which is where such devices need to be placed for maximum detection range.

Understanding that a listening device is better suited higher up to extend its vertical and horizontal range, and that some agencies care about the look of the physical form, we determined that one possible camouflage technique would be to hide FARS in an artificial bird's nest. Such a nest is common in the southeast and could accommodate a solar panel if a power source was not available or accessible.

To build such a device, first an artificial nest was designed to closely approximate a Red-tailed hawk's nest. As seen in Fig. 5a, this first nest was used as a prototype because: a) they are typically found in large trees in North Carolina 13 - 69 ft above the ground with good solar access; b) their variety in construction and vegetative materials enabled fast prototyping with material found in situ; and c) typical Red-tail hawk nest dimensions offer ample opportunity to conceal embedded equipment like batteries or a solar panel (generally 28" to 38" in diameter and up to 38" tall).

Construction and vegetative materials including twigs and branches, pine needles, and leaf detritus were gathered at the experimental site and transported to assembly areas. The nest in Fig. 5a was modelled using construction adhesives and traditional "wood weaving" techniques with a 34"outside diameter. Because the woven wood and glued nest configurations occasionally lost structural integrity under routine transportation and handling, the artificial nest also contained a camouflaged superstructure to hold the materials together.

A Lexan prototype superstructure was fabricated using split trusses assembled with Lexan adhesive and configured in a 3.5" on-center interlocking grid. The gridded trusses interlocked through paired notches at intersection points. The initial prototype was fastened with additional ¼" plastic snap ties to secure the woven wood camouflage. The Lexan superstructure was coated with a matt finish acrylic to reduce potential Lexan reflectivity, which might appear "unnatural" in a forest setting.

While this initial nest in Fig. 5a was very realistic, it was relatively heavy (17.6 kg). The organic material in the form of sticks, twigs and pinecones significantly contributed to the nest's realistic look, but this material quickly decomposed and required continued restoration once deployed. To combat the weight and decomposition issues, we then adapted the initial design to a digital format, including scanning real branches and twigs, and then printed the nest with several 3D printers. Because the design took several different printers, the initial 3D-printed nest resembled a rainbow (Fig. 5b), and then was painted with camouflage colors (Fig. 5c). The weight of the 3D-printed nest was much lighter (3.48 kg) and could be more easily mounted higher up in a tree (Fig. 5d). Moreover, given that the nest is plastic, it will last much longer than any nest made of organic materials.

Stakeholders were impressed with the final outcomes and given that the total cost of the printed nest was $31, it represents a relatively low-cost solution to blending technology into the environment that FARS protects. Indeed, while the groundskeepers at the Duke Gardens were initially wary of our approach, citing the ugliness of cell phone towers made to look like evergreens, they were very impressed with the artistic approach in creating an artificial nest. Given the ubiquity of 3D printers, groundskeepers or prison officials could easily modify or create and print their own designs to house such technology, providing flexibility in developing infrastructure in a low-cost manner.

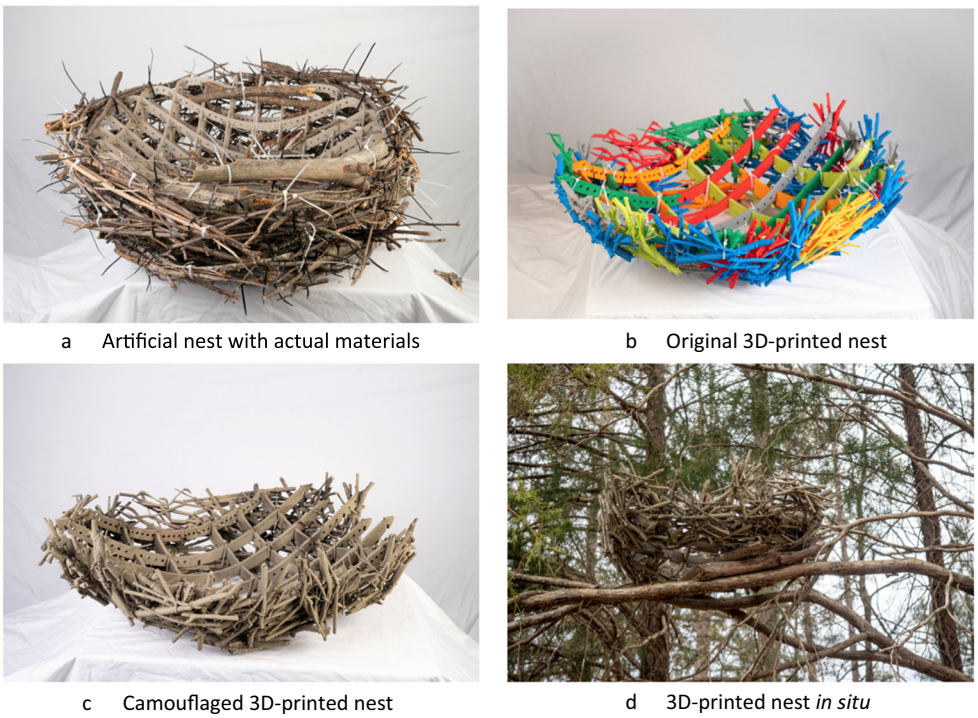


Fig. 5 Artificial Nest Evolution (Photographer: Bill Snead). **a** Artificial nest with actual materials. **b** Original 3D-printed nest. **c** Camouflaged 3D-printed nest. **d** 3D-printed nest *in situ*

4 Designing for Deterrence

While FARS and any containment unit built to hide such a device are the critical technology elements needed for a viable detection system, designing for deterrence is equally important. If operators of rogue drones struggle to achieve their goals, such increased difficulty may be enough of a deterrent in either beginning or continuing an illegal effort. While we examined many possible interventions to make flying drones difficult in a particular area, including directed lights and fog misters to blind onboard cameras and thermal devices to detect drone operators, all of these potential solutions well exceed the cost threshold for both outdoor venues and prisons.

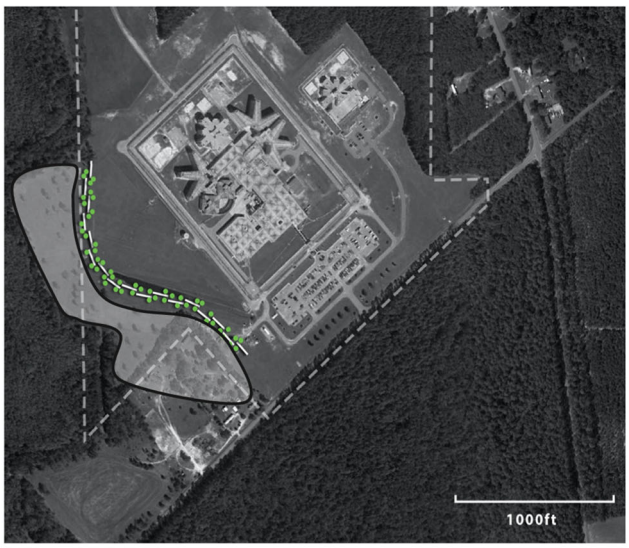
Given that active interventions to rogue drone deterrence would be cost prohibitive, we then examined methods for passive deterrence. Most commercially-available drones only have approximately 30 min of flight time, which is directly affected by any additional weight due to a payload. Thus, most pilots need to be close to their area of interest, especially if they want to drop a package.

This desire for typical drone pilots to be near their area of operation was also confirmed by the venue public managers and prison staff, who noted either finding culprits or evidence of their activity nearby. Moreover, drones that crash near prisons contain forensic data [32, 33], which often show that the pilot was relatively close to drop zone. While it is possible for people to remotely command a drone from miles away using the onboard camera and a ground control station (called beyond-line-of-sight control), such skill levels are difficult to achieve. Most people need to actually see a drone, even if only from a distance, while also looking at the video camera to precisely control it, especially to drop contraband.

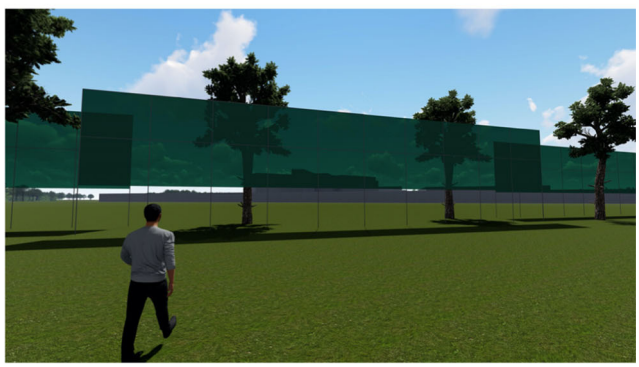
The key insight is then understanding that one major source of deterrence could be making it difficult for operators of rogue drones to achieve their desired lines of sight. Camouflaging nets is a low-cost passive aerial countermeasure military staple, which could easily be adapted to prevent rogue drone pilots from achieving their desired top-down views through the onboard camera. However, managers of venues like botanical gardens are not likely going to adapt such a measure, especially when surveys like ours reveal that the aesthetic experience is the most important characteristic to visitors. Even prisons balk at such ideas since guards need a clear view of prisoners in the outdoor yards and camouflaging nets would occlude such views.

Instead of disrupting the top-down views from the onboard camera, it is possible to disrupt the view of the pilot attempting to watch a drone in flight for more precise control. One natural way to block people's lines of sight in controlling rogue drones is to grow trees, where leaves and branches provide some protection against top-down views, and they also act as deterrent since they often present many difficult navigation challenges. While such interventions have many aesthetic and practical benefits, not the least of which is cost, they can take quite a long time to reach maturity. Moreover, for some venues that need relatively wide-open spaces for flexible uses, growing clusters of trees is not a viable solution.

For those venues that want to deter rogue drone operations without the time and resources to grow trees, there is another low-cost solution. Figure 6 illustrates the use of outdoor screens as a possible cheap and flexible deterrent to such operations. The shaded area in Fig. 6a represents an area near a prison where significant illegal activity has taken place in the past. This area is on private property so prison officials have no control over it, and is a likely hot spot for illegal activity due to its close proximity to the prison and a nearby road that enables fast escape. Operators of rogue drones prefer to stand at the edge of the tree line on the private property so they have



a Overhead photo of prison grounds, outlined by the dotted line. Most likely infiltration area is shaded in grey and the proposed screen is between it and the prison.



b Ground view of the proposed screen

Fig. 6 Possible deterrence screening. **a** Overhead photo of prison grounds, outlined by the dotted line. Most likely infiltration area is shaded in grey and the proposed screen is between it and the prison. **b** Ground view of the proposed screen

a clear line of sight into the prison yard and they can hide in the woods if spotted.

To disrupt the views of a person standing in this area, the prison can install a set of screens that obscures the view so the pilot cannot tell where the drone is in flight, particularly in the drop area. Understanding where these drop areas are, the line of screens in Fig. 6a was designed to maximize obscuration of a person standing at the tree line at roughly 750 ft from the tree line at a height of 20 ft. As illustrated in Fig. 6b, the screen material is only used from 10 to 20 ft high, with the area from the ground to 10 ft clear so that prison officials can at least partially see is someone is running either through or behind the screens.

The screen sections can either be supported by steel or wood poles. At a cost of $34.99 per roll (20' x 50'), this is a low-cost deterrence mechanism that could either be relatively easily relocated or a new section installed should a new area become a vulnerability. The design in Fig. 6 is just an illustration of how interference in a drone operator's line of sight could be addressed and such a solution would not be a likely candidate for venues that place high value on aesthetics. However, for temporary outdoor gatherings like festivals, such a solution may provide needed flexibility.

5 Discussion

Figure 7 summarizes the tradespace that emerged from the technical and social aspects of this effort in determining how to support managers of high-risk venues in inhibiting rogue drone flights. It captures cost variables (gray), technical variables (blue) and also physical design considerations (purple). At the center of Fig. 7 is the need to consider the severity of consequences for a possible drone incursion. While risk of harm to the public viewing an outdoor concert is concerning if a rogue drone attempts to also watch the concert, risk of harm to prison staff and other inmates is substantially higher if a gun or knife is dropped into a prison yard.

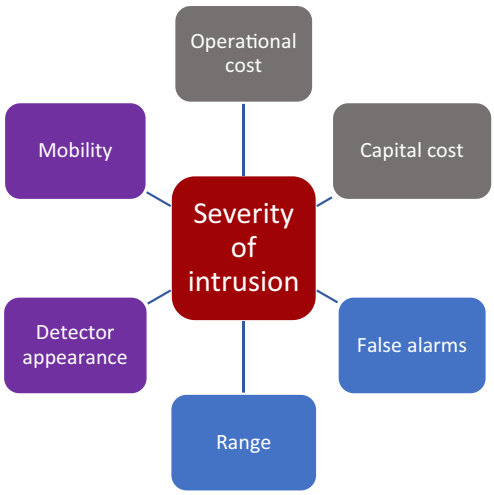


Fig. 7 Tradespace for drone incursion defense

The two cost variables, capital and operational costs, represent real world constraints that likely drive the final selection of such a system. All stakeholders we spoke to clearly considered cost the major driver of their decisions to acquire such a system, and all had very small budgets. As noted in Fig. 7, the cost of a unit (the capital cost), was only half of the cost considerations. Operational costs, which include staff for monitoring, information technology (IT) support, and maintenance, also are important to managers of small venues and public facilities. FARS was designed to minimize these costs, however, there would be intermittent needs for IT support, and maintenance could also be an issue if the nest or screens were installed.

Range and false alarms represent the technical variables in this tradespace. It is a significant finding that while a CNN can perform as well as a human at close ranges (30 m), this performance drops sharply with increasing distance. Such a finding, along with the need to constantly retrain the underlying neural networks with potentially new threats, suggests that a collaboration between humans and AI is needed to mitigate the brittleness of the CNN. This means humans are needed to assist the algorithm, and given that humans were consistently 92 % effective in their detections, our work-around that allows a human to verify the algorithm's predictions is clearly warranted.

While the range of one unit is modest (60-120 m), these units can be connected in a network, potentially greatly extending the range of the system. This would, of course, increase both capital and operational costs (the IT and maintenance costs would likely increase), but also increase the performance of the system. Trading performance for cost is common in such sensor-based systems.

The false alarm variable, while not unique in sensor-based systems, is one that becomes more prominent whenever a machine learning algorithm is used. For a high consequence setting like a prison, staff told us that they would be willing to accept approximately 1 in 5 false alarms a day, meaning that only 80 % of alerts had to be correct for them to consider this to be a useable system. If the underlying training data can sufficiently represent the breadth of possible sources of acoustic false alarms and these can be held to the 1-in-5 threshold suggested by prison guards, then such systems are viable.

While many prisons are located in rural areas with very predictable background noise profiles, many are also located in urban settings with a much more variable set of background noises. It is not practical nor cost effective for prison staff to hire a data scientist to continually retrain an acoustic CNN-based system to detect new noises in the background, so this represents a significant limitation of this system. Indeed, this is why we had to augment the acoustic system with an RF detector.

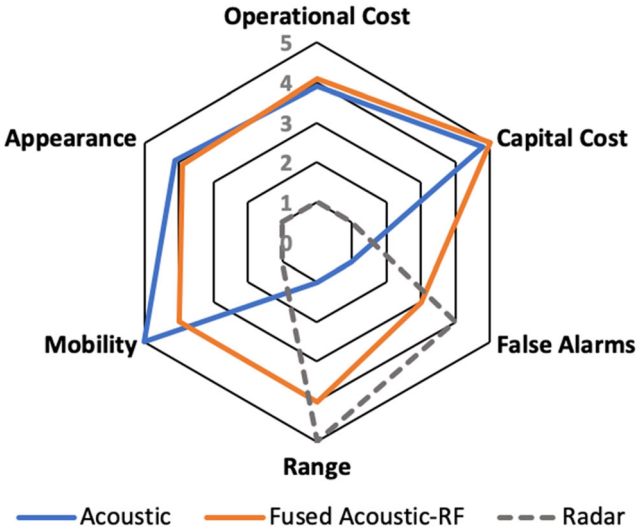


Fig. 8 Tradespace model application for different dronedetection systems

These results add to the growing body of literature about the brittleness of systems with embedded deep learning algorithms. While we were able to methodically improve our system by adding more data to the training set for each new source of a false alarm, such an approach is not scalable for FARS and likely not scalable for any system that operates in dynamic settings. While model-free estimators like CNNs can be useful, this research effort showed that without augmentation from other sensors and humans, deep learning-generated predictions were not sufficient. One area of future research that this effort highlights is the need for automated training data updates, i.e., as new sources of false alarms are identified, how to collect human-labeled data and then automatically train and update a CNN classifier without data scientist intervention.

The last variable grouping in Fig. 7, the physical considerations, includes mobility and the appearance of a detector. If such a device were to be installed in botanical garden or other setting that values aesthetics, it will need to blend in with the environment. Our botanical garden partners were somewhat reluctant to consider installing a system like FARS until they saw the nest in Fig. 5. Once they realized that technology can also become, in effect, art and part of the landscape, they were overwhelmingly in support of the system, further highlighting the important of interdisciplinary collaborations.

While prison staff do not care about aesthetics to the same degree as managers of a botanical garden, the appearance of the detector was a consideration for them in terms of preventing any kind of sabotage effort. If a detector is in a relatively isolated place without continued supervision, it is at risk for tampering or destruction so developing camouflage techniques reflective of the local biodiversity like that in Fig. 5 will be critical to prevent such physical attacks.

The mobility issue is another important finding from this research. Given that many venues may need to better protect certain areas at different times (like for festivals), and that operators would likely change the axis of their preferred attacks based on seasonal foliage and other line-of-sight considerations, having the flexibility to move the units as needed, perhaps in concert with the deterrent screens, may be desirable.

To illustrate the utility of this model, Fig. 8 demonstrates how it could be applied to our original acoustic sensor design, the subsequent FARS design, and also a typical radar like those that could be used at a regional airport, another stakeholder that has experienced significant disruptions due to both intentional and accidental drone flight incursions. From each of the use cases, the 6 elements of the model are plotted on a Likert scale of 1-5, where the exact categories are defined in Table 1. Using these scales, Fig. 8 compares cost considerations, range, appearance (whether in terms of aesthetics or a need to camouflage), minimizing false alarms and mobility for the three use cases.

The maximum score that represents the ideal use case for a passive drone detection system that embodies all the attributes in Fig. 7 is 30. The acoustic-only system use case scored 20, FARS was 24, and the airport scored 13. As seen in Fig. 8, radars have superior range and fewer false alarm issues, but they also have much higher capital and operational costs. The tradespace analysis demonstrates that FARS is a better fit for smaller venues with restricted budgets and other counter-drone systems like those that incorporate radar are not good candidates.

Table 1 Likert scale definitions for the interloping drone attack tradespace

	Operational Cost	Capital Cost	False Alarms	Range	Mobility	Appearance
1	More than 2 people needed per shift	>$100,000	Multiple daily	~50 ft	Cost-prohibitive	Too big to conceal
2	2 people needed per shift	>$10,000,<$100,000	One daily	~100 ft	Difficult	Requires significant camouflage
3	1 person needed per shift	>$5,000,<$10,000	One every few days	~2500 ft	Requires moderate effort	Requires moderate camouflage
4	Intermittent human support	>$1,000, <$5,000	One every few weeks	~1 mi	Requires some effort	Requires some camouflage
5	No human support	<$1,000	Rarely	~5 mi	Easy	Blends in with environment

6 Conclusion

With the rise of popularity in small unmanned aerial vehicles, aka drones, managers and designers of high-risk settings like public spaces and prisons are increasingly concerned with unwanted drone activity, which carries risk of harm to the public and supporting staff. In a survey of commercial drone pilots, one-quarter of respondents reported that they intentionally wanted to fly in areas that increased public risk. Thus, there is a need to understand how this problem can be addressed from a sociotechnical perspective, including what the tradespace of considerations would be.

Through surveys, interviews, technology and infrastructure design, and experimentation, we developed a model of those variables that constitute the tradespace of variables that managers and designers of high-risk settings like public spaces and prisons would need to consider. These include cost considerations, both capital and infrastructure, the technology design elements of range and prediction false alarm rates, and environmental considerations of aesthetics and possibly obstructing drone pilot lines of sight.

This analysis highlighted that, from a performance perspective, detection range will be sacrificed for cost effectiveness. The venue managers and prison officials in our representative applications felt that simply knowing a drone was nearby was the most valuable piece of information, as that knowledge would then inform an action plan dependent on circumstances. So, this trade was acceptable to them, but that might not be the case in every application. Ultimately any venue or public facility will have to determine the importance of each of the variables in Fig. 7 in developing a system that best fits their needs. By addressing the variables in Fig. 7, groups of stakeholders can at the very least, understand the space of possible solutions and where compromises may have to be made.

This effort further highlighted that when developing technologies that rely on convolutional neural networks (aka, deep learning), it is important to note that no solution is foolproof and false alarms could require additional sensors or human-based solutions. Moreover, any deterrence methods can only dissuade or slow down illegal activity so none of the solutions proposed in this effort can provide protection from rogue drones in all situations. However, through the lessons learned and the guidelines set forth in this paper, managers and designers of high-risk settings like public spaces and prisons now have a roadmap for how to balance often competing objectives to obtain the best possible outcomes.

Acknowledgements This research was sponsored by the National Science Foundation under the National Robotics Initiative. Our collaborator Robert Hewitt was a key member of the team, who sadly died during this project. We also thank Oishi Ghosh, Misheel Sodgerel, Sayan Mandal, Rocky Li, Bill Snead, Alex Stimpson, Chunge Wang, and Chip Bobbert and the Duke CoLab for their support. In addition, the assistance from Anthony Campbell and the Town of Cary, prison staff members from North Carolina (especially Loris Sutton), Oklahoma, and Colorado, and the staff of the Sarah P. Duke Gardens were critical in accomplishing this effort.

Author Contributions Cummings obtained the funding, directed and supervised the technical research, and write the paper. Nassar collected human data and generated landscape architectural design solutions and Alaparthy conducted the technical development and experiments.

Funding The National Science Foundation.

Data Availability All acoustic data is available at https://sites.duke.edu/prisdatabase/.

Code Availability Upon request.

Declarations

Ethics Approval IRB approvals were obtained for all human data.

Conflicts of Interest/Competing Interests None.

References

1. Wood, L.: Global Drone service market report 2019: Market is expected to grow from USD 4.4 Billion in 2018 to USD 63.6 Billion by 2025, at a CAGR of 55.9 %, ed: Business Wire (2020)
2. Reed, R.: Watch muse drone crash into audience during concert. Rolling Stone. https://www.rollingstone.com/music/music-news/watch-muse-drone-crash-into-audience-during-concert-162092/. Accessed 30 Jan 2021
3. Grinberg, E., Kuo, V.: Enrique Iglesias injures hand in concert drone mishap. https://www.cnn.com/2015/05/31/entertainment/enrique-iglesias-drone-feat/index.html. Accessed 30 Jan 2021
4. Laris, M.: Stadium and team owners see drones as major league threat. The Washington Post https://www.chicagotribune.com/sports/breaking/ct-spt-drones-theats-to-sports-stadiums-20180511-story.html. Accessed 30 Jan 2021
5. Barmann, J.: Man crashes drone into farmers' market. Then gets mad about being photographed. SUAS. https://www.suasnews.com/2016/01/41519/. Accessed 30 Jan 2021
6. Shear, M., Schmidt, M.: White House drone crash described as a U.S. Worker's Drunken Lark. New York Times. http://www.nytimes.com/2015/01/28/us/white-house-drone.html?_r=0. Accessed 30 Jan 2021

7. Temin, T.: Federal prisons are facing threats from drones dropping contraband, surveilling facilities. Federal News Network. https://federalnewsnetwork.com/agency-oversight/2020/10/ig-federal-prisons-face-danger-from-drones/. Accessed 3 Feb 2021
8. Brooks, S., Jacobus, C., Kouhestani, C., Stikar, J., Faye, E.: Counter-Unmanned Aircraft Systems Market Survey. Sandia National Laboratories, Albuquerque, New Mexico, SAND2019-2801 (2019)
9. Michel, A.H.: Counter-drone systems. Center for the study of the drone. Annandale-on-Hudson (2019)
10. Mandal, S., Chen, L., Alaparthy, V., Cummings, M.L.: Acoustic detection of drones through Real-time Audio Attribute Prediction, presented at the AIAA SciTech, Orlando FL (2020)
11. Alaparthy, V., Mandal, S., Cummings, M.: A comparison of machine learning and human performance in the real-time acoustic detection of drones" In: IEEE Aerospace. Big Sky, Montana (2021)
12. Humphreys, T.: Statement on the security threat posed by unmanned aerial systems and possible countermeasures. Subcommittee on oversight and management efficiency. of the House Committee on Homeland Security, Washington DC (2015)
13. Lamprecht, J.: The pros and cons of active and passive drone countermeasures. Information Security Buzz. https://informationsecuritybuzz.com/articles/pros-cons-active-passive-drone-countermeasures/. Accessed 29 Jan 2021
14. FAA. :Register your drone. US Department of Transportation. https://www.faa.gov/uas/getting_started/register_drone/. Accessed 30 Jan 2021
15. DOJ, D.O.T., DHS: Advisory on the application of federal laws to the acquisition and use of technology to detect and mitigate unmanned aircraft systems. Department of Homeland Security, Washington DC, 9.95.300-UAS (2020)
16. Yaacoub, J.-P., Noura, H., Salman, O., Chehab, A.: Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things (2020). https://doi.org/10.1016/j.iot.2020.100218
17. Busset, J. et al.: Detection and tracking of drones using advanced acoustic cameras. SPIE 9647, Unmanned/unattended sensors and sensor networks XI; and Advanced free-space optical communication techniques and applications, vol. 96470F (2015)
18. Nguyen, P., Ravindranatha, M., Nguyen, A., Han, R., Vu, T.: Investigating cost-effective RF-based detection of drones. In: 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, pp. 17–22. ACM, New York (2016)
19. Nassar, D.: New Poll Reveals Americans' High Hopes For – But High Fears of – Drones. Hawthorn Group, Alexandria (2019)
20. Vincenzi, D., Ison, D., Liu, D.: Public perception of Unmanned Aerial Systems (UAS): A survey of public knowledge regarding roles, capabilities, and safety while operating within the National Airspace System (NAS). Embry-Riddle Scholarly Commons, Daytona Beach, FL. [Online]. (2013) Available: https://commons.erau.edu/publication/639. Accessed 14 Nov 2021
21. Lidynia, C., Philipsen, R., Ziefle, M., Eds. Droning on About Drones—Acceptance of and Perceived Barriers to Drones in Civil Usage Contexts: (Advances in Human Factors in Robots and Unmanned Systems. Advances in Intelligent Systems and Computing. Springer, Berlin (2017)
22. MITRE, "Systems Engineering Guide," The MITRE Corporation, McLean, VA (2014)
23. Boehm, B.: System Qualities (SQs) Ontology, Tradespace and Affordability (SQOTA), Phase 6: 2017-2018. Systems Engineering Research Center SERC-2018-TR-108 (2018)
24. Specking, E., Parnell, G., Pohl, E., Buchanan, R.: Early design space exploration with model-based system engineering and set-based design. Systems. **6**(45). (2018). https://doi.org/10.3390/systems6040045
25. Harvey, B., O'Young, S.: Acoustic detection of a fixed-wing UAV. Drones. **2**(1), 4 (2018). https://doi.org/10.3390/drones2010004
26. Güvenç, İ, Ozdemir, O., Yapici, Y., Mehrpouyan, H., Matolak, D.: Detection, localization, and tracking of unauthorized UAS and jammers. In: IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, pp. 1-10 (2017). https://doi.org/10.1109/DASC.2017.8102043
27. Akande, K.O., Owolabi, T.O., Twaha, S., Olatunji, S.O.: Performance comparison of SVM and ANN in predicting compressive strength of concrete. IOSR J. Comput. Eng. **16**(5), 88–94 (2014). https://doi.org/10.9790/0661-16518894
28. Endsley, M.R.: Toward a theory of situation awareness in dynamic systems. Hum. Factors **37**(1), 32–64 (1995)
29. Wang, C., Cummings, M.: A mobile alerting interface for drone and human contraband drops. Presented at the AIAA Aviation and Aeronautics Forum, Dallas TX (2019)
30. Oliveira, N., Jorge, F., De Souza, J., Junior, V., Botega, L.: Development of a user interface for the enrichment of situational awareness. in emergency management systems, vol. 491, pp. 173–184 (2016). https://doi.org/10.1007/978-3-319-41929-9_17
31. Davenport, T.H., Kirby, J.: Beyond Automation: Strategies for remaining gainfully employed in an era of very smart machines. Harvard Business Review(2015)
32. Marks, P.: How police catch drone-flying criminals. BBC. https://www.bbc.com/future/article/20170731-how-cops-catch-drone-flying-criminals. Accessed 3 Feb 2021
33. McSweeney, K.: How drone forensics can reveal pilot identity. ZDNet. https://www.zdnet.com/article/how-drone-forensics-can-reveal-pilot-identity/. Accessed 3 Feb 2021

Professor Mary (Missy) Cummings received her B.S. in Mathematics from the US Naval Academy in 1988, her M.S. in Space Systems Engineering from the Naval Postgraduate School in 1994, and her Ph.D. in Systems Engineering from the University of Virginia in 2004. An AIAA fellow, she is currently a Professor in the Duke University Electrical and Computer Engineering Department, and the Director of the Humans and Autonomy Laboratory.

Dr. Hala F. Nassar, Professor of Landscape Architecture at Clemson University, holds a BArch, MArch, and Ph.D. in History of Landscape Architecture from Ain Shams University in Cairo, Egypt, and Masters in Landscape Design from the Pennsylvania State University. Dr. Nassar is an Academy Fellow, Council of Educators in Landscape Architecture.

Vishwa Alaparthy received a Ph.D. degree in Electrical Engineering from the University of South Florida in 2018 before becoming a post-doctoral associate with the Duke Humans and Autonomy Laboratory. His current research interests include machine learning, IoT security, autonomous vehicles, and acoustic signal processing.