International Journal of Aviation, Aeronautics, and Aerospace

Volume 5 | Issue 2 Article 8

4-13-2018

Exploring Commercial Counter-UAS Operations: A Case Study of the 2017 Dominican Republic Festival Presidente

Ryan J. Wallace
Embry-Riddle Aeronautical University, ryan.wallace@erau.edu
Jon M. Loffi
Oklahoma State University - Main Campus, jon.loffi@okstate.edu
Michael Quiroga
Intelligent Drone Systems, michael@intelligentdrones.us
Carlos Quiroga
Intelligent Drone Systems, carlos@intelligentdrones.us

Exploring Commercial Counter-UAS Operations: A Case Study of the 2017 Dominican Republic Festival Presidente

Cover Page Footnote
The authors acknowledge the valuable contributions of Mr. Pablo Perez to this research project.

In 2016, the Federal Aviation Administration estimated that unmanned aircraft would balloon to more than 7 million units by 2020 (FAA, 2016). A recent census of users in the FAA's UAS Registration Database totaled 836,577 as of March 23, 2017, providing a rough barometer of domestic UAS market growth (Larls, 2017).

Research Problem

The recent proliferation of small, commercially-available UAS systems has resulted in a small but growing number of illicit activities involving this new technology. Similarly, some UAS operations are taking place in proximity to airports, critical infrastructure, national security areas, and other locations, sparking security and safety concerns. Such incidents have ignited the growth of counter-UAS businesses focused on keeping unmanned aircraft away from sensitive areas and responding to unmanned aerial threats.

An Emerging Threat

At prisons throughout the United States, UAS platforms are being used to illegally deliver illicit contraband to inmates inside. As early as 2013, Georgia law enforcement personnel arrested four individuals who were planning to use an unmanned aircraft to smuggle tobacco and cellular phones into a state prison (Craig, Susso, & Shaffer, 2016). In 2015, officials in Ohio recorded three UAS incidents at correctional facilities, all involving the delivery of narcotics (Craig, Susso, & Shaffer, 2016). Similarly, Oklahoma correctional facilities recovered a crashed UAS inside a state prison carrying hacksaw blades, cellular phone equipment, and narcotics (Craig, Susso, & Shaffer, 2016). Department of Justice records obtained by USA Today indicated more than a dozen documented incidents of drone operators attempting to deliver contraband to U.S. prisons during an unreported period (Abbasi, 2017).

A UAS was even suspected to have aided the escape of South Carolina inmate, Jimmy Causey. South Carolina Department of Correction Director Bryan Stirling, stated, "We also potentially believe that a drone was used to help him [Causey] get the contraband in to escape" (Bolster & Rivera, 2017, p. 1). According to Justin Long, a spokesman for the Bureau of Prisons, "The threat posed by drones to induce contraband into prison and other means is increasing." (Rattigan, 2017, p. 1).

Border patrol and drug enforcement personnel have identified drones are being used to facilitate narcotics smuggling over the U.S.-Mexican border. In 2015,

an unmanned aircraft carrying 6 pounds of crystal meth crashed in the border town of Tijuana, apparently overloaded from its illicit cargo (Valencia & Martinez, 2015). According to Tijuana police, the drone used GPS to send the craft to a particular, unnamed destination (Valencia & Martinez, 2015). It is estimated that the cartels have used unmanned aircraft to smuggle narcotics at least 150 times per year (Shields, 2017). Dinan (2018) highlighted the increasing frequency of unmanned aircraft smuggling, noting a four-day period in November 2017 in which border agents documented 13 separate incidents of drug-laden UAS crossings over one section of the U.S.-Mexico border. In addition to suspected smuggling, drug enforcement expert Sylvia Longmire stated, "the cartels have been using drones for surveillance"—likely to monitor and circumvent law enforcement activities (Valencia & Martinez, 2015, p. 1).

In addition to illicit activities, some UAS operations also create a public hazard. The FAA has shown an interest in counter-UAS technology due to an increasing number of unauthorized UAS operations being conducted in dangerous proximity to airports. Using data collected between December 17, 2013, through September 12, 2015, a study of UAS close encounters with manned aircraft revealed that 58.8% of the 665 reported incidents containing distance data occurred within 5 miles of an airport (Gettinger & Michel, 2015). An updated report evaluating data from August 21, 2015, to January 31, 2016, revealed that 58.8% of reported incidents containing distance data – the identical proportion from the earlier study – occurred within 5 miles of an airport (Michel & Gettinger, 2016). Unmanned aircraft are generally restricted from operating within 5 miles of an airport without providing notification to the airport operator for recreational operations conducted under 14 CFR 101 Subpart E, or without a 14 CFR 107.41 waiver for commercial UAS operations if the airport falls within airspace categorized as B, C, D, or [surface class] E (Special Rule for Model Aircraft, 2016; Small Unmanned Aircraft Systems, 2016). In 2016, the Federal Aviation Administration was directed by Congress via Public Law 114-190, to "establish a pilot program for airspace hazard mitigation at airports and other critical infrastructure using unmanned aircraft detection systems" (FAA Extension Safety & Security Act of 2016, Sec. 2206). The agency subsequently partnered with Nevada Institute for Autonomous Systems, Northern Plains Test Site, and Denver International Airport to evaluate technologies for detecting intruding UAS platforms operating near airports (Carey, 2016).

The full potential of UAS threats is still not fully understood and is an area of emerging research. Wallace and Loffi (2015) attempt to codify a generic taxonomy of currently known UAS threat categories. Just as new legitimate UAS

DOI: https://doi.org/10.15394/ijaaa.2018.1224

applications are continuing to be explored, so too are illegitimate uses of unmanned technology.

Counter UAS Overview

Counter-UAS technology can be facilitated using a wide variety of means, but focuses on two distinct processes: detection and engagement. *Detection* encompasses technology and processes necessary to detect, locate, track, and identify an unmanned aircraft. Conversely, *engagement* involves technology and actions to prevent, disrupt, disable, override, spoof [mislead], or otherwise interfere with UAS operations. Engagement may also include active measures to forcefully capture, inflict damage, or destroy the aerial vehicle. The distinction between these processes is essential, as there are no legal ramifications for conducting UAS detection, whereas significant legal hurdles exist to conducting engagement (Rupprecht, 2017).

Existing Counter-UAS Restrictions

There are several legal impediments to utilizing counter-UAS technology. The Communications Act of 1934 prohibits the use of unlicensed radio equipment such as jammers or other devices that interfere with communication, such as the UAS command link (Rupprecht, 2017). It is further prohibited to manufacture, import, market, sell or operate jamming equipment in the U.S. under 47 CFR 2.803 (Rupprecht, 2017). Finally, 18 USC section 32 imposes imprisonment or fines upon those that damage, disable, or destroy civil aircraft (Rupprecht, 2017). Operators may also be subject to liability associated with tort claims arising from the potential collateral damage, injury, or adverse effects of counter UAS activities (Rupprecht, 2017). Such liability issues may include interference caused by jamming equipment or damage or injury caused by the forced disabling of the offending unmanned aircraft.

Easing Counter-UAS Restrictions

As errant UAS operations continue relatively unabated, Congress has taken notice. In 2016, Congress passed the National Defense Authorization Act of 2017. In Sec. 1697, Congress codified new authority for military leaders to mitigate UAS threats. The statute gave relatively broad powers for the armed forces to disrupt control, intercept, seize, disable, damage, and destroy offending aircraft (Rupprecht, 2017; National Defense Authorization Act of 2017).

Rise of Commercial Counter-UAS

The security risk posed by unmanned aircraft has not gone unnoticed by commercial entities either. Stadiums and other open-air public gatherings are recognizing the need for counter-UAS activities. On November 28, 2017, Tracy Mapes was arrested after flying a small UAS over NFL game at both the Levi Stadium and Oakland Coliseum two days earlier (Gomez & Salonga, 2017). The unmanned aircraft allegedly dropped leaflets over the stands at Levi Stadium. After reviewing surveillance footage of the initial incident, law enforcement personnel anticipated the alleged perpetrator would try the same activity at the nearby Oakland Coliseum. Santa Clara Police Lt. Dan Moreno highlighted the risk of UAS operations over the crowded areas stating, "A drone can lose control and injure someone in the crowd or drop material that may be harmful. We are evaluating our security practices with state and federal authorities to make sure this doesn't happen again." (Gomez & Salonga, 2017, p. 1).

Purpose

While information is available about countermeasure technology, very little information exists about the methods used to conduct counter-UAS operations. The purpose of this study is to develop a better understanding of countermeasure tactics, techniques, procedures, and lessons learned.

Research Objectives

Researchers sought to discover information to fulfill the following research objectives:

1. Describe counter-UAS mission planning considerations.
2. Identify key tasks associated with a counter-UAS engagement.
3. Identify problems, unanticipated conditions, or lessons learned associated with counter-UAS operations.

Method

The authors employed an exploratory research approach with a *critical paradigm*. According to Creswell and Miller (2000), the critical paradigm “holds that researchers should uncover the hidden assumptions about how narrative accounts are constructed, read, and interpreted.” (p. 126).

DOI: https://doi.org/10.15394/ijaaa.2018.1224

Authors interviewed a commercial, counter-UAS organization highlighting a specific, past counter-UAS event. An unstructured interview was used to generate qualitative, descriptive data to address the research objectives. While the majority of the interview was conducted using open-ended questions, the interviewer periodically asked targeted, clarifying questions to ensure accuracy and conceptual understanding.

By qualitative procedures recommended by Creswell and Miller (2000), the authors utilized researcher reflexivity, collaboration, and peer debriefing to maintain study validity. Researcher reflexivity involves the self-disclosure of personal assumptions and biases. Further, the authors closely collaborated with participants as co-researchers when constructing the narratives and perspectives to ensure the accuracy. Additionally, the author's employed member checking to validate complex or technical information. According to Creswell and Miller (2000), *member checking* involves "taking data and interpretations back to the participants in the study so they can confirm the credibility of the information and narrative account" (p. 127). Finally, the authors sought the peer review of several UAS and security experts to assess study methodology, assumptions, and data interpretation.

Assumptions & Limitations

The following limitations and researcher assumptions applied to this project:

1. Procedures utilized by counter-UAS organizations may vary widely, and the approach used by the interviewed organization was unlikely to be representative of all such organizations.
2. The participants provided an accurate account of their experiences associated with the counter-UAS operation.
3. Depending on the counter-UAS event locale, both UAS and counter-UAS rules and regulations may not be universally applicable.
4. The researcher was unable to record the interview due to proprietary and security concerns. Instead, the interviewer took digital notes of key data points, which were assumed to be accurate.
5. The researcher was required to sign a non-disclosure agreement with the participant organization, to withhold specific proprietary or security-sensitive data. The participants agreed to provide a candid interview, which included discussion of specific unclassified, security-sensitive material to enhance researcher perspective. The participants reviewed the paper before publication and were

permitted to strike proprietary or security-sensitive text. When applicable, the researcher replaced deleted security-sensitive text with generic descriptions of the type of information withheld.

6. Technical details and specifications regarding detection and mitigation equipment were withheld for security and proprietary reasons.

Researcher Reflexivity

The primary researcher was not a research subject. The primary researcher does not have direct operational expertise with counter-UAS functions, however, has related military expertise in detection technologies. The primary researcher is seasoned in performing qualitative research related to aviation security issues, including UAS security. The researcher supports the use of counter-UAS means as a mechanism to deter, actively restrict, or mitigate unauthorized UAS operations that pose a security or safety hazard. The primary researcher further supports the enforcement of UAS restrictions and regulations via means that include the interruption, damage, destruction or seizure of a UAS in exigent circumstances of compromised safety or security caused by the UAS operator.

The secondary researcher was not a research subject. The secondary researcher does not have operational expertise with counter-UAS functions, however, has ancillary experience as an advisor for counter-UAS research projects. The secondary researcher is also seasoned in performing qualitative research. This researcher believes that counter-UAS is "much needed" and "woefully behind development." This researcher sees strong demand for counter-UAS activities to support border security, counter-narcotics, and counter-terrorism. Further, this researcher advocates for counter-UAS employment for large stadiums, high population public events, domestic security, and select law enforcement functions.

The tertiary researchers simultaneously served as both research subjects and research collaborators. These individuals have operational experience in performing counter-UAS functions in varied environments. The researchers actively participated in the FAA's PATHFINDER program. The PATHFINDER program is designed to facilitate "incremental expansion of UAS operations into the NAS" by focusing on visual line of sight over people, extended visual line of sight over rural areas, and beyond visual line of sight in rural or isolated areas (FAA, 2016, p. 1). These researchers performed five counter-UAS demonstrations to various organizations, including the U.S. Air Force, Navy, Marine Corps, Coast Guard, Secret Service, as well as a myriad of private companies. Further, these researchers conducted two operational counter-UAS missions—one international

DOI: https://doi.org/10.15394/ijaaa.2018.1224

mission included UAS mitigation, with a second domestic mission limited to detection and reporting. These researchers proactively support unmanned aircraft operations for a variety of practical functions, including security. Conversely, these researchers recognize the need for providing protection against unauthorized or hazardous UAS activities. These researchers espouse the need for counter-UAS development as a basis for UAS detection system evolution and preservation of safety in the BVLOS environment.

Results

An interview was arranged with the CEO, Chief Security Officer, and Chief Pilot from Intelligent Drone Systems (IDS), a Florida-based company specializing in unmanned systems and counter-UAS technology. The interview focused on counter-UAS activities conducted in support of the Dominican Music *Festival Presidente* conducted from November 3-5, 2017 in the Felix Sanchez Olympic Stadium, Santo Domingo, Dominican Republic.

Objective

Intelligent Drone Systems was contracted to furnish a specific security detail to conduct 72 hours of UAS detection and counter-UAS services in support of the Festival Presidente beginning on November 3, 2017, at 0800L. IDS was explicitly charged with enforcing a UAS-free zone in proximity to the performance stage contained within the main stadium and surrounding area out to 1 km [specific contract details withheld]. Figure 1 displays an approximation of team's operations area. The IDS team maintained responsibility for identifying unauthorized UAS in proximity to the exclusion area, tracking UAS craft, locating offending UAS pilots, and engaging UAS craft violating the exclusion area.

Planning

Pre-coordination was conducted with the Dominican Institute of Civil Aviation (IDAC), the Dominican Republic National Police, the Ministry of Defense, Cerveceria Nacional Dominicana (CND) [entertainment contractor], and event security service.

A site survey was conducted before the event to determine likely launch areas for possible intruding UAS platforms. The survey included an overview of the surrounding topography. The team determined that athletic fields immediately east of the stadium were most likely to be the launch site and ingress direction for unauthorized UAS flights. The team focused counter-UAS detection and

directional countermeasures to respond to threats primarily from that area. High rise buildings to the west and north were determined to be unlikely ingress routes for UAS threats due to urban obstructions, the lack of open space to launch a UAS platform, and limited visual line of sight.

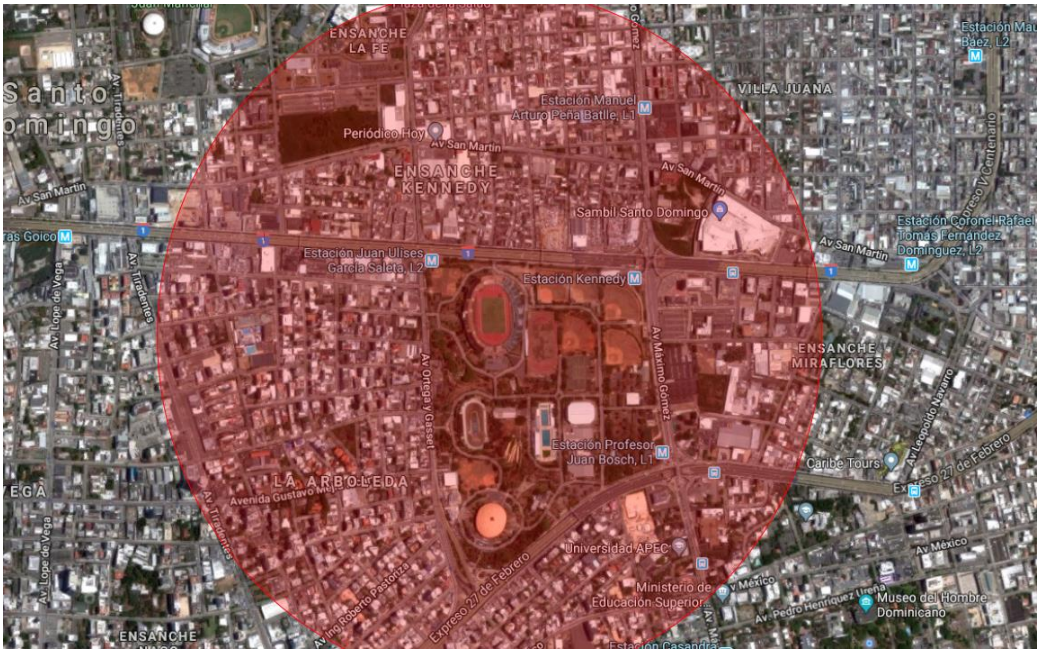

Figure 1. Felix Sanchez Olympic Stadium, Santo Domingo, Dominican Republic. IDS counter-UAS Area of Responsibility identified by red shading, extending 1 km from stadium. (Google Maps/Satellite Overlay)

Complicating the planning process, IDS was also required to coordinate and manage various UAS flights conducted by authorized vendors at the event. IDS personnel coordinated with event planners to establish a *white list* of authorized UAS flights, and documented planned UAS operations via a generic flight plan. IDS was required to monitor and ensure authorized flights complied with their flight plans and were conducted safely. IDS established takeoff and landing protocols for authorized flights, which required operators to pre-coordinate with IDS operators via a digital communications channel 30 minutes prior to scheduled launch, again just before takeoff, and immediately after landing. Initially, two companies were authorized to fly unmanned aircraft during the event.

The IDS team confirmed that IDAC had issued a Temporary Flight Restriction (TFR) for the event and coordinated with CND planners to post

numerous messages to UAS forums and social media sites advising UAS operators of flight restrictions surrounding the event and advising them to avoid the area.

Deployment

IDS deployed three members to support this operation. The *detection and engagement system operator* (DESO) led the IDS team from within the confines of the event operations center and coordinated with event operations staff. A second team member was deployed at an elevated vantage point within the stadium as an *overwatch observer* to aid in UAS visual detection. The third team member was a *mobile liaison* and deployed in conjunction with event security personnel to locate and make contact with unauthorized UAS operators.

To aid in early UAS and UAS operator detection as well as enhance overall situational awareness, the IDS team was prepared to deploy a tethered, rotary-wing UAS to provide high-angle observation. While procedures were in place to make use of tethered UAS information as needed, the team did not employ this device during the 72-hour mission execution period. The team explained that the tethered UAS was not determined to be needed during the employment period.

Communication

The team utilized two primary communication mediums. Voice communication was conducted using Zello, a push-to-talk (PTT) radio application designed for smartphones, tablets, and laptop computers. The application requires internet connectivity, either via Wi-Fi or cellular phone network. The application has a slight latency, with the voice message being delivered to the recipient after the sender releases the PTT button. The application also features user-defined channels, which can also be used to share photos, playback messages, and post to social media.

Sharing of text information was performed via WhatsApp, a digital instant messaging service for VoIP, video calls, images, documents, media, and user location that can be used on a mobile phone or computer. IDS established multiple WhatsApp channels for various functions, including authorized UAS operators, security operations channel for IDS personnel, and a master channel for liaising with event planners and security staff.

Counter-UAS Detection & Engagement System

The team utilized multiple radio frequency (RF) detectors and control signal interruption devices operated from a laptop computer in the event operations center [device manufacturer and model withheld]. The RF detection system was designed to: identify the presence of UAS communication signal parametrics, triangulate the approximate position of the UAS, and automatically display detection information on the user interface. The detection and engagement system operator could choose to monitor the UAS activity in real time or execute an electronic countermeasure that would override the communication links between the remote pilot and UAS. Depending on the UAS type and firmware, the link interruption would cause the UAS to return-to-home—its launch point--or immediately discontinue flight.

In addition to responsive interruption as detailed above, the RF system allowed for the creation of a digital geofence restricted zone that could prevent unmanned aircraft from taking off, entering a defined area, or following the remote pilot's instructions while inside the area. The effectiveness of the geofence zone was limited if the unauthorized UAS were not within initial line-of-sight of one of the four RF countermeasure system transmitters. For this event, a geofence restricted zone was established within a 5 km radius of the stadium and up to 500ft AGL. Due to the potential risks of a UAS falling abruptly and causing injury or property damage, the geofence was configured for automatic-detection and notification only. Each countermeasure was employed manually, in coordination with security, overwatch and with prior authorization from the IDAC liaison or event Chief Security Officer.

Four integrated detection sensors/interruption transmitters were initially planned for deployment, one in each of four cardinal directions from the stadium. One detector was damaged prior to mission execution due to intermittent power availability. As a result, the team was forced to remove sensor coverage from the southern sector.

The RF system was the only active UAS countermeasure system used during the mission. The IDS team did not plan to utilize any form of kinetic engagement to disable unmanned aircraft in the event the RF countermeasure system was ineffective. In the unlikely event, the countermeasure system was ineffective at disabling an unauthorized UAS, the IDS team would report information about the offending UAS and defer action to the event's Chief Security Officer and IDAC liaison.

DOI: https://doi.org/10.15394/ijaaa.2018.1224

Engagement Cycle

IDS personnel established an identification matrix to determine the identity, location, status, and disposition of detected UAS platforms. An overview of the identification matrix is presented in Figure 2. Upon initial detection, the detection and engagement system operator would verify that the UAS operation was not an authorized operation by comparing the parameters against authorized flight plans and coordinated with authorized UAS pilots via WhatsApp.

If the operation was determined to be unauthorized, the detection and engagement system operator reported the cardinal direction of the unknown UAS to the overwatch observer via Zello for visual confirmation and tracking. The mobile liaison was deployed via Zello in conjunction with an event security officer to locate the UAS and UAS operator, receiving supplemental location updates from the overwatch observer. Once the overwatch observer visually located the intruding UAS, he would determine if the craft was within the authorized engagement zone of 1 km from the event site. Additionally, he would perform a visual risk assessment of the ground area below the UAS to determine if the device could be safely disabled without causing injury to people or damage to unprotected structures or property. If the overwatch observer deemed the engagement safe, he would report his findings to the DESO. The DESO would then coordinate with the IDAC or event Chief Security Officer on duty to obtain permission to electronically disable the intruding UAS. If approved, the mobile liaison and accompanying event security officer would proceed to the UAS location to investigate the crash site and secure the unmanned vehicle [if UAS discontinued flight], or follow the UAS back to its launch location [if the UAS returned-to-home]. If the pilot was located, the mobile liaison deferred further action to the event security officer, who had the discretion to arrange an arrest or expel the operator from the event.

Engagement Results

During the contract period, the IDS team detected 23 total UAS events in the exclusion area. Of the 23 events, 15 were unauthorized. Three unauthorized incursions occurred during daylight hours, one incursion occurred during local civil twilight, and 11 incursions occurred at night.

The team responded to all 15 unauthorized events. The IDS team leveraged geofence notifications four times and employed countermeasures preventing or limiting exclusion zone incursions. Electronic counter-measures (ECM) interrupting pilot UAS control was employed during eight incursions. No action was taken during two of the events since the UAS crashed during one event, and

the UAS was unable to be visually located during the second. Event security was dispatched during one event, and an authorized pilot was erroneously detained, with the offending unauthorized pilot escaping backstage before security could intervene. Two unmanned aircraft were confiscated during the event. The confiscated platforms were both DJI products and included Phantom and Mavic models.

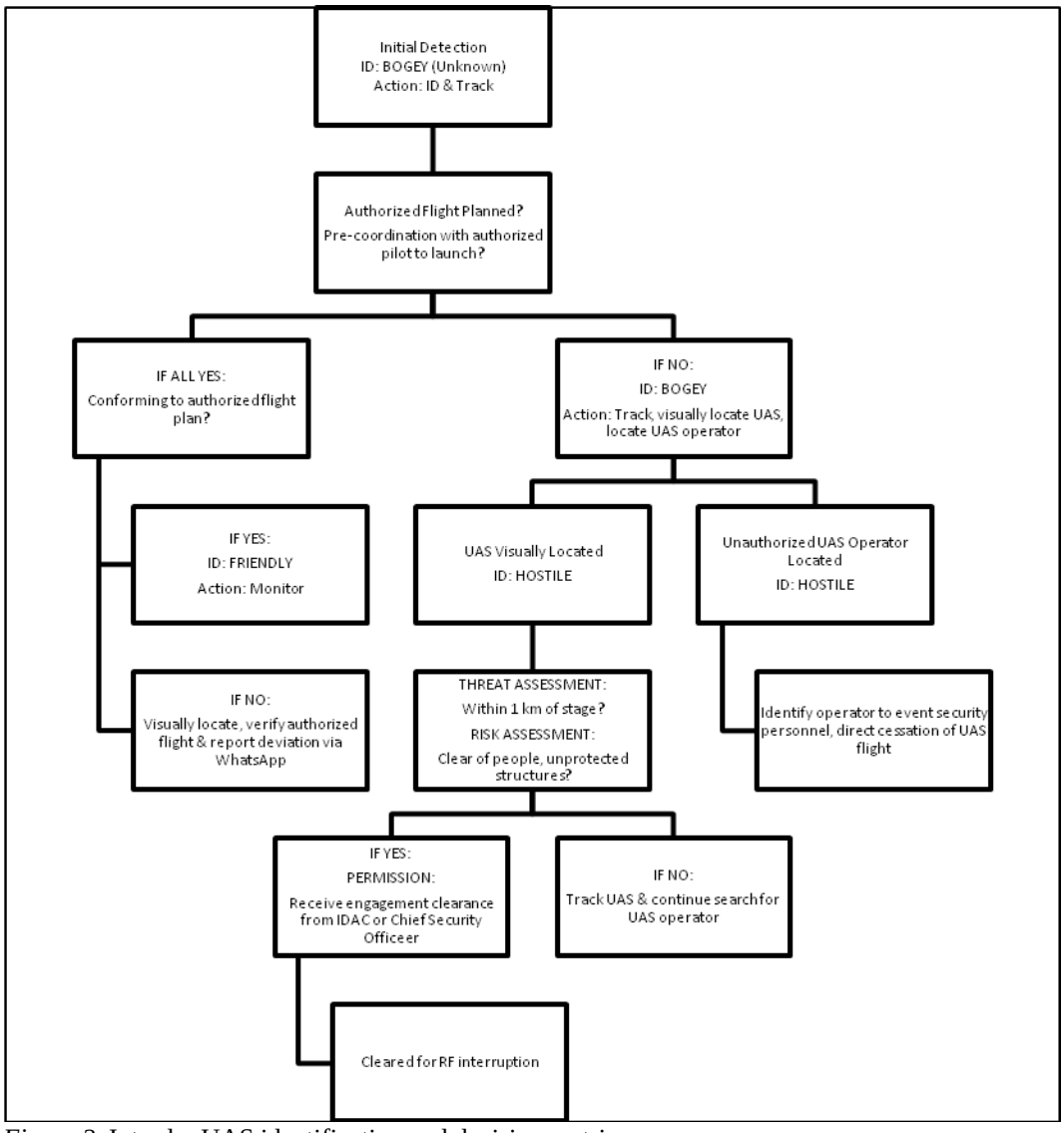

Figure 2. Intruder UAS identification and decision matrix.

DOI: https://doi.org/10.15394/ijaaa.2018.1224

Eight authorized UAS flights were conducted by two companies. One authorized pilot was de-certified for flight after deviating from an established flight plan, failing to coordinate launch with IDS personnel, and performing a flight over the gathered crowd within the exclusion zone on November 3. An overview of incursion and countermeasure employment activity is contained in Figure 3. Details and engagement notes are contained in Appendix 1. A visual depiction of a visually-spotted UAS are displayed in Figures 4 and 5.

Figure 3. UAS activity locations, November 3-5, 2017. (Google Maps/Satellite Overlay)

Figure 4. Intruding, daylight UAS flight; spotter facing southeast.

DOI: https://doi.org/10.15394/ijaaa.2018.1224

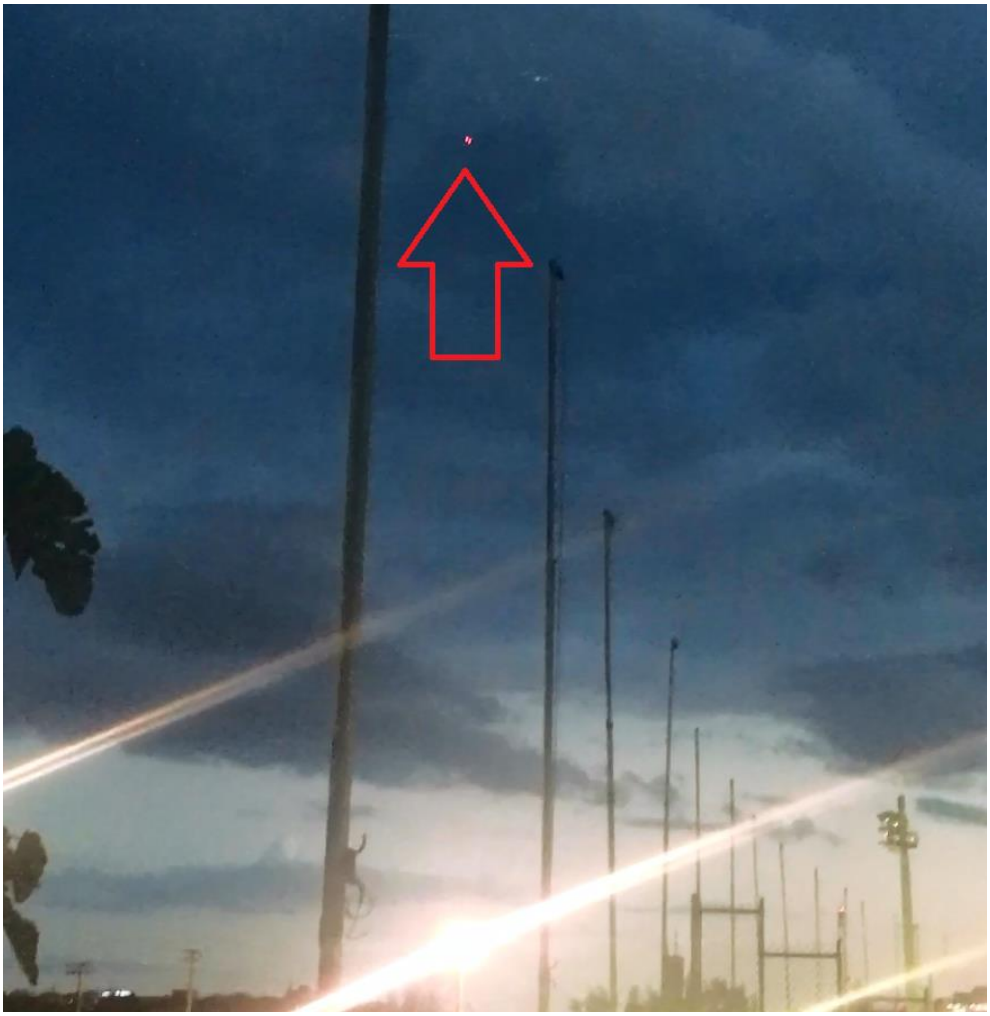

Figure 5. Authorized nighttime UAS flight; spotter facing east-southeast.

Discussion

As evidenced by the multiple lessons learned, it is clear that the commercial counter-UAS field is still very much evolving to discover the best tactics, techniques, and procedures to employ against UAS threats.

During this event, the IDS team solely employed an RF countermeasure system, which proved effective against the intruding, consumer-grade UAS platforms. It is unknown based on the collected data how the RF countermeasure system would have fared against a homebuilt UAS. In this particular case, it is highly likely that the preponderance of UAS intruders were hobbyists, interested in capturing video of the noted, national event. Based on the reported UAS incidents,

it seems unlikely that any of the platforms were being used maliciously to carry out criminal activities or cause substantial harm.

Describe counter-UAS mission planning considerations

The IDS team highlighted the importance of the mission planning process when preparing to conduct counter-UAS activities. Based on the provided data, researchers suggest that the following considerations be taken into account when performing counter-UAS operations:

Identify Mission Objectives:	Determine primary mission objectives such as area or target to be protected, duration, and other requirements.
Site Survey:	Conduct site survey to determine likely areas of UAS launch, ingress, & egress routes. Correlate site locations with established NOTAMS/TFRs, etc. Determine areas where UAS-disabling mitigation strategies would be hazardous (areas of vehicular traffic, crowded areas, etc).
Observation Point Selection:	Determine areas of best visibility for UAS visual detection. Consider sun positioning, background contrast, and lighting. Establish visual landmark references & determine the distance to aid in threat distance estimation and coordination.
C-UAS Equipment Deployment:	Determine line of sight for RF detection & interruption equipment. Determine equipment deployment limitations, based on logistical requirements (availability of electricity, control cord length, communications coverage, etc.). Identify likely coverage gaps based on equipment capabilities & effectiveness.
Probable Threat Assessment & Taxonomy:	Identify possible threat platforms based on probable threat intent (attack, video recording, hobbyist flight, etc), consumer availability, prior encounter experience, local knowledge, environmental favorability (i.e. open areas are favorable to fixed-wing UAS, whereas obstacle-dense areas are not).
Risk Assessment/Risk Tolerance:	Determine risk tolerance to protected target. Codify measurable criteria to determine risk elevation (standoff distance, UAS type, size, speed, etc). Establish risk assessment matrix.
Identification Matrix Development:	Determine means to identify authorized vs. unauthorized UAS flights. Integrate elevated response matrix triggers based on risk tolerance and risk assessment.

DOI: https://doi.org/10.15394/ijaaa.2018.1224

Mitigation Selection:	Determine primary (and if applicable) secondary or tertiary mitigation mechanisms for UAS threats. Ensure appropriateness and effectiveness of mitigation strategies to anticipated threats. Determine how the employment of various mitigations will be determined. Determine engagement authority and coordination requirements, if required.
Communications Plan:	Identify communications requirements modalities and limitations. Establish primary (and secondary) means of communication. Codify coordination plan for authorized UAS flights. Articulate communications purpose and information flow. (should be responsive to who, what, where, when why, how communication should occur)
Coordination Plan:	Identify how C-UAS activities integrate into overall security plan. Describe capabilities response plan to decision-making authorities and other stakeholders. Determine coordination requirements.
Social Media & Public Information:	Identify means of public information dissemination, including the applicability of TFRs, NOTAMS, etc. Identify how information will be disseminated and how communications modalities will be monitored and responsive to public inquiry.

Figure 6. Proposed counter-UAS mission planning tasks. The authors acknowledge that the planning task list does not address every conceivable task associated with counter-UAS operations, but rather captures and codifies key planning elements represented in the collected interview data.

Identify key tasks associated with a counter-UAS engagement

Based on perceptions provided by the research participants, the authors codified a proposed model for key tasks associated with counter-UAS engagement. This model contained in Figure 7 can be used by commercial counter-UAS organizations to facilitate threat mitigation in a concerted, safe, and systematic manner.

Detection:	Detect unauthorized UAS operation.
Track:	Fix location, speed, course, altitude and track visually or via other means.
Threat Assessment:	Confirm regulatory or airspace violation and threat potential of UAS system.
Search:	Conduct hasty search for UAS operator; if found, communicate requirement to disengage activities and land UAS.
Identification:	Determine identification of brand/model of UAS [if possible].
Evaluate:	Evaluate UAS brand/model vulnerabilities

Selection:	Determine appropriate countermeasure/mitigation system to engage UAS.
Situational Analysis:	Evaluate situation and environment to determine hazards or potential collision effects of engagement.
Risk Assessment:	Determine risk level associated with performing an engagement. Balance engagement decision based on measured risk and likely collateral effects.
Decision:	Make engagement decision.
Engagement:	Perform engagement.
Effectiveness:	Determine effectiveness of countermeasure/engagement strategy. Confirm if UAS threat has been neutralized or disabled. If ineffective, return to Evaluate step.
Disengagement:	Discontinue employment of countermeasure system.
Locate:	Locate UAS platform or wreckage.
Examine:	Examine UAS for collateral threats or effects (i.e. attached IED, CBRNE, HAZMAT, fire, etc).
Respond:	Respond to collateral threats or effects.
Investigation:	Collect applicable evidence, including scene photos, UAS identifying markings, testimony of witnesses or other relevant information.
Secure:	Secure the UAS platform, as appropriate.
Enforce:	Locate and report/coordinate detainment/citation/trespass offending individual, as appropriate.
Document:	Document threat, circumstances, engagement, results, and investigation findings.
Report:	File applicable reports with appropriate agency or jurisdictional authority.
Reconstitute:	Reequip for subsequent response or engagement, as required.

Figure 7. Proposed engagement model for counter-UAS actions. Note: This recommended engagement matrix provides a holistic approach to counter-UAS response. This model represents a long-chain decision-making process whereby risk level is relatively low and the responders do not hold indigenous engagement authority. The authors acknowledge that there may be good justification to hasten or even skip certain steps, based on situational conditions, the relative severity of the threat, and timeliness of response.

Identify problems, unanticipated conditions, or lessons learned associated with counter-UAS operations

The IDS team reported that access to reliable electrical power presented a challenge for the operation. Intermittent power to the RF detectors/control signal interruption device caused significant damage to one of the four deployed devices, requiring equipment repair and replacement that could not be performed in the field. This setback required the IDS team to prioritize countermeasure coverage, focusing on vectors of likely UAS incursions. The team stated that robust surge protectors will be included in their future deployment kit to prevent damage to sensitive computer and countermeasure equipment. Moreover, the loss of equipment

DOI: https://doi.org/10.15394/ijaaa.2018.1224

underscores the importance of having reliable equipment redundancy or viable alternatives available.

Additionally, interrupted or unreliable WI-FI coverage limited the team's ability to perform digital updates to the RF detection/control system. Additionally, the lack of reliable WI-FI coverage also forced the team to rely more heavily on cellular phone data for communications and other internet needs. The team plans to acquire alternative communication means that can serve as a backup in the event of limited or interrupted wireless internet connectivity.

The IDS over watch experienced intermittent difficulty visually locating UAS platforms—particularly at night. See Figure 5. During most night UAS encounters, UAS platforms were well illuminated by integrated position lighting, however, on at least one occasion these lights were intentionally obscured or disabled by the operator, likely to avoid visual detection. As a result, the IDS team plans to acquire a monocular night vision device to aid the overwatch observer in spotting unlighted UAS craft. Additionally, the team also plans to include traditional binoculars in its future deployment kit to augment daytime visual detection. Moreover, there may be cause to suggest the need for additional manpower allocation to this critical function to put "more eyes on more sky."

During the event, the RF countermeasure device was accused of causing interference with the event's ticket scanners. However, this interference was never validated. The team suggested that in the future, further efforts will be given to identifying potential collateral EM spectrum interference problems.

The team stated that additional onsite preparation time would have been helpful. The team explained that further coordination with authorized pilots could have streamlined the flight authorization process.

Finally, the team highlighted the importance and effectiveness of social media engagement. The entertainment contractor's prominent social media presence and advisory message postings advising UAS operators to remain clear of the venue played a significant role in deterring unauthorized UAS activity.

Conclusions

As the literature review suggests, unmanned threats are continuing to evolve in application, scope, and complexity. In January 2018, the Russian military reported a swarm attack of crudely-designed, weaponized unmanned aircraft on two of its bases in Syria (Daniels, 2018). Reportedly, Russian air defenses detected 13

"small size air targets" inbound to its bases and successfully engaged them with anti-aircraft and electronic-countermeasures (Daniels, 2018, p. 1). As cited in Daniels (2018), political scientist and terrorism expert Colin Clarke underscored the attack as a wakeup call, urging:

> The U.S. and other nations have a lot of thinking to do about how to deal with the weaponized drone technology because it could be used not just on the battlefield but potentially in urban areas by organized terrorist groups and other bad actors (p. 1).

The overall lack of available literature calls attention to the need to develop further and refine tactics, techniques, and procedures for countering UAS threats. The preponderance of unanticipated setbacks and lessons learned derived from the presented case study suggests that adequate best practices are still very much in the infancy of development. The findings of this study should not be interpreted as conclusive, but rather as a basis of deviation for additional research, exploration, and discussion.

Although not directly studied, participant comments suggested that existing legal and regulatory roadblocks preventing the use of active, counter-UAS mitigation measures in the U.S. may discourage counter-UAS development and place the country at a disadvantage in effecting UAS security. While political leaders have made recent positive steps to rectify this deficiency through more permissible legislation, the remaining legal hurdles are likely to continue curtailing counter-UAS development.

This research project codifies merely one approach to effecting counter-UAS operations. No doubt, there are many more viable and perhaps more effective means of mitigating unmanned aircraft threats. Perhaps the most important conclusion that can be gleaned from this study is the glaring need for additional research in this highly fluid, evolving field.

DOI: https://doi.org/10.15394/ijaaa.2018.1224

References

Abbasi, W. (2017). Inmates fly mobile phones, drugs and porn into jail – via drone. *USA Today.* Retrieved from https://www.usatoday.com/story/news/2017/06/15/inmates-increasingly-look-drones-smuggle-contraband-into-their-cells/102864854/

Bolster, K. & Rivera, R. (2017). Prison employee fired after inmate escapes from Lieber Correctional. *WSMV.* Retrieved from http://www.wsmv.com/story/35816591/scinmate-captured-in-texas-with-guns-cash-phones-drone-may-have-aided-escape

Carey, B. (2016). FAA will evaluate 'Counter-UAS' technology at Denver Airport. *AIN Online.* Retrieved from https://www.ainonline.com/aviation-news/aerospace/2016-11-09/faa-will-evaluate-counter-uas-technology-denver-airport

Craig, T.R., Russo, J. & Shaffer, J.S. (2016). Eyes in the skies: the latest threat to correctional institution security. *Corrections Today.* Retrieved from https://www.justnet.org/pdf/Craig-Russo-Shaffer.pdf

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into Practice, 39*(3), 124. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/218779368?accountid=27203

Daniels, J. (2018). Russia says it killed rebels behind swarm drone attack in Syria, but experts see more such strikes ahead. *CNBC News.* Retrieved from https://www.cnbc.com/2018/01/12/russia-says-it-eliminated-rebels-behind-swarm-drone-attack-in-syria.html

Dinan, S. (2018). Thirteen drones in four days: How drug smugglers are using technology to beat Border Patrol. *Washington Times.* Retrieved from https://m.washingtontimes.com/news/2018/jan/2/drones-fly-drugs-us-no-border-patrol-detection-tec/

FAA Extension, Safety, and Security Act of 2016, Pub. L. 114-190, 130 Stat. 615 codified as amended at 49 U.S.C. §§ 40101

Federal Aviation Administration. (2016). Focus area Pathfinder Program. Retrieved from https://www.faa.gov/uas/programs_partnerships/focus_area_pathfinder/

Gettinger, D. & Michel, A.H. (2015). Drone sightings and close encounters: An analysis. *Center for the Study of the Drone at Bard College.* Retrieved from http://dronecenter.bard.edu/drone-sightings-and-close-encounters/

Gomez, M. & Salonga, R. (2017). Man suspected of flying drone over 49ers, Raiders games arrested. *Security Info Watch.* Retrieved from http://www.securityinfowatch.com/news/12383982/man-suspected-of-flying-drone-over-49ers-raiders-games-arrested

Larls, M. (2017). John Taylor fought the FAA over registering drones and won, but now what. *Washington Post.* Retrieved from https://www.washingtonpost.com/local/trafficandcommuting/john-taylorfought-the-faa-over-registering-drones-and-won-but-now-what/2017/05/29/56b83bf8-416a-11e7-adba394ee67a7582_story.html?utm_term=.6e4b6090ca17

Michel, A.H. & Gettinger, D. (2016). Analysis of new drone incident reports. *Center for the Study of the Drone at Bard College.* Retrieved from http://dronecenter.bard.edu/analysis-3-25-faa-incidents/

National Defense Authorization Act of 2017, Pub. L. 114-328, 130 Stat. 2000.

Rattigan, K. (2017). DOJ reports on drones flying contraband to prisons. *Data Privacy & Security Insider.* Retrieved from https://www.dataprivacyandsecurityinsider.com/2017/06/doj-reports-on-drones-flying-contraband-to-prisons/

Rupprecht, J. (2017). 7 big problems with counter-drone technology (drone jammers, anti-drone guns, etc.). *Rupprecht Law.* Retrieved from https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems

Small Unmanned Aircraft Systems, 14 C.F.R. § 107 (2016).

Special Rule for Model Aircraft, 14 C.F.R. § 101E (2016).

DOI: https://doi.org/10.15394/ijaaa.2018.1224

Valencia, N. & Martinez, M. (2015). Drone carrying drugs crashes south of U.S. border. *CNN*. Retrieved from http://www.cnn.com/2015/01/22/world/drug-drone-crashes-us-mexico-border/

Wallace, R.J. & Loffi, J.M. (2015). Examining unmanned aerial system threats & defenses: A conceptual analysis. *International Journal of Aviation, Aeronautics, and Aerospace*, 2(4). Retrieved from https://doi.org/10.15394/ijaaa.2015.1084

Appendix 1

Summary of UAS Activity, Response, & Disposition

DTG	Status	Response	Disposition
031755	Unauthorized	None	UAS detected & crashed
032020	Authorized	None	N/A
032049	Authorized	Pilot Grounded	Authorized pilot deviation from flight plan
032154	Unauthorized	Geofence	Unable to employ countermeasures due to crowd proximity; performed GPS Jamming; UAS RTH; Tracked back to operator
032256	Unauthorized	ECM	UAS landed 200' outside stadium; Notified security
030022	Unauthorized	Geofence	UAS RTH; operator located outside perimeter
030216	Unauthorized	Geofence	UAS RTH
041211	Unauthorized	None	UAS detected; unable to rectify
041755	Authorized	None	TV UAS crew; duration 15 mins
041939	Authorized	None	TV UAS crew; duration 10 mins
041952	Unauthorized	ECM	UAS detected; no visual contact; Presumed unable to initiate launch
042005	Unauthorized	ECM	UAS detected; visually spotted flying low over crowd; ECM initiated; landed 1800' west of stadium
042012	Unauthorized	ECM	UAS detected; visually spotted high altitude flight pattern; ECM initiated; RTH westbound
042016	Unauthorized	ECM	UAS detected; visually spotted UAS launch from VIP tower; descended near stage; UAS secured by spotter/ ID'd operator; referred to security
042053	Authorized	None	TV UAS crew; duration 11 mins
042122	Authorized	None	TV UAS crew
042145	Authorized	None	TV UAS crew
042212	Authorized	None	TV UAS crew

DOI: https://doi.org/10.15394/ijaaa.2018.1224

DTG	Status	Response	Disposition
042237	Authorized	None	TV UAS crew
042348	Authorized	None	TV UAS crew
051656	Authorized	None	TV UAS crew; duration 28 mins
051744	Unauthorized	ECM	UAS detected; visually spotted 2 mi east of stadium; ECM initiated; uncontrolled descent; security unable to locate
051808	Unauthorized	ECM	UAS visually spotted 1 mi west of backstage; ECM initiated; UAS crash landed outside perimeter
051927	Authorized	None	TV UAS crew; duration 16 mins
051959	Unauthorized	Geofence	4x UAS detected; UAS platforms RTH
052112	Authorized	None	TV UAS crew
052322	Unauthorized	ECM	UAS spotted by TV crew; authorized UAS landed; ECM initiated; landed outside northeast stadium
052328	Unauthorized	Security dispatched	Erroneously detained authorized UAS operator; unauthorized operator recovered downed UAS and escaped backstage