Thinking Rather than Panicking about the Current Drone Threat

Dr. Tom Foley & Dr. Tyrone Groh

College of Security and Intelligence, Embry-Riddle Aeronautical University

A Paper Presented at the

Aviation, Aeronautics, and Aerospace International Research (A³iR) Conference

Phoenix, AZ

January 17, 2015

Thinking Rather than Panicking about the Current Drone Threat

Drones pose a number of threats to venues with large crowds. To better prepare and respond to these threats, the problems drones may cause should be broken down to allow different actors with different interests to develop different strategies for dealing with these threats. To maximize efficiency and effectiveness, the variety of strategies should be complementary and synergistic. This document seeks to establish different strategies for the interested parties and provide some insight for how to formulate and operationalize counter-drone strategies.

Before delving into what should be done, it is important to consider first the desired outcomes for those involved. With respect to large venues and the organizations that depend on them, the goal of a counter-drone strategy is to stop or mitigate the use of drones that could *unintentionally* damage infrastructure or harm spectators/participants. Those involved should focus on stopping those that could unintentionally cause harm based on the logic that it is the *most likely* threat. Focusing on the *most dangerous* threat for sport or entertainment venues enters a realm where the costs of pursuing such a strategy far exceed the capabilities of those involved and does not match the benefits gained. Ultimately, the goal of a counter-drone program is ensure that sport and entertainment venues appear safe enough to encourage people to return after an event occurs. Trying to prevent those with the intention to cause damage or harm simply falls outside the scope of those responsible only for venue security and must remain within the domain of those responsible for law enforcement and counter-terrorism operations.

For law enforcement and counter-terrorism agencies, the goal is to prevent or mitigate the effects of drones when intentionally used to create damage or harm; these agencies must focus on both the most likely and the most dangerous threats. Law enforcement and counter-terrorism agencies must also balance their activities to cover both possibilities and consider far more complex scenarios to avoid becoming overly focused on one possibility and getting blind-sided by another. For example, a terrorist network that wishes to target a large venue could realistically use drones as a diversion for a much larger attack. As another example, drones could just be one part of a complex operation, such as providing surveillance for a group of operatives attempting to conduct an act of terror.

It is important to note that there are two desired goals surrounding venue security: 1) stopping the use of drones before they cause damage or harm, and 2) mitigating the effects should a drone cause, or threaten to cause, damage or harm. Most importantly, venue security must balance their efforts to ensure they do not appear too lax or too restrictive/paranoid. A guiding question for all operations should be "Will people feel comfortable bringing loved ones to the venue?" If an incident occurs and the response is perceived as efficient and effective, people will likely remain willing to attend future events. Operations designed to create effective and efficient responses to unintentional acts will also serve well should an intentional attack occur. This is where venue security can create a necessary synergy with law enforcement and counter-terrorism operations designed to mitigate the effects of an intentional attack.

Risk Assessment

Risk is the most important consideration when deciding how best to manage the problem of drones at public events. Careful consideration of the threats, vulnerabilities, likelihood of occurrence, and consequence will result in better decisions regarding risk management strategies. The best risk management strategies are cost-effective, feasible, and reasonable. There are four risk management strategies: [1]

1. Risk Avoidance – Eliminating risk by cancelling an event

2. Risk Control – Implementing measures to reduce the likelihood or consequences of an incident

3. Risk Acceptance – A decision not to implement countermeasures because of low likelihood or the cost of the countermeasures exceeding the benefits derived from those countermeasures.

4. Risk Transfer – Shifting some or all of the risk to another entity (e.g., insurance)

Risk avoidance is an extreme risk management strategy that will only be justified in the presence of extreme risk. At this time, given the size, range, and payload capacity of civilian drones risk avoidance should only be considered when there is specific, credible intelligence that an attacker

1. *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*, (Washington, D.C.: U.S. Department of Homeland Security, 2011), 23.

intends to use a drone to deliver a nuclear, radiological, chemical, or biological payload capable of causing mass casualties and has the ability to do so. Mere desire is insufficient to justify risk avoidance or implementation of extreme countermeasures. Risk control will be the most common risk management strategy to address the risk drones pose to public events.

Threat assessment is the first step in the risk assessment process. Considering drone use at a public event as single threat will lead to inefficient, ineffective, and wasteful use of security resources. The threat is the operator of a drone, not the drone itself. A potential drone operator's skill level, intent, motivation, and incentive to fly a drone over a large outdoor venue will influence risk as well as the selection of appropriate countermeasures. Categorizing drone operators by intent is critical to choosing appropriate and cost-effective countermeasures. The two threat categories for drone operators are malicious and non-malicious.

Malicious Drone Operators

Malicious drone operators intend to use a drone to kill, injure, or frighten people or to disrupt the event. They will be politically, religiously, or ideologically motivated. These operators pose the greatest threat, but are the least likely to materialize since there are much easier, reliable, and effective means of achieving these goals. Shooting into a crowd queuing at the entrance to a venue is easier and will likely cause more casualties and chaos than a small quad copter with a three to five pound explosive device payload. Fragmentation injuries are the most common cause of injury and death in open-space explosions.[2] To maximize the number of casualties, an attacker would need to add shrapnel to the device requiring a compensatory reduction in explosive weight used in the device because of drone payload limitations.[3] In addition, the attacker would have to maintain visual observation of the drone or mount a camera on the drone in order to fly it to the target. Direct visual observation will require the attacker to be inside the venue. Banning drones within the venue and screening attendee at venue entry points will eliminate this threat. Flying a drone into the venue, or "into the bowl," from outside the stadium will require the drone to carry a camera, requiring further reduction in the weight of the explosive device. Furthermore, it is possible to eliminate the risk of a drone flying into a retractable dome stadium by closing the

2. Sidney B. Brevard, Howard Champion, and Dean Katz, "Weapons Effects: Chapter 2," 57.

3. Ibid., 56.

dome. These technical limitations reduce the viability of using current civilian drone technology as an effective weapon delivery system.[4]

Malicious drone operators will be difficult to deter, and risk control efforts for this threat should focus on quickly and efficiently responding to the incident, treating the injured, and crowd control. How the event organizer and first responders handle such an incident will have a great impact on public perceptions of safety at large outdoor events.

Developing technologies to counter or shoot down a small drone may have unintended consequences that are as bad as, or worse than, the consequences of a small drone attack. Jamming radio frequencies to interfere with an operator's ability to control the drone would require FCC approval and may interfere with the public's ability to use their cellular phones. This could prevent attendees from calling for help or to report suspicious activity.[5] Since 71 percent of 911 calls are placed from cellular phones,[6] the consequences of jamming activity that impairs the public's ability to request emergency assistance may exceed, or add to, the consequences of a small drone terror attack. Public backlash over having their phones jammed and First Amendment litigation may also arise because of jamming.

Shooting a drone down or hacking its radio link to assume control of the aircraft also poses problems. First, in the case of a shoot-down, debris or errant bullets may hit innocent parties on the ground. Hacking into the drone to take control may likely shift legal liability onto security personnel should the drone crash into the crowd and cause injures.

Non-malicious Drone Operators

Non-malicious operators are hobbyists, photographers, videographers, or fans who do not intend to cause harm or disruption and are using a drone to take photographs or record video of the event from a unique angle or perspective. These operators pose a lesser threat, but are the most likely to materialize. The primary threat posed by non-malicious drone operators is spectator

4. While these factors may reduce the risk of a drone attack on a crowd to cause mass casualties they do not reduce the risk of a drone being used for a targeted assignation of a high profile individual. See https://www.youtube.com/watch?v=qKV6g47hgRs

5. Federal Communications Commission, "Enforcement Advisory No. 2011-04," https://apps.fcc.gov/edocs_public/attachmatch/DA-11-250A1.pdf.

6. "Guide: 911 Wireless Services," http://www.fcc.gov/guides/wireless-911-services.

injury caused by an unintentional crash of the drone. The consequences of such a crash are likely to be minor. For example, a drone crash into crowded stands at Virginia Motorsports Park caused "very minor" injuries to five people.[7]

While the injuries sustained by spectators at the Virginia Motorsports Park were minor, the potential for spectator injury is of significant concern, especially for event organizers. Public perception of drone crash incidents at outdoor venues may eventually result in lower attendance if people fear they cannot attend a ballgame, race, or other large outdoor event without the risk of drone hitting them. Thus for both safety and business reasons, strategies must be developed to address the problem of non-malicious drone operators. Reducing or eliminating the number of non-malicious drone incidents will make malicious drones more obvious and easier for security personnel to identify imminent threats.

Strategy and Operations to Prevent or Mitigate Unintentional Damage or Harm

Two particular strategies should guide security operations: deterrence and compellence. The predominant strategy is deterrence. Deterrence guides operations that will keep drone hobbyists from unintentionally creating a dangerous situation. Several different actions will support the deterrence strategy. First and foremost, venue security should partner with local law enforcement and other involved agencies—primarily the Federal Aviation Administration (FAA)—to educate the public about the dangers and penalties associated with using drones in the vicinity of large venues.

At this time, non-malicious drone operators pose the greatest risk to large outdoor public events because of the likelihood they will materialize and the increasing frequency of non-malicious drone flights over public venues. Since this group of operators is motivated by personal or commercial gain, deterrence will be an effective preventative measure. Criminal and civil prosecutions will be powerful deterrents if the penalty (cost) exceeds the gain (benefit) to the non-malicious drone operator. Federal, state, and local statutes and ordinances should be created to impose stiff financial penalties and possible incarceration for flying a drone over a crowd of people. Any state or local law should supplement federal regulations. All local statutes,

7. Martin Weil, "Drone Crashes into Virginia Bull Run Crowd," http://www.washingtonpost.com/local/drone-crashes-into-virginia-bull-run-crowd/2013/08/26/424e0b9e-0e00-11e3-85b6-d27422650fd5_story.html.

ordinances, or regulations must be written to allow drone use at public events with preauthorization from the event organizers and the FAA.

The process of educating the public should focus both on deterring hobbyists from engaging in dangerous activities and informing/incentivizing the public to aid in preventing or mitigating such activities. For example, a venue can post physical signs in areas most conducive to launching and recovering drones that forbid the operation of drones; those same signs can also provide information on how to notify authorities that illicit activities are occurring. As an additional incentive, venues could offer small rewards, such as free admission for a future event, to further incentivize people to take the time to alert authorities.

To be more effective, education should include how current civil and criminal laws affect drone operations. Deterrence of non-malicious drone operators will be most effective if irresponsible drone operators are caught while flying the drone, are immediately cited or arrested, and quickly prosecuted. Local law enforcement is better able to prosecute these types of cases quickly than the FAA because of the availability of resources.

A second facet of education involves the use of social media. Those responsible for managing venues, as well as those that use them, could engage in open source intelligence to gauge the level of drone activity and to find the websites or applications that are most used to post information about drone activity. These websites should then be used to educate people about the risks inherent in operating drones in the vicinity of large gatherings. For example, a video could be posted to any website or app specifically designed to show pictures or videos (e.g., YouTube, Instagram, Facebook) of the drone crash that injured five people in a crowd at an event in 2013 (https://www.youtube.com/watch?v=law1SsMtg_g). To make these posts more of a deterrent, the video should include information about the civil and criminal charges levied against the operator. In addition, the key words posted with such a video should specifically include “drone” and “DIY.” Another opportunity for education using social media is to put advertisements on Amazon or other web-based retail sites that provide warnings about the risks involved with operating drones (a term that should include any type of remotely controlled aircraft).

A third facet that can augment education and contribute to overall deterrence is to map out likely areas for launch, recovery, and operation. Maps should include overlays of different

potential operating ranges and limitations. For example, ranges based on battery life, fuel capacity, and speed could be combined with line-of-site restrictions and, if warranted, an electro-magnetic spectrum assessment. Although this type of information would most likely come from either law enforcement or counter-terrorism agencies, there are other potential sources such as universities with classes that specialize in physical security. Such a map with the overlays described could be done well in advance and should indicate the most likely areas for drone operation. To expand awareness and education, signs should be posted at these locations to clearly explain the violations and penalties associated with the illicit use of drones. Further, the signs should provide details on how to report such activity and indicate that potential rewards are available. Lastly, it is important that these maps be updated regularly to include changes in the surrounding environment.

The second strategy focuses on compellence. Under normal conditions when threat assessments indicate low risk for terrorist activities, venues and law enforcement can rely on the public to report suspicious drone activities. Under periods of higher threat, such as a particularly popular event (NFL Super Bowl, MLB All-Star Game, post-season events, etc.), law enforcement or venue security teams can post trained individuals in the likely areas for drone launch and recovery operations. If a person is found conducting illicit, but not nefarious, drone flights, then security or law enforcement personnel should be trained how to facilitate the recovery of the drone without causing further danger.

Strategy and Operations to Prevent or Mitigate Intentional Efforts to Cause Damage or Harm

Although law enforcement and intelligence agencies provide the largest efforts to prevent or mitigate terrorist activities, venues and the organizations that rely on them can augment those efforts using a two-pronged deterrent strategy. The first focuses on response. If venue security incorporates robust response measures, then that particular venue will not appear as soft of a target. Venues are typically viewed as a soft target, meaning that it is not too difficult to bypass security to conduct an attack. Even more desirable, large venues make it easier to avoid detection. Therefore, response must include two different aspects: response after an attack has occurred and response after a drone has been detected. If post-attack response measures can

prevent mass panic and create the perception of order and control, then the target will not appear as worthwhile.

Creating and exercising post-attack response measures poses a significant challenge; it is difficult to train venue security personnel for a real event, mostly because simulations would require significant expense. One way to overcome this challenge is for venues to offer a reduced price or free admission for a particular section of the venue that will take part in a post-attack response exercise during pre-event activities.

Developing and practicing responses to detected or reported drones are easier. Venue security can partner with local law enforcement to create simulations that involve a real drone operator. This type of activity enables security teams to test and exercise reporting procedures and determine if signs and incentives sufficiently motivate the public to get involved in venue security (reporters should be rewarded for their efforts, even during simulations). Response times, engagement protocols, and passive and active detection measures can all be evaluated, debriefed, and improved.

The second prong of this particular deterrent strategy is to create random anti-drone measures. The nature of such measures will depend on the surrounding conditions and infrastructure. One example would be for a venue to close its retractable roof during fair weather conditions. A second example would be for a venue to announce the deployment of drone detection equipment. Although such equipment is currently expensive and subject to limited availability, decoys could be used in the meantime to bolster the deterrent. Looking more long-term, venues or organizations could partner with, or create incentives for, outside entities to facilitate the development of such technology.

Although the current status and proliferation of drones do not yet warrant significant concern, those charged with protecting the public should begin to shape policy and behavior now. The rate at which people are purchasing drones and the rapid advancement of technology that make drones easier to operate and more capable will offer hobbyists and potential criminals or terrorists with options that are not currently available. Making sure law enforcement, the intelligence community, and those with significant stakes in large venue security are not caught unaware will reduce the potential for serious harm.