Terror from Above

How the Commercial Unmanned Aerial Vehicle Revolution Threatens the US Threshold

Maj Bryan A. Card, USAFR

Amazon is not the only organization interested in using unmanned aerial vehicles (UAV) to deliver packages. Soon, terrorist organizations may also employ UAVs for their diabolic purposes. The US is on the cusp of a burgeoning commercial UAV revolution. Federal Aviation Administration (FAA) regulations have limited commercial employment of UAVs within the US; however, this is changing with newly implemented FAA guidelines.[1] As the regulatory impediments to using UAVs in the US for commercial purposes continue to decrease, commercial demand will increase, and UAV technology providers will develop more capable and user-friendly UAVs and control systems. Unfortunately, greater commercial accessibility to UAV technology will make UAVs more attractive as a delivery method for terrorist attacks, and policy makers should consider different courses of action to combat this emerging threat.

The DOD classifies UAVs into five different groups, based on the gross weight, operating altitude, and speed of the UAV.[2] This article will focus on the small UAVs in groups 1 and 2, which include UAVs under 55 lbs., flying under 3,500 feet above ground level, and under 250 knots. There are two primary reasons for focusing on these UAVs. First, the FAA has created a new remote pilot certification for UAV operators, no longer requiring UAV operators to hold a recreational, sport, or commercial pilot's license for unmanned aircraft weighing less than 55 lbs.[3] With this new regulation, it is anticipated that most commercial development into pilot-less systems in the US will fall into unmanned aircraft of this size. Second, it is more likely that individuals or a small group can build a group 1 or 2 UAV in a garage, on a small budget, for use in a terror attack without attracting suspicion.

Definitions

First, it is helpful to look at some of the terms and acronyms associated with unmanned aerial vehicles:

- *Unmanned aerial vehicle* (UAV): UAV refers to an actual air vehicle, sometimes simply referred to as an unmanned aircraft (UA).
- *Unmanned aerial system* (UAS): This term typically refers to the entire system of systems that allows a UAV to fly and perform its mission, including the ground station, telemetry, communication and navigation equipment, sensor package, and the UAV itself.
- *Remotely piloted aircraft* (RPA): An unmanned aircraft controlled by a trained pilot; this is a term primarily used by the USAF to denote unmanned aircraft.[4]
- *Drone*: A common term used to refer to UAVs but can refer to any form of automated robot or machinery.

Despite the distinctions among these terms, they are often used interchangeably. This article will primarily use the term *UAV* unless referencing a complete system of systems, in which case the term *UAS* will be used.

Last, the following terms will be used to characterize potential terrorist targets and assets that law enforcement and defensive planners wish to protect.

- *High-value target*: A target whose loss will significantly bolster the terrorist's campaign, due to several factors that could include the symbolic nature of the target and the amount of media attention the target would generate.[5]
- *High-risk personnel*: Personnel who, by their position, grade, assignment, or symbolic value, are likely to be attractive terrorist targets.[6]
- *High-risk event*: An event that due to its symbolic value, mass attendance, or media attention, is likely to be an attractive and accessible terrorist target.

Current Assessments of Unmanned Aerial Vehicles as Threats to National Security

Until recently, the literature discussing the threat from UAVs focused on either large-scale UAVs that pose an external threat to US security or on domestically operated UAVs that could threaten the privacy of citizens. Recent events, such as the UAV crashing on the White House lawn and UAV sightings in France—throughout Paris and at nuclear power plants throughout the country—have brought attention to the use of small UAVs and the potential danger they pose.[7]

One of the most critical pieces of research to date examining the threat of UAVs to the US homeland is a RAND Corporation study entitled *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*, henceforth referred to as the *Novel Threats* study. This 2008 study conducts a "Red" analysis of alternative attack modes, comparing "the suitability of cruise missiles and UAVs against other options, such as vest bombs, car bombs, and mortars."[8] The success of potential attacks is based on three primary tactical outcomes:

1. Targeted individuals are injured or killed.
2. Property is damaged or destroyed.
3. An activity in or by the target state is disrupted.[9]

To determine if an attack mode could successfully achieve these tactical outcomes, the study considered: (1) warhead effectiveness (measured by weight of payload); (2) the type of ordinance delivered; (3) the accuracy of the weapon; and (4) the probability of reaching the target. Generally speaking, the larger the payload that can be delivered, the less accuracy required to achieve the tactical objective.

The study concludes that UAVs and cruise missiles best provide the following five operational advantages:

1. Circumventing perimeter defenses
2. Attacking from outside national borders
3. Staging multiple simultaneous attacks
4. Sustaining protracted terrorist campaigns and
5. Dispersal of unconventional weapons.[10]

Despite these operational advantages, the study claims that UAVs are unlikely to be widely embraced due to their "greater complexity, technological uncertainty, cost, and risks."[11] The authors do concede that attack methods are "driven by the actions of the defense or security measures" in place; however, they conclude that significant soft targets within the US exist to make it unnecessary for terrorists to employ UAVs for attacks.[12]

In arriving at their conclusion, the *Novel Threats* authors failed to take into consideration two important factors that will contribute to terrorist use of UAVs. First, they do not consider communication, or "messaging," as a tactical objective of terrorist violence. Second, the study does not account for the commercial expansion of

UAVs that the US is now beginning to experience or the effects commercialization is having on the costs and accessibility of UAVs. Consideration of these two factors will demonstrate that the use of UAVs in terrorist attacks can no longer be dismissed as highly unlikely.

Terrorism as Communication

A key component of terrorism is communication. In *Communicating Terror*, Joseph Tuman proposes that terrorists engage in violence to send a message to a target audience. He writes: "The primary audience will be those who witness and observe the violence and destruction and engage in discourse about what they have seen."[13] Thus, the message is not the violence or destruction itself, but rather the message is either embedded within the violence or follows from it in subsequent messaging.[14] Therefore, the tactical output of a terrorist action may not be the people killed or the damaged property but rather the message it sends to a target audience that is separate from those targeted in the attack.

By striking a particularly high-value target, such as a high-ranking political figure, celebrity, or athlete, a terrorist organization can demonstrate its ability to overcome the defensive capabilities of the state, displaying the terrorists' strength and the state's weakness. The more attention the action will garner—through sheer destruction or due to the target's high value—the more lucrative a particular target becomes. Simply assuming that terrorists will attack soft targets rather than protected ones due to the additional operational complexity is simplifying the issue too much. By failing to address the idea that terrorism is communication through violence, the *Novel Threats* authors discount the real possibility that terrorists may choose an accurate delivery method capable of circumventing perimeter defenses to strike at a high-value target and thus garnering the terrorists a high degree of attention and infamy. By not addressing terrorists' propensity for choosing targets of symbolic significance or for media attention, the *Novel Threats* study comes to the rebuttable conclusion that UAVs are not a probable threat. UAVs are indeed a probable threat.

The Commercialization of Unmanned Aerial Vehicles

A second factor the *Novel Threats* study fails to account for is the burgeoning commercial UAV revolution. Missy Cummings, a former Navy fighter pilot and the director of the Humans and Autonomy Lab at Duke University, has stated:

> *We're going to see many commercial applications and much more civilian development than in the military. In 15 years, you could look up in the sky and see UAVs doing window washing and building inspections. You also could see every jealous ex-husband or wife following their significant other around. For good or bad, we are on the cusp of a new era.*[15]

One's imagination may be the only limiting factor to the multitude of uses for UAVs. Current commercial uses include aerial photography, monitoring oil fields and pipelines, transporting critical goods, and conducting search and rescue operations. One example of this new demand for UAVs is provided by University of Nebraska

journalism professor Matt Waite, who spent almost two decades as a reporter covering natural disasters. At a digital-mapping conference he saw the GateWing X100 UAV, which can fit in the back of a sport utility vehicle, is hand-launchable and equipped with a downward-facing high resolution camera. Controlled by a tablet computer using a digital map, one simply touches the screen and tells it where to fly—no piloting skills required. The X100 is extremely useful for reporting on fires, floods, hurricanes, and tornadoes—just about any situation where it is prohibitively dangerous to fly a manned aircraft.[16] This utility was demonstrated recently in the aftermath of Hurricane Harvey, where the FAA issued at least 43 authorizations to fly commercial UAVs in support of recovery efforts, helping local authorities "assess damage to homes, roads, bridges, power lines, oil and gas facilities, and office buildings."[17]

Human supervisory control is one of the largest advantages of UAV technology, allowing those with minimal training to control these aircraft. Instead of having to understand aeronautical principles and the complex controls of an aircraft—as a pilot must—UAV operators are performing, human supervisory control, a higher-level function where the operator "encourages" the aircraft to do what she or he wants.[18] Thus, you have UAVs that fly themselves to waypoints without the operator having to know the first thing about aerodynamics. Engineers, surveyors, search and rescue crews, and other professionals who would benefit from a UAV can simply go through minimal training and operate the aircraft themselves.

In one of Cummings' experiments with human supervisory control, micro-aerial vehicle visualization of unexplored environments (MAV VUE), researchers had an operator in Seattle, Washington controlling a micro-UAV in an open field in Cambridge, Massachusetts.[19] The controller used an iPhone connected to the internet via a wireless hotspot while the UAV communicated with a ground-station, also connected to a wireless hotspot. The operator had two levels of control—waypoint control and nudge control. Using waypoint control, the operator simply clicked on a digital map to tell the UAV where to fly. Using nudge control, the operator, with the help of a forward-facing view from the UAV's camera, flew the UAV by tilting the iPhone in the direction she wanted it to go. The researchers also selected random passersby to control the UAV to demonstrate how a minimally trained operator could easily operate a small UAV. Test subjects received three minutes of instruction and were able to successfully control the UAV and perform tasks like identifying people through the video feed sent to the iPhone from the UAV's camera. Such technology allows operators to move away from traditional command and control systems that require them to micromanage the behavior of the vehicle, and to concentrate instead on the more mission-relevant part of command and control.

Additionally, the relatively low cost of group 1 and 2 UAVs will make them a viable delivery mechanism for terrorists. Exemplifying the increased accessibility of UAVs is the hobbyist website *DIYDrones.com*. *DIYDrones.com* is dedicated to helping drone enthusiasts gather and exchange ideas and information about how to build and operate drones. Through it, a person can learn to build a UAV equipped with high-definition (HD) cameras, telemetry, and control systems. These hobby-built UAVs can be assembled with a full telemetry kit and autopilot for a cost of between $2,000–$10,000.[20] Chris Anderson, founder of *DIYDrones.com* stated, "If we make the technology cheap, easy and ubiquitous, regular people will figure it out."[21] Cer-

tainly if your average person can build a UAS, so can a terrorist, and the $2,000–$10,000 price range falls well within the historical costs of many terrorist attacks.[22]

In 2012, Cummings stated, "companies are chomping at the bit" to integrate UAVs into their operations, "and there's no technical reason we can't do this now. . . the only reason we don't is regulatory issues."[23] Now, with the barriers to operating UAVs in the US diminishing, we will see a rise in commercial development, leading to greater accessibility for individuals and businesses. Unfortunately, such increased accessibility will also make UAVs more attractive to those who would use them for nefarious purposes, thus eliminating the barriers to entry into the realm of airpower.

The Attraction of Unmanned Aerial Vehicles

With the understanding that terror attacks are communication through violence and that the technical and monetary costs of using UAVs are decreasing, we will now highlight some of the characteristics of UAVs that make them well-suited for terrorist attacks. The *Novel Threats* study argues that the primary reason UAVs are attractive as a delivery mechanism is their inherent mobility—the ability to conduct attacks over perimeter defenses. While many potential terrorist targets in the US lack perimeter defenses or barriers, "individual protected targets may still be attractive to an adversary if a successful strike on such a target is viewed as particularly valuable in advancing the group's goals."[24] For instance, it is not hard to imagine the media sensation that would occur if terrorists are able to successfully fly a weaponized UAV into a huddle of football players during the next Super Bowl, an outdoor music concert, or an elementary school playground at recess. Another frightening example would be if a UAV were flown toward the US president at the next inauguration. Even a minimal 1–2 lb. explosive charge could cause deaths and severe injuries, all while 100 million people watch in horror.

This ability of a UAV to bypass perimeter defenses is exemplified by several recent events. In 2013, at a campaign event in Dresden, German Chancellor Angela Merkel and Defense Minister Thomas de Maizière were interrupted by a quadcopter flying onto the stage (fig. 1).[25] In January 2015, a quadrotor UAV crash landed on the White House lawn and three months later a gyrocopter—the size of a larger UAV—landed on the lawn near the US Capitol, flying unimpeded through restricted airspace.[26] In these examples, no one was injured, and there was no demonstrable malicious intent on the part of the operators; however, they show how easily UAVs can access secure areas. Either of these events could have been tragic had the operator's intent been nefarious and the aircraft carrying energetic material.

A second reason terrorists will adopt UAVs is their ability to lower operational risks to the terrorists themselves. While some terrorists have shown a willingness to sacrifice themselves for their cause, others may be attracted to the ability to commit a terrorist attack with a much lower risk of apprehension, allowing for the possibility of conducting a protracted terror campaign. The MAV VUE project demonstrates how a UAV operator can be 3,000 miles away, controlling a UAV over the internet. Someone would certainly need to be on the ground to deploy the UAV; however, a UAV equipped with a 3G or 4G cellular phone can be controlled from

virtually anywhere. Such operations would significantly complicate law enforcement investigations because of the limited footprint that terrorists would leave on the ground near the attack. A weaponized UAV could be launched miles away from the intended target, forcing law enforcement to greatly expand the search area for potential witnesses and/or physical evidence.

Courtesy of ArsTechnica

Figure 1. German chancellor Angela Merkel smiles as a Parrot AR drone comes in for a crash landing during a Christian Democratic Party campaign event 15 September 2013. (Reprinted from "German Chancellor's Drone 'Attack' Shows the Threat of Weaponized UAVs," ArsTechnica, 8 September 2013, https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/.

A final reason that UAVs are attractive to terrorists is that it would be difficult to thwart an attack in progress. It is difficult to detect UAVs using radar, the traditional method of detecting air defense threats. The gyrocopter that landed on the Capitol building lawn exemplifies this difficulty. White House spokesman Josh Earnest said that the low-speed, low-altitude flight made it difficult to detect the small gyrocopter on radar.[27] Marcus Weisgerber, a *Defense One* writer, stated, "Radars can only see above the treeline so if he's flying on the treeline they are going to have a hard time spotting him."[28] Additionally, the small size of UAVs makes them difficult to detect on radar, since "(existing radar systems) are not designed to look for something like a quadcopter."[29] Finally, by the time UAVs are detected, their high speed (70–plus mph) can make them difficult to defeat or evade.

There are already weaponized, small-scale UAVs developed for military application, designed to be rapidly deployable, easily controlled and equipped to destroy soft targets. AeroVironment's "Switchblade is designed to provide the warfighter

with a back-packable, non-line-of-sight precision strike solution with minimal collateral effects."[30] The Switchblade weighs 2.8 kg, carries a 0.45 kg payload, and can reach an estimated top speed of 80–100 mph.[31] AeroVironment claims "the vehicle's small size and quiet motor make it difficult to detect, recognize and track even at very close range."[32] While the Switchblade may well never fall into terrorist hands due to sales and export restrictions, the principle of the Switchblade—a small, fast UAV with an onboard camera for targeting—provides an important example of the potential of this threat.

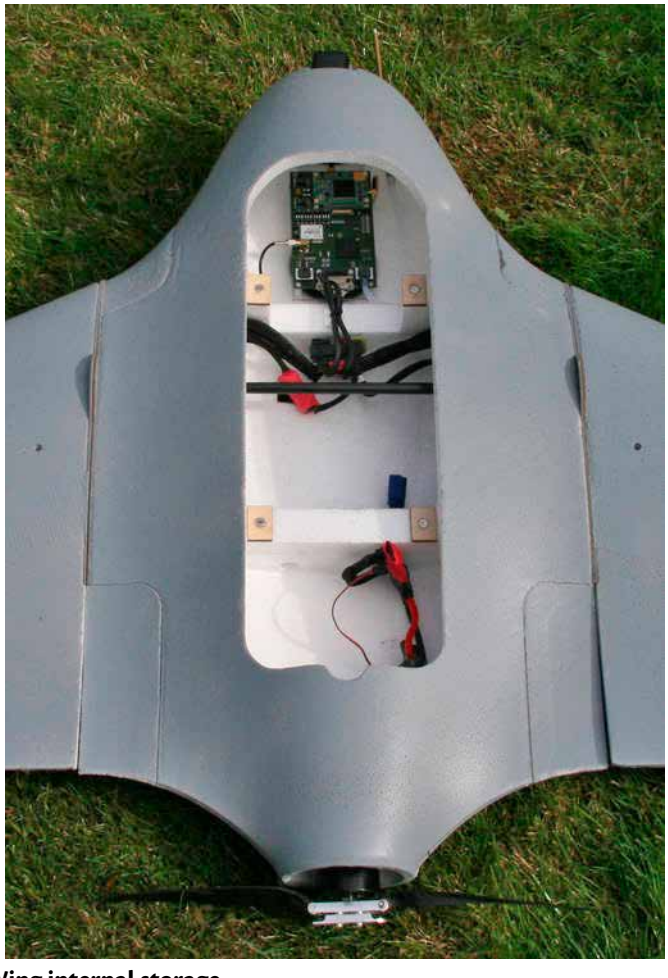

Figure 2. X8 Flying Wing internal storage

One example of a hobbyist remote control (R/C) aircraft that can be converted into a weaponized UAV is the X8 Flying Wing. The X8 has ample space for electronics and a small explosive. (fig. 2) It weighs a mere 2.2 kg, is capable of holding an additional 2.3 kg payload, can cruise at 40 mph with a maximum speed of 70 mph, and has an endurance of up to three hours.[33] The base kit can be purchased for

$160; a complete system with an engine, autopilot, first-person view HD camera and video transmitter can cost an amount between $2,000–$10,000. There are also options to purchase the X8 as a turn-key UAS. Spain-based Airelectronics sells the X8 Flying Wing complete with a ground station, its U-Pilot autopilot, and a sensor suite. Airelectronics claims an endurance of up to three hours, with redundant navigation using dead reckoning if GPS signals are lost. This system is estimated to cost approximately $20,000.[34] The X8 is just one of several hobby-grade UAVs that can be used for attacks, highlighting once again the real terrorist threat UAVs pose today.

Defensive Approach

US military joint doctrine discusses both defensive and offensive methodologies for countering air threats.[35] Borrowing from this operational concept, we will examine both active and passive defense, as well as a more proactive approach utilizing intelligence and law enforcement operations before a possible UAV attack. Active defense consists of "direct defensive actions taken to destroy, nullify, or reduce the effectiveness of hostile air" threats, while passive defense includes measures "taken to minimize, mitigate, or recover from the consequences of attack aircraft and missiles."[36] Finally, intelligence and law enforcement operations can be used to seek out and apprehend terrorists before they strike.

Active Defense

UAVs are not a traditional air defense threat as they are generally smaller than manned aircraft and fly lower and slower, making them harder to detect, thereby complicating the role of active defense. Radars can only detect objects within their direct line of sight, and the lower an object flies, the shorter the possible detection range due to being masked behind trees and buildings. Finally, the small size of UAVs further complicates detection with radars. Based on an Army Research Lab report, a small UAV may have an approximate radar cross-section (RCS) of -15 dBsm, or decibels referenced to a square meter, which is a logarithmic measure of how much a particular object will reflect electromagnetic energy.[37] This is comparable to a large bird (-20 dBsm), while, on the other hand, a large commercial airliner could have an RCS around 40 dBsm and a small jet might be in the 1–2 dBsm range.[38] Therefore, even if a UAV is detected on radar, it may be disregarded as a bird due to their similar size, altitude and speed.

To make matters worse, even if a UAV threat is identified, the options for dealing with the threat are limited. First, in urban environments, where attacks are more likely, law enforcement and the military will be averse to shooting UAVs down because any projectile used for a kinetic attack may cause collateral damage when it returns to the ground. Furthermore, many UAVs would likely be difficult to shoot down due to their light weight, requiring minimal lift to remain airborne.[39] UAVs made of Styrofoam, fiberglass or similar materials could likely take several hits and remain operational unless a critical component is damaged—such as the engine, navigation, or receiver. The use of an explosive ordinance could help alleviate this

issue, but it will add additional concern about collateral damage and public safety. Lastly, a kinetic model for defending a target in an urban environment could require several systems with trained operators to be in place along likely air avenues of approach to adequately defend the area. This model will increase the cost of defending against UAV threats, perhaps prohibitively so, which is one of the reasons the *Novel Threats* study does not recommend the development of a robust active defense system for this threat.

One form of active defense that does hold promise, however, is the use of jamming to block the command channel and/or telemetry of UAVs. Jamming can be particularly effective against hobby-grade UAVs because their command frequencies are regulated; therefore, anything purchased off the shelf will be in a frequency range that can be anticipated. By jamming the most common frequencies, one could effectively eliminate the ability of a terrorist UAV operator to conduct accurate targeting within the denied area. Additionally, unlike kinetic fires, jamming would not necessarily require the same type of tracking precision to engage the threat. Jamming can be omnidirectional, thus only requiring the threat be detected within a certain proximity, allowing for nontraditional methods of detection, such as acoustic and radio frequency detection.

There are three basic factors to consider debating when attempting to jam a UAV command channel or its telemetry data:

- Transmit power of both the control station and the UAV
- Antenna gain of the transmitters
- Radio-frequency (RF) noise level in the environment.

For a terrorist to conduct dynamic targeting, the control station and UAV need to communicate. By preventing this communication, an attack may be thwarted or, at a minimum, cause a loss of precision in targeting, which is critical when considering the small payload of these UAVs.

Theoretically, radio waves, by which the ground station and UAV communicate, travel infinitely; however, as they travel, they disperse, and their signal weakens by the square of the distance they travel.

$$\left(Intensity \times \frac{1}{Distance^2}\right)$$

This rule is known as the inverse square law of propagation, and it is the major determinant of the range in which a UAV control station can make contact with a receiver. Antenna gain also affects this distance in that the better the antenna can translate power into radio waves, the further the usable signal will travel. Third, the signal needs to overcome the RF noise level in the environment. Once the signal can no longer be discerned from the noise, it becomes unusable. Jamming works by effectively raising the RF noise level, preventing a useful transmission from reaching the receiver on the UAV. As the UAV approaches the defended asset and collocated jammer, the harder it is for the transmitter to overcome the RF noise of the signal jammer.

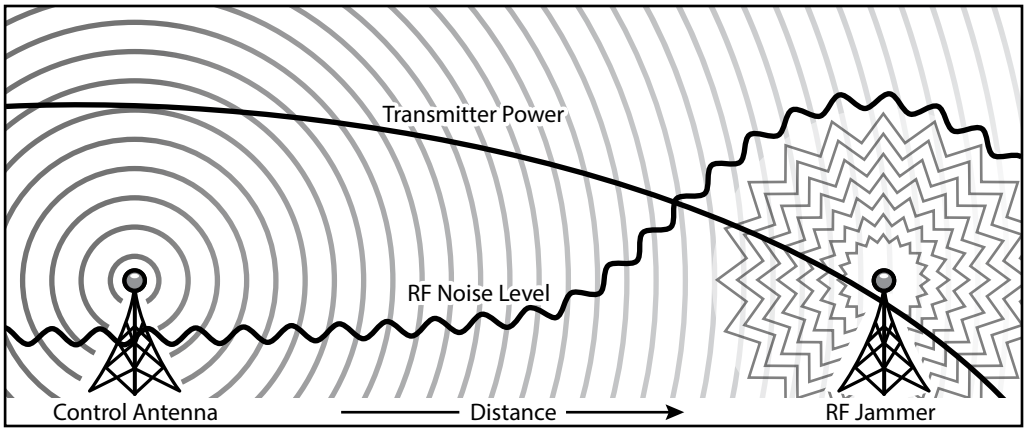

Figure 3. Transmitter power versus RF noise level

Figure 3 shows how such a jammer would work by raising the RF noise level in the vicinity of the area that is to be defended. Once the signal from the control antenna falls below the RF noise level, the operator would no longer be able to control the UAV. To overcome the signal jammer, the terrorist would then have to change frequency bands, increase transmit power, or get closer to the target area, none of which are particularly easy. Changing the frequency band or increasing the power output of the transmitter would require significant knowledge of electrical and radio frequency engineering, unlikely to be had except in the case of the most determined and/or technical of terrorists. Additionally, forcing the terrorist to move closer to the target raises the operational risk for the terrorist since he then may be observed and interrupted midoperation, thus negating some of the operational advantages of UAVs.

One of the downsides of using jamming against UAVs, however, is that there are many users of the electromagnetic spectrum, and jamming may disrupt legitimate users of the spectrum. R/C aircraft and UAVs are only authorized to utilize certain frequencies: 27 MHz, 49 MHz, 50 MHz, 53 MHz, 72 MHz, and 75 MHz for single channel use and 2.4 GHz for spread spectrum use.[40] Additionally, telemetry kits that send back video and positioning information can usually be found in the 433 MHz, 900 MHz, 2.4 GHz, and 5.8 GHz ranges. While the single-channel control frequencies would not be particularly problematic to jam, the 433 MHz, 900 MHz, 2.4 GHz, and 5.8 GHz ranges are part of what is known as the industrial, scientific and medical bands (ISM), and jamming them could cause undesirable interference. Common devices that use these bands include Bluetooth devices, cordless phones, and wireless internet protocol networks. Additionally, a complicating factor in the utilization of jammers is the use of cellular networks to control UAVs. To extend the range of UAVs and the telemetry they send back, terrorists may attempt to utilize cellular networks by integrating a smartphone or other wireless mobile device into their UAV design, as exemplified in the MAV VUE experiment. Jamming such signals would require interrupting cellular services within a given area. The general

public would likely disapprove of continuous, unnecessary interruptions of cellular services and other wireless functions in protected areas. Fortunately, there are ways to help mitigate undesired interference.

Active and passive detection systems—radars, acoustic sensors, and RF detectors—can help mitigate interference with the general public use of cellular services and the ISM bands by allowing jamming only when a UAV is detected within restricted airspace. Radars optimized against small, low, and slow UAVs—such as those using new holographic and micro-Doppler radar technology—may be effective at detecting and identifying UAVs operating in restricted airspace.[41] Additionally, nontraditional detection methods such as acoustic and radio frequency sensors may also prove useful in both detecting UAVs and distinguishing them from other objects like birds. Acoustic systems detect the relatively unique audio signature that UAVs produce from their propellers, while RF detection involves creating a mesh network of receivers "that can triangulate moving transmitters."[42] Thus, once a UAV is detected entering restricted airspace or approaching a high-risk event, jammers can then be turned on to defeat the threat, minimizing the interruption of cellular services and the ISM bands and alleviating public concerns.

Obviously, the choice to interrupt cellular service, wireless networks, and Bluetooth devices should not be taken lightly; however, when faced with the alternate choice of expending live ordinances over a population center in order to disable a threatening UAV, the prudent choice to use jamming is clear. The use of a warning network—radar, acoustic sensors, and RF detectors—to detect UAV threats combined with RF jamming of UAV command and telemetry systems seems to be a highly promising way to defeat such threats.

Passive Defense

One of the best methods of mitigating a UAV terrorist attack is through a strong passive defense. Passive air defense measures can include detection and warning systems, camouflage and concealment, deception, and hardening. One particularly effective passive method for defeating UAV attacks is to host high-risk events indoors. Most commercial structures provide adequate physical protection—hardening—from the warheads that small UAVs would be able to carry, approximately 1–5 kg. By merely hosting events inside, one could greatly reduce the likelihood of being targeted. While it may be possible to fly a UAV inside a structure, it is not desirable due to a lack of mobility, difficulty in route planning and the strong possibility of losing RF signals indoors. Hosting an event indoors removes the ability of the UAV to bypass perimeter defenses and would likely cause a terrorist to choose a different target or delivery method.

In case of an outdoor event, passive defenses can still be implemented. By utilizing detection systems to provide advanced warning, high-risk personnel can be moved to a sheltered area if a UAV were to enter into a restricted area. Since small UAVs cannot carry a large payload, this shelter could range from an armored vehicle to a nearby building. For outdoor events on a covered stage, deployable netting could prove effective at preventing a UAV from getting close to an intended target.

Passive defense can even act as a deterrent against attacks since terrorists may be led to believe that their weapons would not be able to reach the desired target.

Finally, traditional forms of operational security can help protect high-risk personnel from being targeted by UAV attacks. Such measures include using unpredictable transport routes and varying the times that high-risk personnel arrive and leave work and residences, as well as not announcing arrival and departure times of high-risk personnel at high-risk events. These measures generally make it harder for terrorists to target high-risk personnel using any method of attack, not just UAVs.

Intelligence

Currently, almost all of the technology related to hobby-grade R/C aircraft and UAVs is widely available, and it would be nearly impossible to stop the proliferation of this technology.[43] However, it may be possible to discover those who are building UAVs that can be operated beyond visual range. The one distinction between UAVs and R/C aircraft is navigational control. Navigational control can be separated into two distinct pieces of technology—GPS receivers and autopilots. While GPS receivers are commonplace, the autopilot fills a highly specialized role, as it is only procured by individuals operating aircraft or building UAVs. Because the development and use of a UAV require this highly specialized piece of technology, law enforcement, and intelligence agencies have something they can specifically look for in screening for potential terrorist threats.

If law enforcement and intelligence personnel gained the ability to monitor purchases of autopilots, they could then cross-reference those purchases against other indicators of terrorist activity, such as ties to extremist groups and the purchase of chemicals that can be used in making explosives. Similarly, the purchase of any commercial-off-the-shelf (COTS) UAV that includes an autopilot and is capable of holding a 1–5 kg payload (or more) could be monitored. Therefore, it is recommended that provisions be put in place that would enable law enforcement and appropriate intelligence agencies to monitor purchases of autopilots and COTS UAVs.

Conclusion

The employment of UAVs by terrorists is not a far-off threat. The commercialization of UAVs is occurring now and with the latest announcement from the FAA, creating an operator status for small UAVs, eliminating the costly requirement of a licensed pilot, we will see more commercial demand. UAV companies and technology providers will endeavor to make UAV technology even more accessible to both businesses and individual hobbyists to increase its marketability. Unfortunately, commercial development will make such technology more attractive and accessible to terrorists, as well.

Terrorists will seek to acquire small UAVs because of their significant potential benefits. Terrorists use violence as communication, and they understand that it is not necessary to kill numerous people to send a message. UAVs provide the ability to bypass defensive perimeters, allowing terrorists to strike high-risk personnel or

events, which can produce immediate, live media coverage and depict weakness in the government for its inability to protect such targets. Additionally, using UAVs provides a certain degree of safety for the terrorist by enabling him to be farther away from the target location, possibly allowing the terrorist to conduct subsequent attacks before being apprehended. Terrorists are now increasingly able to capitalize on the benefits of using UAVs through technological advances such as those in human supervisory control and through a decrease in the costs of obtaining a UAV. All in all, the likelihood of seeing UAVs used in terror attacks is significantly increasing.

While UAVs may be more difficult to defeat than traditional air threats, there are measures that can be taken to help mitigate the threat from small UAVs. Hosting high-risk events and the appearances of high-risk personnel indoors is probably the best way to protect against the threat from small UAVs. This passive defense measure also happens to have the fewest negative consequences and is probably the lowest cost option among the alternatives. Of course, it will not always be possible to host an event indoors. Events such as the Boston Marathon will still provide lucrative targets for terrorists; however, risk can be mitigated through active defense measures. Radar assets can be brought to bear to detect these threats, providing early warning that enhances passive defense. Also, jamming can be utilized as part of an active defense to disable UAVs once they are detected entering into a restricted area. Finally, by monitoring those who purchase autopilots and COTS UAVs that have built-in autopilots and a certain payload capacity can help law enforcement and intelligence operations can help discover, ahead of time, those who would use UAVs (among other tools) to harm us.

Unfortunately, the reality today is that UAVs complicate matters for security personnel and defensive planners. They democratize airpower, forcing the consideration of the third-dimension when thinking about potential threats to high-risk personnel and events. The advantages gained by utilizing UAVs will undoubtedly attract terrorists to potential targets that will now be more accessible. While resources may be limited to adequately protect the vast number of potential targets, small-scale UAVs are a growing threat and one for which the US government should be preparing. ✪

Notes

1. Federal Aviation Administration (FAA), "Summary of Small Unmanned Aircraft Rule (Part 107)," *FAA News*, 21 June 2016, https://www.faa.gov/uas/media/Part_107_Summary.pdf.
2. "United States Air Force Unmanned Aircraft Systems Flight Plan 2009–2047," (Washington, DC: Headquarters, USAF, 2009), 25, http://fas.org/irp/program/collect/uas_2009.pdf.
3. FAA, "DOT and FAA Finalize Rules for Small Unmanned Aircraft Systems," 21 June 2016, https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20515.
4. Air Force Instruction 11-202, vol. 3, *Flying Operations: General Flight Rules*, 10 August 2016, 69, http://static.e-publishing.af.mil/production/1/af_a3/publication/afi11-202v3/afi11-202v3.pdf.
5. This is similar to the term used by the DOD; *see* "Joint Publication (JP) 1-02, *Dept. of Defense Dictionary of Military and Associated Terms*," 15 March 2015, 108, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
6. JP 3-07.2, *Antiterrorism*, 24 November 2010, GL-6, http://www.dtic.mil/doctrine/docnet/courses/operations/icdjo/resources/JP3_07X2.pdf.
7. Michael D. Shear and Michael S. Schmidt, "White House Drone Crash Described as a U.S. Worker's Drunken Lark," *New York Times*, 27 January 2015, http://www.nytimes.com/2015/01/28/us/white

-house-drone.html?_r = 0; and Amar Toor, "Paris has a Drone Problem," *The Verge*, 26 February 2015, http://www.theverge.com/2015/2/26/8113291/paris-drone-uav-eiffel-tower-charlie-hebdo.

8. Brian A. Jackson, David R. Frelinger, Michael J. Lostumbo, and Robert W. Button, *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*, Rand Corporation: National Defense Research Institute, 2 March 2008, 8, http://www.rand.org/pubs/monographs/MG626.html.

9. Ibid., 13.

10. Ibid., 58–59.

11. Ibid.

12. Ibid.

13. Joseph Tuman, *Communicating Terror*, 2nd ed. (Los Angeles, Sage Publications: 2010), 34.

14. Ibid., 32.

15. Patrick Hruby, "Out of 'Hobby' Class, Drones Lifting Off for Personal, Commercial Use," *Washington Times*, 14 March 2012, http://www.washingtontimes.com/news/2012/mar/14/out-of-hobby-class-drones-lifting-off-for-personal/?page = all.

16. Ibid.

17. Aarian Marshall, "Above Devastated Houston, Armies of Drones Prove Their Worth," *Wired.com*, 4 September 2017, https://www.wired.com/story/houston-recovery-drones/.

18. Missy Cummings, "Can a 'Computer Co-pilot' Help Anyone Be a Surgeon?" *TEDTALK 2012*, 10 July 2012, http://www.tedmed.com/talks/show?id = 7355&videoId = 6923&ref = about-this-talk.

19. Tom Koehler, "Smart Phones Fly Mini Drones," *Boeing*, 29 August 2011, http://www.boeing.com/Features/2011/08/corp_drone_08_29_11.html.

20. This range includes the cost of the hobby aircraft, autopilot, telemetry kit, and ground-station. More information on various pricing options can be found on the *DIYDrones.com* website and the affiliated 3DRobotics website: http://www.diydrones.com and http://3drobotics.com, respectively.

21. Hruby, "Out of 'Hobby' Class."

22. Eben Kaplan, "Tracking Down Terrorist Financing," *Council on Foreign Relations*, 4 April 2006, http://www.cfr.org/terrorist-financing/tracking-down-terrorist-financing/p10356#p4.

23. Ibid.

24. Jackson et al., *Evaluating Novel Threats*, 29.

25. Sean Gallagher, "German Chancellor's Drone 'Attack' Shows the Threat of Weaponized UAVs," *ArsTechnica*, 18 September 2013, http://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/.

26. Shear and Schmidt, "White House Drone Crash Described;" and Krishnadev Calamur, "Florida Mailman Who Flew Gyrocopter onto Capitol Lawn Charged," *the two-way*, 16 April 2015, http://www.npr.org/sections/thetwo-way/2015/04/16/400195580/florida-mailman-who-flew-gyrocopter-onto-capitol-lawn-charged.

27. Calamur, "Florida Mailman Who Flew Gyrocopter."

28. Robin Young, "How Did This Pilot Make it All the Way to the Capitol Lawn?" *Here and Now*, 16 April 2015, http://hereandnow.wbur.org/2015/04/16/gyrocopter-capitol-security.

29. Tereza Pultarova, "Drone-detecting Air-traffic Radar Successful in Trials," *Engineering and Technology Magazine*, 6 May 2015, https://eandt.theiet.org/content/articles/2015/05/drone-detecting-air-traffic-radar-successful-in-trials/.

30. "Switchblade," *AeroVironment*, 13 June 2015, https://www.avinc.com/uas/adc/switchblade/.

31. "2010–2011 UAS Yearbook," *The Global Perspective—8th Edition*, June 2010, http://uas.usgs.gov/UAS-Yearbook2010/pdf/P161-195_World-UAS-Reference-Section.pdf; and Gary Mortimer, "Lethal Miniature Aerial Munition System (LMAMS) to be Deployed Soon?," *UAS News*, 1 January 2011, http://www.suasnews.com/2011/01/3260/lethal-miniature-aerial-munition-system-lmams-to-be-deployed-soon/.

32. AeroVironment, "Switchblade."

33. "Airelectronics X8 Flying Wing Datasheet," *Airelectronics* website, 13 June 2015, http://www.airelectronics.es/products/x8_brochure.pdf?PHPSESSID = itg7avr0agek17jv0o6njqt7h3.

34. Airelectronics does not publicly state the cost of the complete system, but the ground station, autopilot, and control software retails for approximately $16,000, which would be the bulk of the cost of the system.

35. "JP 3-01, *Countering Air and Missile Threats*," 21 April 2017, I-3, http://www.dtic.mil/doctrine/new_pubs/jp3_01_20172104.pdf.

36. JP 3-01, *Countering Air and Missile Threats*, I-6 and V-15.

37. Thomas J. Pizzillo, "RCS Measurements of a PT40 Remote Control Plane at Ka-Band," *Army Research Laboratory*, March 2005, http://www.arl.army.mil/arlreports/2005/ARL-TN-238.pdf.

38. J. A. Spruyt and Ph. van Dorp, "Detection of Birds by Radar," *TNO Physics and Electronics Laboratory*, August 1996, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA321060; and Merrill I. Skolnik, *Introduction to Radar Systems*, 2nd ed. (London: McGraw-Hill Book Co., 1981), 44.

39. Quadcopters may be more susceptible to kinetic fires due to their reliance upon multiple motors to maintain lift.

40. Academy of Model Aeronautics, "Frequency Chart for Model Operation," 13 June 2015, http://www.modelaircraft.org/events/frequencies.aspx.

41. Tereza Pultarova, "Drone-detecting Air-traffic Radar;" and P. Molchanov, K. Egiazarian, J. Astola, R. I. A. Harmanny, and J. J. M. de Wit, "Classification of Small UAVs and Birds by Micro-Doppler Signature," *Proceedings of the 10th European Radar Conference*, 9–11 October 2013, http://www.cs.tut.fi/~molchano/papers/EuRad2013.pdf.

42. Bryan Lifkin, "Detection Systems Listen for Drones Flying Under the Radar," *Gizmodo*, 18 May 2015, http://gizmodo.com/detection-systems-listen-for-drones-flying-under-the-ra-1704764102; and "Credible Personal Drone Detection Systems Now Available on Kickstarter from Domestic Drone Countermeasures LLC," *PR Newswire*, 13 June 2014, https://www.prnewswire.com/news-releases/credible-personal-drone-detection-systems-now-available-on-kickstarter-from-domestic-drone-countermeasures-llc-263016721.html.

43. Ajay Lele and Archana Mishra, "Aerial Terrorism and the Threat from Unmanned Aerial Vehicles," *Journal of Defense Studies* 3:3 (July 2009): 54–65, http://skyjack.co.il/pdf/jds_3_3_alele_amishra.pdf.

Maj Bryan A. Card, USAFR

Major Card (AB Stanford University; MS, University of Texas at El Paso) is the chief of weapons and tactics for the 710th Combat Operations Squadron, Joint Base Langley–Eustis, Virginia. He is responsible for training and tactics development and evaluation to support air component operations. He recently returned from the US Air Forces Central Command Combined Air Operations Center, where he worked as a nonkinetic duty officer, integrating air, space, and cyber capabilities into joint operations. Major Card is also a project manager with the US Army Fires Center of Excellence, Capabilities Development and Integration Directorate, providing command and control and tactical data link support to the Army and Joint Staff. Before joining the Air Force Reserve, he spent five years in the US Army, serving as an air defense artillery fire control officer, responsible for the control and coordination of surface-to-air missile fires. He also served as an infantryman before his commissioning through the Officer Candidate School. Major Card has deployed to Afghanistan and Qatar, and he is a graduate of the US Air Force Weapons School and the Joint Interface Control Officer Course.