The Commercialization of UAVs:

How Terrorists Will Be Able to Utilize UAVs to

Attack the United States

Bryan Card
November 12, 2014
Capstone
Dr. Valero

Amazon.com™ is not the only organization interested in using unmanned aerial vehicles (UAVs) to deliver packages right to your door. Soon, terrorist organizations may also employ UAVs for their own diabolic purposes. The United States is currently on the cusp of a burgeoning commercial UAV revolution. Federal Aviation Administration (FAA) regulations have thus far limited commercial employment of UAVs within the United States; however, this is about to change. As the regulatory impediments to using UAVs in the United States for commercial purposes decrease and commercial demand for UAVs increases, UAV technology providers will compete to develop more capable and user-friendly UAVs and control systems, making them more accessible. Unfortunately, greater accessibility to UAV technology will also enable terrorists to utilize this technology for their own purposes. In other words, the commercialization of UAVs will make UAVs more attractive and accessible to terrorists as a delivery method for their attacks. As this is not a far off threat, the United States government should look into different courses of action to combat this emerging threat.

Definitions

First, it is helpful to look at some of the many 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, sensor package, and the UAV itself. The FAA defines an UAS as:

  > the unmanned aircraft (UA) and all of the associated support equipment, control station, data links, telemetry, communications and navigation equipment, etc., necessary to operate the unmanned aircraft. The UA is the flying portion of the system, flown by a pilot via a ground control system, or autonomously through use of an on-board computer, communication links and any additional equipment that is necessary for the UA to operate safely. The FAA issues an experimental airworthiness certificate for the entire system, not just the flying portion of the system (Unmanned Aircraft General Facts, 2014).

- Remotely Piloted Aircraft (RPA): This is a term adopted by the U.S. Air Force to denote a UAV that is controlled by a trained pilot, as opposed to one controlled by an operator who is not a trained pilot.
- Drone: A common term used to refer to UAVs, but can refer to any form of automated robot or machinery.
- Unmanned Combat Aerial Vehicle (UCAV): A UAV that has been weaponized to employ munitions or a UAV that is a munition itself.

Despite the distinctions among these terms, they are often used interchangeably. This paper will primarily use the term UAV unless referencing a complete system of systems, in which case the term UAS will be used. RPA will only be utilized when referencing a U.S. Air Force unmanned aircraft.

It should also be noted that there are important distinctions between UAVs and hobby remote controlled (R/C) aircraft, which can be converted into UAVs. Hobby R/C aircraft are typically controlled with a hand-held radio by an operator in direct visual contact with it. The FAA Modernization and Reform Act of 2012 defined model or hobby aircraft as:

1. Capable of sustained flight in the atmosphere;
2. Flown within visual line of sight of the person operating the aircraft; and
3. Flown for hobby or recreational purposes (Section 336).

There are currently no specific regulations regarding hobby UAVs—modified R/C aircraft capable of autonomous flight—and operators of such aircraft usually try to comply with the FAA's guidance for hobby model aircraft to avoid drawing any special attention from the FAA.

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

- High payoff 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, the amount of media attention the target would generate,
- High-risk personnel: personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets,
- High-risk event: an event that due to its symbolic value, mass attendance, or media attention, is likely to be an attractive or accessible terrorist target.

It is important to note that the term high payoff target is usually reserved for targets that U.S. military forces desire to strike for the success of an operation. The definition used here turns this on its head in order to define what targets that terrorists might strike.

Literature Review: Current Assessments of UAVs as Threats to National Security

Much of the current literature discussing the growing threat from UAVs focuses either on large scale UAVs that pose an external threat to U.S. security or on domestically operated UAVs that pose a threat to the privacy of citizens. One such article is "Armed and Dangerous? UAVs and U.S. Security," a 2014 RAND study that notes how the U.S. should be interested in the proliferation of drone technology and discourage its misuse. The article looks at larger, more complex drones and not really at UAVs that could potentially be employed by sub-state groups; however, the authors do note that inexpensive, precise navigation and GPS technology "is available to practically anyone in the world, including powerful and weak states, sub-state groups, and hobbyists" and that there is little that can be done to change this trend (p. 4). Other studies discuss how the commercialization of UAVs will threaten the right to privacy. Uri Volovelsky discusses in his article, "Civilian Uses of Unmanned Aerial Vehicles and the Threat to the Right to Privacy—An Israeli Case Study," the proliferation of UAVs and how they should be regulated without compromising the advantages inherent in their usage. Unfortunately, neither of these types of articles discuss much about the potential use of small-scale UAVs for terrorist attacks within the United States.

However, one study that does introduce the idea of UAVs as a terrorist threat is Lele and Mishra's "Aerial Terrorism and the Threat from Unmanned Aerial Vehicles." Lele and Mishra briefly summarize the history of aerial terrorism and introduce the idea that UAVs will be used to conduct terrorist attacks. They point out that the devastation caused from using a hijacked aircraft was not fully realized until the 9/11 attacks—which they call the classic case of aerial terrorism. They point out that

the counter-terrorism measures that states have employed since 9/11 have largely thwarted similar attacks. Furthermore, they claim that aerial terrorism is now shifting from traditional forms to forms that rely more upon modern technology and knowledge based attacks, using the Mumbai attack of November 2008 as an example of modern technology as an enabler. Lele and Mishra demonstrate that terrorists do desire aircraft and UAVs as weapons, citing a history of their use or intended use. However, the evidence the authors cite does not demonstrate actual usage of UAVs, and the overall article is weakened by a lack of analysis as to why terrorists would choose to use a UAV in place of a more traditional weapon. They do point out that "the most worrisome situation stems from model aircraft, where uncontrolled access to the knowledge, skills and equipment required for mini-UAV assembly exists"—the very topic of this paper (p. 61).

Perhaps the most critical piece of research to date that examines the threat of UAVs to the U.S. homeland is a RAND study entitled "Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles," henceforth referred to as the "Novel Threats" study. The 2008 study took a two-pronged approach in first conducting a red analysis of alternative attack modes and then examining defensive approaches to countering these "novel threats." One of the strengths of this study is that the researchers acknowledge that there are other threats to the homeland and that it is impossible to protect everything all the time from all possible threats. They write, "Before the country invests in a wide array of cruise-missile or other air defense assets for the nation, the problem needs to be bounded so that scarce resources can be focused productively" (p. xiv).

The "Novel Threats" study begins by comparing the capabilities of UAVs and cruise missiles to other delivery methods for high-explosives, evaluating "the suitability of cruise missiles and UAVs against other options, such as vest bombs, car bombs, and mortars" (p. 8). The researchers first compare the payload capability of various delivery methods, ranging from suicide bomber vests to large trucks and business jets, and then assess each delivery method's ability to reach an intended target or

complete an intended mission. The authors come up with five operational problems that UAVs and cruise missiles best solve:

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

After assessing the operational advantages of UAVs and cruise missiles, the authors conduct an analysis of tactical and operational decision-making that would influence whether or not a group is likely to utilize one of these novel threats, taking into account the following considerations:

- Access to and costs associated with UAV and cruise-missile technologies;
- Access to and costs associated with alternative technologies;
- Ability and willingness to develop the expertise necessary to operate the systems;
- Technological preference (p. 61).

The authors conclude that while UAVs and cruise missiles do provide "major advantages over other ways of carrying out operations against similar targets," they argue that the choice of one of these methods of attack will be "driven by the actions of the defense or security measures" that are in place (p. 58). Furthermore, they state that these appear to be "niche threats" that are unlikely to be widely embraced (p.58). Of particular importance in this study is the authors' claim that terrorists do not really have a need for the capabilities that UAVs and cruise missiles provide due to the wide availability of soft targets within the U.S..

Finally, the authors offer suggestions for defensive solutions against UAVs and cruise missiles. They offer practical solutions ranging from intelligence and law enforcement efforts to active and passive defense methods to deterrence. The authors consider the limited resources that a government has to spend on defense and conclude that expensive efforts focused only on this specific threat would be unrealistic due to alternative attack methods and uncertainties associated with the success of UAV and cruise missile attacks (p. 90). They recommend focusing on counter-intelligence, law enforcement

activity, and forensic investigation. Counter-intelligence activity specifically helps to prevent the use of UAVs and cruise missiles in terrorist attacks while forensic investigation helps deter future incidents if the perpetrators can be quickly found and brought to justice; law enforcement supports both of these activities. The authors suggest that increases in these areas will not only help combat the threat from UAVs but also increase security generally due to these activities are not specific to countering air threats.

In general, there is a dearth of research on the possibility of UAV threats to the U.S. homeland, especially the threat posed by terrorist groups or individuals operating within the United States. The "Novel Threats" study provides an excellent basis for further exploration of the threat that small-scale UAVs can pose to the U.S. homeland due to its extensive analysis of alternative attack methods and its examination of the operational benefits that UAVs provide. However, because the "Novel Threats" study focuses on all potential UAV and cruise missile threats, the authors may have been distracted from addressing the relevant threat posed by terrorists' use of UAVs. Therefore, this study will examine this threat from the standpoint that the commercialization of UAVs will make UAV technology that much more accessible to terrorists. In addition, this paper will provide concrete information on how terrorists might use UAVs in their operations. Finally, it will provide recommendations on courses of action to prevent and defeat the most commonly anticipated UAVs that terrorists can employ.

Current Regulation of UAVs in the United States

In 1981, the FAA issued Advisory Circular 91-57, providing guidance for how remote control aircraft hobbyists should fly their aircraft. The circular is one page long and states that model aircraft should be flown no higher than 400 feet at a sufficient distance from populated areas and that if they are flown within 3 miles of an airport, the hobbyist should coordinate with the airport to deconflict their

flights. Significantly, compliance with the FAA Advisory Circular is voluntary ("FAA Advisory Circular 91-57," 1981).

The FAA has since established rules for the operation of UAVs through a memorandum titled "Unmanned Aircraft Systems Operations in the U.S. National Airspace System (UAS Policy 05-01)," which established the process for UAS operators seeking Certificate(s) of Waiver or Authorization to operate within the national airspace system ("Unmanned Aircraft Operations in the National Airspace System," 2007). This memorandum created a de facto ban on the commercial use of UAVs within the national airspace system and thus, the FAA had not approved until very recently a single UAV for commercial operation within the national airspace system. However, public entities (federal, state and local governments, and public universities) have been able to apply for a Certificate of Waiver or Authorization (COA) to fly within the National Airspace System (Busting Myths, 2014). Hobbyists, on the other hand, have been able to fly drones by voluntarily complying with FAA Circular 91-57—flying under 400 feet above ground level (AGL), maintaining visual line-of-sight, and not using the UAV for any commercial purposes.

In an attempt to help speed up the integration of unmanned aircraft into the National Airspace System, Congress passed the FAA Modernization and Reform Act of 2012. The act mandated that the FAA ease the introduction of UAVs into the national airspace system. Section 332 (a) (3) states the FAA "shall provide for the safe integration of civil unmanned aircraft systems into the national airspace system as soon as practical, but not later than September 30, 2015." As part of the introduction of UAS into the NAS, the Act mandated that the FAA develop a publically available roadmap to provide guidance to potential UAS providers and users. Additionally, the Act established the use of the Arctic region for research and commercial purposes, designed to help develop the "processes to facilitate the safe operation of unmanned aircraft beyond line of sight" (FAA Modernization and Reform Act of 2012).

Furthermore, the act specifically limited the FAA's ability to regulate hobby/model aircraft as an unmanned aircraft, provided that the following is true:

1. The aircraft is flown strictly for hobby or recreational use;
2. The aircraft is operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization;
3. The aircraft is limited to not more than 55 pounds unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization;
4. The aircraft is operated in a manner that does not interfere with and gives way to any manned aircraft; and
5. When flown within 5 miles of an airport, the operator of the aircraft provides the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport) with prior notice of the operation (model aircraft operators flying from a permanent location within 5 miles of an airport should establish a mutually-agreed upon operating procedure with the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport) ("FAA Modernization and Reform Act of 2012," Section 336).

Up until very recently, the FAA had been aggressively issuing cease and desist orders to individuals and companies that it had suspected of utilizing UAVs and hobby R/C aircraft for commercial purposes. From 2012 to February 2013, 13 companies were issued such orders, and in May 2013 a real estate photographer who was using a hobby-grade craft to photograph homes was also issued a cease and desist order. It appears that a recent court ruling may lead to an increase in the commercialization of UAVs. The court case stemmed from a $10,000 fine the FAA had issued to a commercial UAV operator, Raphael Pirker, after he made a promotional video of the University of Virginia campus using a UAV. The FAA's stance was that any hobby R/C aircraft used for commercial purposes becomes a UAV, and is therefore subject to FAA regulations; however, the court determined that the policy memoranda the FAA issued were not sufficient for defining UAS and that FAA Notice 07-01 does not meet criteria for legislative rulemaking, which is required for imposing fines. In addition, the court found that the FAA's guidance within 07-01, stating that "Advisory Circular 91-57 only applies to modelers, and thus specifically excludes its use by persons or companies for business purposes" specifically brought into

question the size of the aircraft. The court told the FAA that it cannot treat model aircraft that falls within the parameters of Advisory Circular 91-57 as aircraft for businesses, and thus subject them to Federal Aviation Regulations, if it exempts the same model aircraft for hobbyists. Furthermore, the court brought into question the FAA's vague use of the term "business," stating that it "is not defined, so it is unclear if the term is limited to ongoing enterprises held out to the general public, or if it includes a one-time operation for any form or amount of compensation" (*FAA vs. Pirker*, 2014). This ruling may have temporarily opened the door for operators of UAS that fall within the parameters of Advisory Circular 91-57—primarily, flying within visual sight of the operator, under 400 ft. above ground level, and 3 miles from any airport.

Recent developments have thus suggested a change in the regulatory environment of UAVs. In June 2014, the FAA approved the first commercial UAV to operate over land in the national airspace system, issuing a Certificate of Waiver or Authorization to BP Corporation and AeroVironment—a leading manufacturer of UAVs—to operate their Puma UAV in Alaska to monitor BP's oilfields ("FAA Approves First Commercial UAS Flights Over Land," 2014). This is an important development for both UAV manufacturers and those who wish to employ UAVs for commercial purposes since it is an opportunity to refine the practices for operating in a more complex environment than Alaska. It also sets a precedent for flying commercial UAS within the national airspace system. Most recently, in September 2014, the FAA approved six aerial photography and video production companies to operate within the national airspace system as it found that "the UAS to be used in the proposed operations do not need an FAA-issued certificate of airworthiness based on a finding they do not pose a threat to national airspace users or national security" which is in compliance with Section 333 of the FAA Modernization and Reform Act (U.S. Transportation Secretary Foxx Announces FAA Exemptions for Commercial UAS Movie and TV Production, 2014).

The Commercialization of UAVs

Whether through court action or through the Congressionally mandated FAA Roadmap, one thing is clear: UAVs will be used commercially in the near future in the United States. Missy Cummings, a former Navy pilot and current Director of the Human Automation Lab at the Massachusetts Institute of Technology has stated:

> I think 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 (Hruby, 2014).

There are many potential commercial uses for UAVs, ranging from monitoring oil fields and farms to transporting goods to conducting search and rescue operations. One example of this new demand and use for UAVs is demonstrated by University of Nebraska journalism professor Matt Waite, who spent nearly 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. It is controlled by a tablet computer using a digital map—one simply touches the screen and tells it where to fly. Such a system would be extremely useful for reporting on fires, floods, hurricanes and tornadoes—just about any situation where it might be prohibitively dangerous to fly a manned aircraft. In addition, the X100 UAV requires no special piloting skills. Mr. Waite recalls, "I went to the sales guy and said, here, take my money, how do I take this thing home?" He was told that it was $65,000 and it was illegal in the U.S. (Hruby, 2012).

Figure 1: AeroVironment's Qube UAV and Control Unit

Another example of a potential use for UAVs is demonstrated by AeroVironment's Qube UAV that it is

marketing to first responders for both search and rescue operations and for conducting surveillance. The Qube can be stored in a vehicle trunk, has vertical take-off and landing capability, 40 minute flight endurance, and high resolution color and thermal cameras. It is controlled by a ruggedized tablet, again requiring no specialized pilot training (Qube Data Sheet, 2014).

According to Cummings, "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" (Hruby, 2014). Cummings describes the changes that are coming to skill-based fields. She predicts that with advances in artificial intelligence and robotics, we will start seeing a shift to more knowledge-based professionals, as we allow computers to execute complex, skill-based tasks, such as flying aircraft, driving cars, and conducting surgery. This shift has already affected the aviation field; as a former Navy F-18 pilot, Cummings points out that pilots today don't actually fly aircraft in the same manner as their predecessors did. Today, computer controls augment the pilot's ability to maintain control of the aircraft through complex fly-by-wire systems, enabling the pilot to concentrate more on other tasks, such as finding and engaging the enemy. UAVs are accelerating this trend; instead of having to understand all the complex controls of an aircraft—as a pilot must—UAV operators are performing what she calls human supervisory control. Human supervisory control is a higher level function where instead of controlling the machine, the operator "encourages" it to do what the operator wants (Cummings, 2012). Thus you have UAVs that fly themselves to waypoints without the operator having to know the first thing about aerodynamics.

In a recent experiment Ms. Cummings conducted in conjunction with Boeing called the 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. 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 could simply click on a digital map and tell the micro UAV where to fly. Using nudge control, the operator had a forward facing view from the UAV's camera and was able to fly the UAV by tilting the iPhone in the direction the user wanted it to go (utilizing the iPhone's built in accelerometer). Additionally, researchers selected random passersby to control the UAV to demonstrate how a minimally trained operator could easily operate a small UAV. The test subjects received three minutes of instruction and were able to successfully control the UAV and perform tasks, such as 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 the operator to micromanage the behavior of the vehicle, enabling the operator to concentrate on the more mission-relevant part of command and control (Koehler, 2011).

Human supervisory control is one of the largest advantages of UAV technology, as it allows experts in other fields to control these aircraft. This can be a significant cost savings for businesses because not only are UAVs less expensive to build and operate than manned aircraft, but they also have the potential to be used by relatively unskilled operators. Providing user-friendly human supervisory control capabilities is probably the greatest benefit that UAV technology companies can provide consumers. Unfortunately, providing such increased accessibility will also make UAVs even more attractive to those who would use them for nefarious purposes.

Terrorism as Communication

One of the premises of this paper is that terrorism is communication through violence. Joseph Tuman writes in his book, *Communicating Terror*, about how terrorists engage in violence to send a message to a target audience. Thus, the tactical outputs of a terrorist action are not 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. Tuman writes: "The primary audience will be those who witness and observe the

violence and destruction and engage in discourse about what they have seen" (p. 34). Thus, the message is not the violence or destruction itself, but rather is either embedded within the violence or follows from it as the violence is designed to gain attention (p. 32). Failing to address terrorism as a communicative process was one weakness of the "Novel Threats" study, and we will look at how their examination of tactical outputs could lead them to believe that UAVs fall into a "niche threat" category.

Typically, higher casualties can produce larger media sensations, which in turn help to transmit the terrorist's message. However, high payoff targets, which include targets that can be prosecuted on live television in front of large audiences, will also attract terrorists. Such was the case during the sensational 1972 Munich Olympic attacks, where the terrorists knew they could garner live international media attention even though there were relatively few casualties. The 9/11 attackers also orchestrated such an attack with United Airlines 175, which flew into the South Tower of the World Trade Center on live television. They knew that after the first attack, the nation's media would focus on the Twin Towers, during which time the second aircraft would hit. In a digital era where many people no longer watch live television, sporting events offers one of the last bastions of a large live audience without the need for coordinating large attacks, which may be particularly lucrative targets for terrorists using UAVs.

When considering a direct attack with a UAV, the authors of the "Novel Threats" study claim that there are four primary determinants of success: warhead effectiveness (measured by weight of payload), type of ordinance delivered, accuracy of the weapon, and probability of reaching the target. The study focuses on the casualty rate that an attack can produce by examining and comparing the payload capacity of various delivery vehicles. What the study fails to take into account is the lucrativeness of a particular target. Instead, the authors take a rather straightforward view of the goals of employing violence, stating that "violence produces specific 'tactical outputs'" which include:

- Targeted individuals are injured or killed;
- Property is damaged or destroyed;

- An activity in or by the target state is disrupted (p. 13).

The authors claim that these tactical outputs must be linked to achieving goals, resulting in changes in the targeted state's behavior. While this makes sense, it leads them to a conclusion that UAVs are unlikely hosts for terrorist weapons and will remain a "niche threat." By failing to address the idea that terrorism is communication through violence and by failing to look at the lucrativeness of a target, the authors discount the possibility that terrorists may choose an accurate delivery method that can circumvent perimeter defenses, such as a UAV, in order to strike at a high payoff target, garnering them a high degree of attention and infamy. The "Novel Threats" study unfortunately fails to address terrorists' propensity for choosing targets for their symbolic significance or the media attention that the attack can produce and, as a result, comes to the mistaken conclusion that UAVs are not a probable threat in regards to being used by terrorists.

Terrorist Use of UAVs

So far, this paper has explained that 1) UAVs will be integrated into the national airspace system in the near future, 2) there is currently a market for the commercial use of UAVs, 3) that market will be satisfied by companies providing user-friendly ways to operate UAVs, and 4) terrorists use violence as a communication tool and will be attracted to the idea of using UAVs to strike high payoff targets to communicate to a target audience. This paper will now focus on some of the practical aspects of UAV technology and how terrorists might conduct operations employing UAVs in the United States.

UAVs are attractive to terrorists for several reasons. The first reason is the inherent mobility that UAVs provide. UAVs provide the ability to conduct attacks over perimeter defenses. While many potential terrorist targets in the U.S. lack any sort of 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" (Jackson, Frelinger, Lostumbo, and Button, 2008,

p. 29). Thus UAVs provide an increased ability to strike at high-profile or high-value targets. For example, it is not hard to imagine the media sensation that would occur if terrorists were able to successfully fly a high-speed, weaponized UAV into a huddle of football players during the next Super Bowl. Another frightening example would be to fly one towards the President at the next Presidential 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 was perhaps best exemplified by the interruption of a German campaign event in Dresden where German Chancellor Angela Merkel and Defense Minister Thomas de Maiziere were speaking. During the event, a spectator flew a Parrot quad-rotor UAV onto the stage where Merkel and de Maiziere were speaking. While Merkel seemed amused, security personnel were not. Had the operator's intent not been simply to make a point about drone surveillance, that day could have turned tragic.

Figure 2: UAV hovering near Chancellor Merkel

In addition, the mobility of UAVs can provide a platform for terrorists to conduct surveillance of targets. UAVs have been extremely successful at conducting surveillance for the U.S. and other governments and there is no reason to believe that terrorists could not employ them similarly—if more crudely. The ability to conduct surveillance and even direct targeting using UAVs can be enhanced by adding different payloads, in addition to the now typical high resolution camera. For instance, during a security conference in 2011, one presenter demonstrated "a drone that flew silently and identified and tracked human targets by locking in on their cellphone signals" (Hruby, 2012). Certainly, this type of technology in terrorist hands would pose great danger to high-risk targets, such as political figures, high-ranking members of business, and sports and entertainment professionals.

Another reason terrorists may adopt UAVs is for their ability to lower the risks to the terrorists themselves. While some terrorists have shown their willingness to sacrifice themselves for their cause, there are others who will be attracted to the ability to commit a terrorist attack with a much lower risk of apprehension. The MAE VUE project demonstrates how the UAV controller can be half a world away from the UAV. Someone would certainly need to be on the ground to deploy the UAV; however, if the UAV was equipped with a 3G or 4G cellular phone, a controller could operate the UAV using the internet from virtually anywhere. Such operations would significantly complicate law enforcement investigations because of the limited footprint that terrorists would need on the ground near the attack. Additionally, because a weaponized UAV could be launched at range and fly into the target, law enforcement would be forced to greatly expand the search area for potential witnesses and/or physical evidence.

A third reason that UAVs will be an attractive delivery method to terrorists is their increased accessibility and relatively low cost. Terrorists can build UAVs today for under $10,000, which is well within the costs of historical terrorist attacks. The website DIYDrones.com is designed to help drone enthusiasts gather and exchange ideas and information about how to build and operate drones. Through DIYDrones.com, a person can learn to build aircraft, equip them with first person viewing cameras, telemetry systems, and various methods of controlling the UAV. The three most critical pieces to turning a R/C model aircraft into a UAV are a GPS unit, an autopilot, and a ground station or control unit. GPS units are readily available in most smartphones and autopilots can be purchased for anywhere between $200 and $20,000. For instance, the Kestrel Autopilot can be purchased for either fixed or rotary-wing UAVs for between $8,000 and $9,000 with the ground station costing an additional $3,700 to $5,000 with additional support for video surveillance and laser range-finding (Kestrel Autopilot Price Sheet, 2012). Alternatively, Australian company Cloud Cap Technologies offers the Piccolo Nano Autopilot specifically for small UAVs and is expected to be priced in the $1,000 range, not including the ground station components (Cloud Cap Technology Launches Piccolo Nano Autopilot for Small UAS,

2013). Most significantly, the company 3D Robotics specializes in catering to the drone hobbyist, and offers even less expensive autopilots in the $200 range for sale through DIYDrones.com. In addition, these autopilots can be controlled using a tablet or laptop computer, dramatically increasing the accessibility of UAV technology in terms of both cost and reduced specialized equipment. The ability to build a UAV by utilizing the expertise on DIYDrones.com is particularly troublesome for intelligence personnel and law enforcement and particularly attractive to terrorists because it may be impossible to sort out hobbyists from potential terrorists.

Whether a terrorist chooses the DIY route or purchases a system outright, the costs associated with small UAVs falls within the budget of many terrorist operations. For instance, the cost of the 2002 Bali nightclub bombing was approximately $50,000; the 2004 Madrid train bombing was believed to have cost between $10,000 and $15,000; and the 2005 London transit system bombing cost about $2,000. The 9/11 attacks are estimated to have cost nearly half a million dollars, but those attacks are on a different scale from a small UAV attack (Kaplan, 2006). A $2,000 to $10,000 investment in a UAV falls in line with the costs of most other terrorist attacks. Furthermore, as time goes on, one can expect that the technology associated with UAVs, especially with hobbyist equipment, will become more accessible and even less expensive. Chris Anderson, founder of DIYDrones.com and co-founder of 3D Robotics, has stated, "if we make the technology cheap, easy and ubiquitous, regular people will figure it out" (Hruby, 2012).

Practical Application

Imagining how a UAV can be utilized to strike a high-profile target is not far-fetched. AeroVironment's Switchblade is a military UAV designed to be rapidly deployable, easily controlled and is equipped to take out soft targets. Weighing 2.8 kg with a 0.45 kg payload, the Switchblade can reach

an estimated top speed of 80-100 mph (2010-2011 UAS Yearbook, 2010 and Mortimer, 2011 Jan). AeroVironment's website describes:

> The Switchblade® is designed to provide the warfighter with a back-packable, non-line-of-sight precision strike solution with minimal collateral effects. It can rapidly provide a powerful, but expendable miniature flying intelligence, surveillance and reconnaissance (ISR) package on a beyond line-of-sight (BLOS) target within minutes. This miniature, remotely-piloted or autonomous platform can either glide or propel itself via quiet electric propulsion, providing real-time GPS coordinates and video for information gathering, targeting, or feature/object recognition. *The vehicle's small size and quiet motor make it difficult to detect, recognize and track even at very close range*. [Emphasis added.]

The Switchblade may well never fall into terrorist hands in the United States due to restrictions on the sale of lethal UAVs to civilians; however, the principle of the Switchblade—a small, fast UAV with an onboard camera for targeting and capable of holding a small payload—provides an important example of the potential of this threat.

Figure 3: X8 Flying Wing

One hobbyist R/C aircraft that can be converted into a UAV and could be particularly promising for potential terrorists is the X8 Flying Wing. The X8 has ample space for electronics and a small explosive (see Figure 4.). It weighs a mere 2.2 kg, and it is capable of holding an additional 2.3 kg payload (Aeroelectronics X8 Flying Wing Datasheet, 2014). According to one UAV enthusiast, his X8 is capable of a cruise speed of 50-60 mph with a maximum speed of 70 mph in level flight with 35 minutes of flight time. Another user reported a flight time of 85 minutes with his X8, a difference caused by the use of different number and types of batteries on board and the amount of time at full throttle (X8 flying wing, 2011). The base kit can be purchased for $160, not including the engine

Figure 4: Internal Payload Capacity of X8

or other electronics. Including an engine, autopilot, and first-person view HD camera and video transmitter, one can expect to spend anywhere from $2,000 to $10,000. Alternatively, the Spain-based company Aeroelectronics offers a complete turn-key solution for the X8 Flying Wing complete with a ground station, its U-Pilot autopilot, and a sensor suite. Aeroelectronics claims that their version of the X8 has an endurance of up to 3 hours and can use waypoint navigation and dead reckoning, if GPS signals are lost. Aeroelectronics does not publicly release the cost of this complete system, but based on the published cost of their ground station and U-Pilot system, this system is estimated to cost slightly over $20,000.

We have already seen the first hints of UAV terrorism in the United States. In 2011, Rezwan Ferdaus, an American born al-Qaeda supporter planned to launch attacks on the Pentagon and the U.S. Capitol buildings using remote controlled hobby aircraft fitted with GPS and an autopilot. Fortunately, the C-4 that Ferdaus was trying to acquire was harder to come by than the UAV he was building. Ferdaus was arrested after purchasing what he thought was 25 lbs. of C-4 from undercover FBI agents (Dolmetsch, 2011).

It is important to point out that once a terrorist is able to acquire all the necessary materials, a UAV attack would be very difficult to thwart. Again, the benefit of UAVs is their ability to bypass physical security barriers, and any open-air event—from major sporting events to Presidential Inaugurations—would be vulnerable. UAVs like the X8 could be launched 25 or more miles away from the intended target. Running on an electric motor which is fairly quiet, it can be painted to blend in with the sky, reducing the ability to detect it both audibly and visually. Furthermore, the small size of UAVs makes them difficult to detect on radar, and by the time they are detected, their high speed (70+ miles per hour) can make them difficult to defeat or evade.

One final risk factor with the commercialization of UAVs is the potential for terrorists to intercept the signals from legitimate UAVs and then take control of the UAV. In 2009, it became public

knowledge that Iraqi militants used a $26 piece of Russian software intended to steal satellite television to intercept the real-time video feed from U.S. surveillance drones flying over Iraq. In 2011, a keylogging computer virus infected the ground stations of U.S. Predator and Reaper RPAs (Goodman, 2013). While there is a technological leap between either intercepting video feeds or infecting a computer with a virus and being able to take over a UAV's command signal, there is certainly a potential risk that terrorists will develop this capability. This risk may be very small for the U.S. RPA fleet of Predators and Reapers because their control signals are encrypted (Shachtman and Axe, 2012). However, there are currently no regulations governing encryption of private UAV control signals, and due to the added cost of encryption, there may be resistance to it from both companies and hobbyists alike. Unencrypted command channels would make it much more likely that terrorists could "hijack" commercial UAVs and turn them into miniature cruise missiles. This is less of a threat today than another plot similar to Rezwan Ferdaus's; however, if Missy Cummings is correct that in 15 years from now, we will be seeing UAVs littered across the skyline, then this may be a real threat to consider.

Defensive Approach

As the "Novel Threats" study points out, "there is a temptation to begin by examining active defense systems designed to shoot down these threats" (2008, p. 73). Active defense—neutralizing a threat once it is airborne or the air attack is in progress—is only part of a broader concept of defense against air attack. Unfortunately, one of the benefits of UAVs for terrorists is that they are not a traditional air defense threat, thereby complicating the role of active defense. While active defense is a critical part of air defense, it is important to also consider passive defense and intelligence operations.

Active Defense

The UAVs we have discussed are much smaller than traditional manned aircraft. In a publically released Army Research Laboratory report, a remote control aircraft roughly the size of the UAS we have examined had an average radar cross section (RCS) of 14.55 dBsm, which is nearly the RCS of a large bird (20 dBsm) (Pizzillo, 2005 and Spruyt and van Dorp, 1996). Decibels referenced to a square meter, or dBsm , is a measure of how much a particular object will reflect radar energy. For comparison, a commercial airliner could have a dBsm around 30, while a small jet might be in the 0-5 dBsm range (Stimson, 1983). Not only are UAVs harder to detect due to their size, but because they fly at similar speeds and altitudes to birds there is additional risk of not detecting them. This is because it is usually not desirable for surveillance radars to detect birds as they end up cluttering the radar operator's air picture. Therefore it stands to reason that since UAVs have similar kinematics to birds, surveillance radars may ignore those particular objects. Therefore, for high-risk events and known appearances of high-risk personnel it may be necessary to bring in radars that have the fidelity to detect such small objects and operators trained to distinguish between birds and UAVs, as it is unlikely that the surveillance radars the FAA uses to monitor air traffic within the National Airspace System will be able to detect UAV threats.

To make matters worse, even if it is possible to detect UAV threats, the options for dealing with the threat are limited. First, in urban environments, where attacks are more likely, law enforcement and military will be averse to shooting UAVs down due to the fact that any projectile used 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[*]. UAVs made of Styrofoam, fiberglass or similar materials could likely take several hits and remain operational unless a critical component was hit—such as the engine, navigation or receiver. The use of an explosive ordinance could help alleviate this issue but may add additional concern about collateral damage and

[*] Quad-copters, such as the Qube, are more susceptible to kinetic fires due to their reliance upon multiple motors to maintain lift.

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 in order to adequately defend the area. This 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 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 that can be anticipated. By jamming the most common frequencies, one could effectively eliminate the ability of the UAV operator to conduct accurate targeting within the denied area.

There are three basic points to take into consideration when considering jamming a UAV command channel:

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

In order to control the UAV, the control station and UAV need to communicate. Theoretically, radio waves 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 is known as the inverse square law of physics, and it is the major determinant of the range in which an UAV control station can make contact with a receiver. Antenna gain also affects this distance in that the better the antenna is able to translate power into radio waves, the further the usable signal will travel. Third, the signal needs to overcome the radio frequency 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.

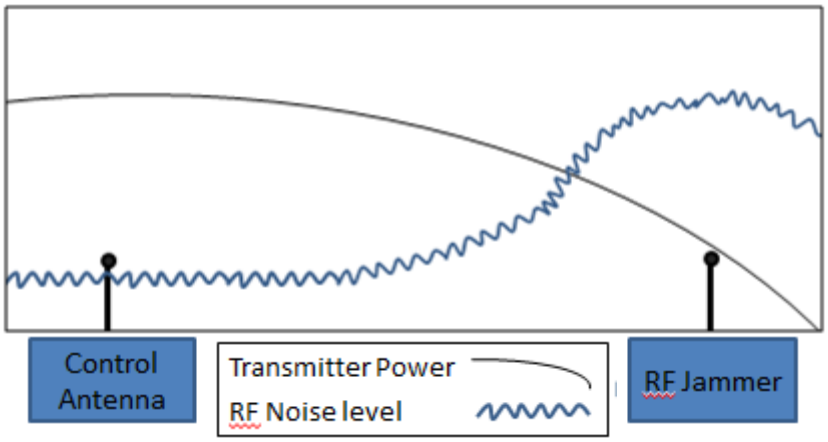

Figure 5: Simplified RF Jamming Effects

Jamming could be particularly effective against UAVs because of the inverse square law. The further the UAV travels from the control station and the closer it moves towards the jammer (presumably the jammer would be collocated with the asset that is being defended), the harder it is for the transmitter to overcome the RF noise of the signal jammer. Figure 5 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. In order to overcome the signal jammer, the terrorist would then have to change frequencies, increase power or get closer to the target area, none of which are particularly easy.

In order to change frequency bands, the terrorists would have to understand how to manipulate the transmitter and receiver. This is not a trivial task, and without significant knowledge of electrical and radio frequency engineering, it would be an unlikely path for terrorists. Similarly, the amount of transmit power is regulated, so it would also be difficult to change the output power of the transmitter without specific electrical and radio frequency engineering knowledge. Finally, if the operator moves closer to the target, some of the advantages of using an UAV, such as stand-off distance, begin to be eliminated. Forcing the terrorist to move closer to the target raises the operational risk for the terrorist since he could then be observed and interrupted mid-operation. In fact, the likelihood of being caught can increase to the point at which it becomes prohibitive for the terrorist to conduct the operation.

On the other hand, one of the downsides to using jamming against UAVs is that there are many users of the electromagnetic spectrum and jamming will necessarily disrupt other users due to some of

the unique features of UAV and R/C aircraft controls. According to the Academy of Model Aeronautics, remotely controlled models 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 (Frequency Chart for Model Operation, 2014). Additionally, telemetry kits that send back video and positioning information can usually be found in the 900 MHz, 2.4 GHz, and 5.8 GHz ranges. While the single channel control frequencies would not be particularly problematic to jam, the 900 MHz, 2.4 GHz, and 5.8 GHz ranges are part of what is known as the industrial, scientific and medical (ISM) bands, and jamming them may create public backlash. Common devices that use these bands include Bluetooth devices, cordless phones, wireless internet protocol networks, and even microwave ovens. Jamming would likely have to be used sparingly and be limited to extremely high profile events during which citizens would be accepting of the loss of some technological services. To help mitigate interference, jamming could be used in conjunction with radars so that the jammer would be turned on only if any UAVs were detected coming into the restricted area. In this case, specialized radars designed to detect small objects such as UAVs would need to be deployed with the jammer. This would still likely be a less risky and less costly course of action than a kinetic option to defeat the threat. A kinetic system also requires a radar for detection; but, unlike a kinetic system, a jamming system could likely be operated by the same person operating the radar and/or radar picture.

Another complicating factor would be the use of cellular networks to control UAVs. In order 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 by the MAE VUE experiment. In order to jam such signals, it would require jamming cellular services within a given area. Again, the public would likely disapprove of persistent jamming that would interrupt service to their cellular phones and wireless mobile devices. However, if incorporated with a

radar warning system or used with credible intelligence, such jamming of cellular services and denials of service would likely be very minimal.

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 seems fairly clear. The use of a warning radar designed to detect such a threat and a jamming system seem to be a highly effective way defeat it.

Passive Defense

In addition, one of the best methods of mitigating a UAV terrorist attack is through a strong passive defense. According to the military's Joint Publication 3-01: Countering Air and Missile Threats, passive defense is measures "taken to minimize, mitigate, or recover from the consequences of attack aircraft and missiles" (p. V-19, 2012). 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-profile events indoors. Most commercial structures provide adequate physical protection—hardening—from the warheads that small UAVs would be able to carry, approximately 1-5 kilograms. Merely by hosting events inside, one could greatly reduce the likelihood of even being targeted. Additionally, while it may be possible to fly a UAV inside a structure, it is unlikely to be a viable course of action for several reasons. First, fixed-wing UAVs would not be feasible at all due to their speed and space requirements for maneuvering, and controlling a quad- or multi-rotor UAV within a structure would likely prove difficult at best. Routes inside the structure would have to be planned out precisely and there would need to be enough headspace for the UAV to travel above people to get to its intended target. Furthermore, the structure will likely eliminate direct LOS control of the UAV because the 2.4 GHz control channel most common for hobby-built UAVs will not

travel well through a commercial structure. Therefore, the only practical method of controlling a UAV will then be through a cellular network or some kind of Wi-Fi hotspot. Such a method would significantly raise the operational risk of the attack due to increased complexity and the risk that the signal could be lost at some point inside the structure, rendering the UAV inoperational. All of this additional risk would help deter a terrorist from choosing such a target or would compel him to choose a different delivery method.

In the case of an outdoor event, passive defenses can still be implemented. By utilizing radars, which provide advance warning, high-risk personnel can then be moved to a sheltered area if a UAV were to enter into an unauthorized area. In order to defend against small, hobby-scale UAVs, this shelter could range from an armored vehicle to a nearby building. While there still may be an attack, the government can take steps to protect the targeted individuals from the attack. If UAV attacks are thwarted in this manner, then passive defense can act as a deterrent for future attacks since terrorists will believe that their weapons cannot reach their desired target.

Finally, other forms of passive defense that help protect high-risk personnel from being targeted by terrorist attacks will continue to work against UAVs. 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 will make it harder for all terrorists to target high-risk personnel, not just against possible UAV attacks, and it is recommended these measures continue to be used.

Intelligence

Currently, almost all of the technology related to hobby-grade R/C aircraft and UAVs is freely available, and it would be nearly impossible to cease the proliferation of this technology (Lele and Mishra, 2009). However, it may be possible to try and monitor those who are building UAVs that could

be operated beyond visual range. The one piece of technology that sets UAVs apart from R/C aircraft is navigational control. Navigational control can actually be separated into two distinct pieces of technology—GPS receivers and autopilots. Of these two devices, 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 an UAV require a highly specialized piece of technology, law enforcement and intelligence agencies have something they can specifically look for in screening for potential terrorist threats.

As the "Novel Threats" study indicated, it would be beneficial to reach out to businesses to make them aware of the potential for misuse of their products and to solicit their cooperation in reporting suspicious purchases. 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 a known strong dissatisfaction with the government, 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) UAVs that include an autopilot and are capable of holding a 1-5 kg payload (or more), likely UAVs for terrorist use, could be monitored. Therefore, it is recommended that provisions be put in place that would enable law enforcement and appropriate intelligence agencies to monitor the 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. With the pressure from companies to lift regulations banning the commercial use of UAVs and the Congressional mandate to the FAA to incorporate UAVs into the national airspace system, it is only a matter of time before UAVs are more common-place in the United States. We are currently seeing the beginning stages of this process with the FAA granting permission to six companies to use UAVs within the National Airspace System in the movie and video production industry. A more

permissive regulatory environment will lead to more commercial demand and UAV companies and technology providers will endeavor to make that technology even more accessible to both businesses and individual hobbyists in order to increase their marketability. Unfortunately, commercial accessibility will also make such technology more accessible and attractive to terrorists though advances in human supervisory control and reduced system cost.

While commercial UAS may be difficult for terrorists to acquire—at least in the current regulatory environment market—hobby-grade UAVs are currently well within reach of terrorists. Terrorists will seek to acquire these hobby-grade UAVs because the offer significant potential benefits—bypassing defensive perimeters, providing a relatively safe method of attack, and cost-efficiency. Furthermore, the ability to bypass defensive perimeters enables the potential to strike high payoff targets, such as major sports events or high-ranking political figures. Finally, if terrorists learn to use UAV technologies and acquire the requisite equipment, defeating attacks in progress will be problematic. Even hobby-grade UAVs can travel at high speeds and can be difficult to detect—both visually and on radar. Terrorists will seek to employ such UAVs because the allow them to strike at high payoff targets that would otherwise be inaccessible due to perimeter defenses. Terrorists use violence as communication and they understand that it is not necessary to kill a lot of people to send a message (although it can help). Targeting high-payoff targets can serve the dual function of striking at a target that will provide immediate media coverage and depicts weakness in the government for its inability to protect high-risk personnel and events.

While UAVs may be more difficult to defeat than traditional air threats due primarily to difficulties with detection—not only requiring a radar, but a radar that can detect low, slow and small objects, yet there are measures that the government can take in order to help mitigate the threat from terrorist use of UAVs. Hosting high-risk events and known appearances of high-risk personnel indoors are probably the single biggest factors that can protect against the small UAV threat. It 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 events indoors. Events such as the Boston Marathon will still provide lucrative targets for terrorists; however, risk can be mitigated through an active defense. Radar assets can be brought to bear to detect these threats, providing early warning to enhancing passive defense. In addition, jamming can be utilized as part of an active defense to disable UAVs once they are detected entering into a restricted area. Finally, by gaining the ability to monitor who purchases autopilots and COTS UAVs that have built-in autopilots and a payload capability can help law enforcement and intelligence operations discover those who would use UAVs (among other tools) to harm us.

Unfortunately, UAVs complicate matters for security personnel and defensive planners. They democratize air power—even if currently the power gained is slight. They force the consideration of the third-dimension when thinking about potential threats for high-risk personnel and events. This is a growing threat and one that the U.S. Government should be preparing for.

Bibliography:

2010-2011 UAS Yearbook (2010, June). *The Global Perspective – 8th Edition.* Retrieved from: http://uas.usgs.gov/UAS-Yearbook2010/pdf/P161-195_World-UAS-Reference-Section.pdf

Aeroelectronics X8 Flying Wing Datasheet (2014). *Aeroelectronics*. Retrieved from: http://www.airelectronics.es/products/x8_brochure.pdf?PHPSESSID=itg7avr0agek17jv0o6njqt7h3

Busting Myths (2014). *Federal Aviation Administration*. Retrieved from: http://www.faa.gov/news/updates/?newsId=76240

Cloud Cap Technology Launches Piccolo Nano Autopilot for Small UAS (2013, March 3). *UAS Vision*. Retrieved from: http://www.uasvision.com/2013/03/22/cloud-cap-technology-launches-piccolo-nano-autopilot-for-small-uas/

Cummings, Missy (2012). Can a "computer co-pilot" help anyone be a surgeon?*TEDTALK2012*. Retrieved from: http://www.tedmed.com/talks/show?id=7355&videoId=6923&ref=about-this-talk

Davis, Lynn E., Michael J. McNerney, James Chow, Thomas Hamilton, Sara Harting, Daniel Byman (2014). Armed and Dangerous? UAVs and U.S. Security. *Rand Corporation*. Retrieved from: http://www.rand.org/pubs/research_reports/RR449.html

Deener, Sarah (2014, June 11). FAA approves first commercial unmanned flights over land. *Aircraft Owners and Pilots Association*. Retrieved from: http://www.aopa.org/News-and-Video/All-News/2014/June/11/FAA-approves-first-commercial-unmanned-flights-over-land.aspx

Dolmetsch, Chris (2011, September 29). Massachusetts Man Charged With Plotting Airborne Pentagon Attack. *Bloomberg Businessweek.* Retrieved from: http://www.businessweek.com/news/2011-09-29/massachusetts-man-charged-with-plotting-airborne-pentagon-attack.html

FAA Advisory Circular 91-57 (1981, June 9). *Federal Aviation Administration*. Retrieved from: http://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentid/22425

FAA Approves First Commercial UAS Flights over Land [press release](2014, June 10) Retrieved from: http://www.faa.gov/news/press_releases/news_story.cfm?newsId=16354

FAA Modernization and Reform Act of 2012 (2012). House of Representatives Report 112-381. Retrieved from http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt381/pdf/CRPT-112hrpt381.pdf

FAA Notice 07-01: Unmanned Aircraft Operations in the National Airspace System (2007, February 13) Federal Register Vol. 72, No. 29. Retrieved from: http://www.gpo.gov/fdsys/granule/FR-2007-02-13/E7-2402

Federal Aviation Administration vs. Pirker, National Transportation Safety Board Office of Administrative Law Judges, Docket CP-217 (2014, March 6). Retrieved from: http://www.kramerlevin.com/files/upload/PirkerDecision.pdf

Frequency Chart for Model Operation (2014). *Academy of Model Aeronautics*. Retrieved from: http://www.modelaircraft.org/events/frequencies.aspx

Gallagher, Sean (2013, September 18). German chancellor's drone "attack" shows the threat of weaponized UAVs. *ArsTechnica*. Retrieved from: http://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/

Goodman, Marc (2013, January 31). Criminals and Terrorists Can Fly Drones Too. *Time*. Retrieved from: http://ideas.time.com/2013/01/31/criminals-and-terrorists-can-fly-drones-too/

High Speed FPV UAV 200kmh+ with HD Hero, suggestions? (2011, February 20) *DIYDrones.com*. Retrieved from: http://diydrones.com/forum/topics/high-speed-fpv-uav-200kmh-with

Hruby, Patrick (2012, March 14). Out of 'hobby' class, drones lifting off for personal, commercial use. *The Washington Times*. Retrieved from: http://www.washingtontimes.com/news/2012/mar/14/out-of-hobby-class-drones-lifting-off-for-personal/?page=all

Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap (2013). *US Department of Transportation, Federal Aviation Administration.* Retrieved from: http://www.faa.gov/about/initiatives/uas/media/uas_roadmap_2013.pdf

Jackson, Brian A., David R Frelinger, Michael J. Lostumbo, Robert W. Button (2008). Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles. *Rand Corporation*. Retrieved from: http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG626.pdf

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

Kestrel Autopilot Price Sheet. (2012, October 16). *Lockheed Martin*. Retrieved from: http://www.lockheedmartin.com/content/dam/lockheed/data/ms2/documents/procerus/procerus_pricing_022713.pdf

Kershner, Isabel (2013, April 25). Israel Shoots Down Drone Possibly Sent by Hezbollah. *The New York Times*. Retrieved from: http://www.nytimes.com/2013/04/26/world/middleeast/israel-downs-drone-possibly-sent-by-hezbollah.html?_r=0

Koebler, Jason (2014, February 6). These Are the Companies the FAA Has Harassed for Using Drones. *Motherboard*. Retrieved from: http://motherboard.vice.com/blog/these-are-the-companies-the-faa-has-harassed-for-using-drones

Koehler, Tom (2011, August 29). Smart phones fly mini drones. *Boeing*. Retrieved from: http://www.boeing.com/Features/2011/08/corp_drone_08_29_11.html

Lele, Ajay and Archana Mishra (2009). Aerial Terrorism and the Threat from Unmanned Aerial Vehicles. *Journal of Defense Studies, Vol 3. No 3*. Retrieved from: http://idsa.in/system/files/jds_3_3_alele_amishra.pdf

Miasnikov, Eugene (2004). Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects. *Moscow Institute of Physics and Technology: Center for Arms Control, Energy and Environmental Studies*. Retrieved from: http://www.armscontrol.ru/uav/UAV-report.pdf

Mortimer, Gary (2011, January 1). Lethal Miniature Aerial Munition System (LMAMS) to be deployed soon?*sUAS News*. Retrieved From: http://www.suasnews.com/2011/01/3260/lethal-miniature-aerial-munition-system-lmams-to-be-deployed-soon/

Mortimer, Gary (2011, September 2) U.S. Army Awards AeroVironment $4.9 Million Contract for Switchblade Agile Munition Systems and Services. *sUAS News*. Retrieved from: http://www.suasnews.com/2011/09/7892/u-s-army-awards-aerovironment-4-9-million-contract-for-switchblade-agile-munition-systems-and-services

Puma AE UAS (n.d.) *AeroVironment*. Retrieved from: http://www.avinc.com/public-safety/solution/puma-ae-uas

Puma Data Sheet (n.d.). *AeroVironment*. Retrieved from: http://www.avinc.com/downloads/DS_Puma_Online_10112013.pdf

Qube Data Sheet (n.d.). *AeroVironment*. Retrieved from: http://www.avinc.com/downloads/Qubedatasheet.pdf

Rodkin, Dennis (2014, May 29) FAA to drone photographer: Cease and perhaps desist. *ChicagoBusiness.com*. Retrieved from: http://www.chicagobusiness.com/article/20140529/NEWS07/140529748/faa-to-drone-photographer-cease-and-perhaps-desist

Scan Eagle System (n.d.) *Insitu*. Retrieved from: http://www.insitu.com/systems/scaneagle

Shachtman, Noah and David Axe (2012, October 29) Most U.S. Drones Openly Broadcast Secret Video Feeds. *Wired*. Retrieved from: http://www.wired.com/2012/10/hack-proof-drone/

Spruyt, J.A. and Ph. Van Dorp (1996, August). Detection of Birds by Radar. *TNO Physics and Electronics Laboratory*. Retrieved from: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA321060

Stimson, George W. (1983). *Introduction to Airborne Radar*. Glendale, CA: Hughes Aircraft Co.

Switchblade (2014). *AeroVironment*. Retrieved from: https://www.avinc.com/uas/adc/switchblade/

Taylor, Guy (2013, November 10). U.S. Intelligence Warily Watches for threats to U.S. now that 87 Nations Possess Drones. *The Washington Times*. Retrieved from: http://www.washingtontimes.com/news/2013/nov/10/skys-the-limit-for-wide-wild-world-of-drones/?page=all

Unmanned Aircraft General Facts (2014, May 16). *Federal Aviation Administration*. Retrieved from: http://www.faa.gov/about/initiatives/uas/uas_faq/?print=go#Qn1

U.S. Transportation Secretary Foxx Announces FAA Exemptions for Commercial UAS Movie and TV Production [Press Release] (2014, September 25). Retrieved from: https://www.faa.gov/news/press_releases/news_story.cfm?newsId=17194

Volovelsky, Uri (2014, June) Civilian Uses of Unmanned Aerial Vehicles and the Threat to the Right to Privacy—An Israeli Case Study. *Computer Law and Security Review, Vol. 30. Issue 3* pp. 306-320. Retrieved from: http://www.sciencedirect.com/science/article/pii/S0267364914000600

X8 flying wing(2011, December 13) *DIYDrones.com*. Retrieved from: http://diydrones.com/profiles/blog/show?id=705844%3ABlogPost%3A736012&commentId=705844%3AComment%3A808803&xg_source=activity