Global Security and Intelligence Studies

Volume 2
Number 1 *Fall 2016*

Article 6

2016

An Assessment of Lone Wolves Using Explosive-Laden Consumer Drones in the United States

Matthew Hughes
American Public University System

James Hess
American Public University System

An Assessment of Lone Wolves Using Explosive-Laden Consumer Drones in the United States

Matthew Hughes[A] & James Hess[B]

The recent advent of the consumer drone offers terrorists new capabilities in sophisticated attacks, particularly lone wolves who can afford these drones and benefit from standoff and other features. Although terrorists have not yet employed explosive-laden drones in domestic attacks, drones available on the market can carry a payload sufficient to achieve lethal or destructive objectives sought by lone wolves motivated by diverse ideologies targeting long-term static, short-term static, or mobile targets. The Diffusion of Innovations Theory suggests that explosive-laden drones are not an immediate threat, but as pioneering terrorists experiment with consumer drones, this tactic may become more commonplace as existing defense mechanisms fail to protect targeted buildings, events and individuals. As consumer drones become more popular and more sophisticated, countermeasures and government policies must keep stride with this new and evolving threat.

Keywords: *analysis, lone wolf, terrorism, drones, national security*

Introduction

Lone wolf terrorism gains increasing media coverage as attack frequency and death tolls increase, but such attacks are also a testing ground for innovation. Advances in technology, competition in manufacturing and the diffusion of ideas through media arm the individual terrorist with a wider assortment of weapons and knowledge over time. On January 7, 2013, the Chinese drone manufacturer DJI released the Phantom drone for $679, marking the advent of the consumer drone and the availability of affordable drones to the public (Ripley 2015, 68). Though designed for drone enthusiasts and a variety of commercial and recreational uses, nefarious actors began experimenting with consumer drones. Outside the United States (US), there have been at least a dozen instances of terrorists attempting to use drones in an attack, either to carry an explosive to a target or to deliver a chemical agent (Quan 2014). While established terrorist organizations, mainly in the Middle East, experiment with larger captured drones or expensive models, consumer drones offer capabilities of bypassing traditional security measures to small organizations and sole individuals at affordable prices. In September 2013, a member of the German Pirate Party crashed a Parrot quadcopter near the feet of German chancellor Angela Merkel at a campaign rally in Dresden in order to protest government drone surveillance

[A] MA Candidate, School of Global and Security Studies, American Military University
[B] Associate Professor, School of Global and Security Studies, American Military University

doi: 10.18278/gsis.2.1.5

(Gallagher 2013). The motive was purely political, but the proximity of the drone to a head of state revealed a new challenge for security forces to tackle. Another high-profile incident occurred in January 2015, when a government employee accidently crashed his friend's DJI Phantom quadcopter into the White House lawn (Schmidt and Shear 2015). The innocent mistake exposed vulnerabilities of one of the most protected sites on U.S. soil and demonstrated how a sole actor can circumvent traditional security measures to gain access and proximity to a target. Just 3 months later, Japanese police arrested a man who landed a drone carrying a bottle of radioactive sand on the roof of the Japanese Prime Minister's Tokyo office (Abbott et al. 2016, 12, 14). Although many drone incidents are unintentional or carried out without harmful intent, these events highlight a relatively new capability available to the public, particularly lone wolf terrorists who may procure explosives, purchase a consumer drone and conduct an attack independently. The gravity of this drone risk increases each year, as the FAA estimates that "by 2020 there could be as many as 30,000 drones in the sky in the United States alone" (McKelvey, Diver, and Curran 2015, 44). Government policies lag far behind this evolving threat, presenting significant concerns for the near future.

What is the feasibility of a lone wolf using an explosive-laden consumer drone to conduct an attack in the United States? This question necessitates a thorough investigation of trends among lone wolf attacks and profile characteristics of a lone wolf in the United States, capabilities of drones currently on the market, modern and future defense measures, legislation relevant to drone flight and sales. Given current conditions, a reasonable hypothesis is that if the U.S. Government stalls in producing legislation relevant to consumer drones and corporations fail to take adequate steps in enhancing defense measures, then the feasibility of a lone wolf's use of an explosive-laden consumer drone increases, as does the probability of success in targeting infrastructure, the public or a high-profile individual. The purpose of this study is therefore three-fold: (1) to analyze the feasibility for a lone wolf to use an explosive-laden consumer drone in an attack within the United States; (2) to assess the vulnerabilities and security gaps based on current defense mechanisms and forecasted drone capabilities; and (3) provide recommendations for further analysis of relevant threats and risk mitigation strategies.

Analytical Framework

This study investigates the security concern that lone wolf terrorists may affix explosives to consumer drones for use in a domestic terrorist attack. The independent variable in this research is the feasibility of employing an explosive-laden consumer drone in a terrorist attack in the United States. Independent variables include consumer drone capabilities and limitations (present and future), relevant domestic lone wolf terrorism trends (i.e., target type, weapon of choice, ideologies), defense mechanisms and policies governing drone manufacture and use.

Analysis in this study relies on the assumption that lone wolf terrorism trends will generally remain consistent in the near future. Another assumption is that consumer drone technology will continue to improve and popularity will continue to grow as forecasted by researchers. The Diffusion of Innovations Theory, introduced by French sociologist Gabriel Tarde in 1903 and further developed by E.M. Rogers in 1995, closely relates to this study of terrorists' use of consumer drones. This theory investigates "the conditions which increase or decrease the likelihood that a new idea," such as using an explosive-laden consumer drone in a terrorist attack, "will be adopted by members of a given culture," such as lone wolf terrorists in the United States ("Diffusion of Innovations Theory" 2016). Conditions contributing to the likelihood of lone wolves using drones include types of targets, advantages achieved through use of a drone, availability and cost, payload capacity, and the ability to use a drone as a lone operator with little training or practice. Rogers explained innovation "consists of four stages: invention, diffusion through the social system, time, and consequences" ("Diffusion of Innovations Theory" 2016). These stages represent factors influencing how ideas spread through a society and the rate at which members of that society adopt these ideas. Rogers elaborated on diffusion, stating that there are five categories of adopters, all following a standard deviation curve, with innovators espousing the new idea in the earliest stages (2.5%), early adopters following suit shortly thereafter (13.5%), the early majority (34%), the late majority (34%), and the laggards (16%) ("Diffusion of Innovations Theory" 2016). In regard to the consumer drone dilemma, terrorists, in general, remain in the invention phase as innovators experiment with the concept of delivering explosives in an attack via air. As terrorists continue to experiment with drones, the probability of such an attack increases as consumer drones become more widely available and the government lags behind in legislation and restrictions.

Analysis and Findings

It is necessary to thoroughly review trends among past lone wolf attacks in the United States in order to assess implications of new consumer drone technology available to terrorists. Trends reveal commonalities in target selection and aid in predictive analysis. Comparing drone models currently on the market reveals potential new capabilities for lone wolves, helping to discern how such terrorists might employ drones against select targets. A study of strengths and weaknesses of various defense mechanisms further sheds light on weaknesses in homeland security. A careful study of these factors exposes faults and gaps that must change, aiding in determining the most practical recommendations to shore up these vulnerabilities.

Lone Wolf Terrorism within the United States

Established terrorist groups have attempted to use drones in attacks, but most incidents have occurred in the Middle East. With large sums of money and resources, these groups have had the means to purchase or capture a drone and equip it with explosives. Even so, large groups such as Al-Qaeda or the Islamic State have not conducted a drone attack in the United States, preferring to use bombs or firearms in attacks. Payoffs involved in utilizing consumer drones generally do not support these larger terrorist groups' objectives. The limited payload of consumer drones does not support the large bombs and high death tolls characteristic of Al-Qaeda or Islamic State attacks. Similarly, martyrdom is a chief objective sought after by Islamic State operatives, who either conduct a suicide attack equipped with a bomb on their person or plan a complex attack, shooting a crowd until killed. Such groups generally use bombs and firearms in attacks and seek shock and awe through publicity, but utilizing a drone detracts from this objective given the limited carnage. These factors may explain why larger terrorist groups, which have the resources and means to purchase or capture a drone and equip the drone with explosives, have not attempted such an attack in the United States.

The closest semblance of a specialized attack with a drone occurred when the FBI foiled a plot in September 2011 involving large model aircraft. The FBI arrested Rezwan Ferdaus, a Massachusetts-based Al-Qaeda supporter, who planned to target the Pentagon and East Potomac Park with model aircraft packed with explosives supplied by FBI undercover employees he believed to be Al-Qaeda operatives ("Man Sentenced" 2012). Although the scenario did not meet criteria for a lone wolf incident, Ferdaus' independent purchase of model aircraft, personal surveillance of targets, and innovative plot to fly explosive-laden model planes into targets demonstrates the feasibility of a sole actor acquiring the materials necessary for a similar attack. Large terrorist groups have had the means to conduct an attack with drones, Consumer drones seem particularly attractive to lone wolves, as opposed to members of established terrorist groups, due to affordable prices, risk-averse utility, and payoffs closely aligned with objectives of lone wolf terrorists, as evidenced by trends of domestic lone wolf terrorism.

In the past, the expensive nature of aerial platforms likely deterred lone wolves from experimenting with such a tool in an attack. Individuals plotting without outside resourcing or support were generally restricted to either stealing an industrial drone used for crop dusting or commercial purposes or purchasing an expensive model through hobbyist channels. High costs and restrictive supply channels made such a prospect highly unlikely to domestic lone wolves, who were generally "unemployed, single white males with a criminal record" (Hamm and Spaaj 2015, 6). Trends since 2012 indicate domestic terrorists are younger and often without a criminal record due to their youth, largely due to Islamic State recruiting efforts on social media platforms. Consumer drones, with popular models priced below $2,000 and likely to become more affordable in coming years, are now within purchasing ability of the typical lone wolf in the United States. Purchasing these models does not require a background check, nor is specialized training required to operate these drones, enabling an individual to acquire and gain proficiency on a drone with minimal personal interactions.

Consumer drones offer advantages to risk-averse lone wolves. Lone wolves in the United States generally "mix personal vendettas with established ideologies," seeking political change or retaliation for some perceived wrong while maintaining a degree of self-preservation (Eby 2012, 34). The most common ideologies fueling attacks include Islamist, anti-government, anti-abortion, racism, and personal motivations. Between September 11, 2011 and June 30, 2016, approximately 40.3% of domestic lone wolf incidents were motivated by Islamist ideologies, in many cases inspired by

Islamic State propaganda on social media platforms (Hughes 2016, 66). While Islamist terrorists can certainly employ consumer drones in attacks, lone wolves responsible for attacks motivated by anti-government, anti-abortion, and other ideologies might be more prone to using drones for the safety benefits. Such terrorists generally have a stronger sense of self-preservation than religiously motivated terrorists seeking glory and martyrdom, such as followers of Al-Qaeda and the Islamic State. Physical standoff afforded by consumer drones, with up to a 2,000-m reliable range, grant lone wolves greater chances for evasion following an attack (Abbott et al. 2016, 5). This distance and the ability to fly an explosive-laden drone into a target remotely avoids risks associated with security video footage and access control points scanning or checking identification.

Trends in domestic lone wolf terrorism indicate the utilization of consumer drones would yield strong benefits for lone wolves. Bombs were the weapon of choice in 54% of domestic lone wolf attacks between 2001 and 2012 (Eby 2012, 37). Consumer drones provide a means to deliver a bomb in a way that bypasses traditional security measures hindering placement by hand. Aerial delivery also reduces the risk of discovery of the bomb prior to detonation, as the terrorist can fly the bomb to the target and detonate the bomb once within an acceptable blast radius. Between 2001 and 2012, lone wolf targets included buildings (43% of cases), the public (37%), a person or place of interest (14%), and infrastructure (4%), with the remaining 2% of targets unknown to law enforcement (Eby 2012, 33). Consumer drones provide lone wolves the means to bypass security features around buildings, such as perimeter fences and access control points. Drones can also increase the carnage in an attack targeting the public by detonating a bomb at a slightly higher altitude and increasing the blast radius, or achieve greater proximity to a person of interest by guiding the drone remotely past personal security escorts and guards.

The advent of consumer drones, now affordable and widely accessible to the public, may influence future attacks due to new capabilities, such as overcoming physical standoff and bypassing layered physical security through flight, anonymity through remote control operation, and other risks to the terrorist. Terrorist applications of consumer drones remain a foggy area, due to the lack of historical attacks involving drones, but innovators will likely experiment and hone methods in the coming years. As Hamm and Spaaj conclude, "although lone wolf terrorism may not be increasing in the United States, it is undergoing dramatic changes in terms of modus operandi," which may include consumer drones in the near future (Hamm and Spaaj 2015, 5). As consumer drones drop in cost and include more features, lone wolves will likely experiment with drones for terrorist plots.

Although drones are now affordable to the common profile among lone wolves in the United States, it is unlikely attacks in the near future will incorporate this new technology, at least, in the form of carrying explosives toward a target. According to the Diffusion of Innovations Theory, 2.5% of a given population is innovators, experimenting with new methods and tactics, which others in the population adopt at later stages ("Diffusion of Innovations Theory" 2016). Due to the lack of events involving consumer drones among lone wolf attacks, lone wolves likely fall into this invention and innovation phase. Explosive-laden consumer drones are an unlikely terrorist tool in near-term attacks, but variables such as types of targets and standoff, drone payload capacities and drone defense mechanisms can influence the likelihood of lone wolves employing such methods of attack.

Feasibility of the use of Explosive-laden Consumer Drones

To date, there has not been a terrorist attack in the United States involving a consumer drone carrying explosives, though similar plots exist as far back as 2011, as revealed in the FBI investigation of Rezwan Ferdaus (Finn 2011). As consumer drones become more accessible, affordable and sophisticated, security concerns continue to grow. Consumer drones vary in dimensions, capabilities and cost. Table 1 includes six popular drone models currently on the market, listing characteristics of capabilities relevant in a terrorist attack involving an explosive-laden drone. All six are equipped with a camera and can only operate in dry conditions.

Table 1: Select List of Commercially Available Drones and Relevant Factors

Model	Weight (kg)	Payload (kg)	Flight Time (min)	Range (m)	Max Speed (mph)	Price
Blade 350 QX2	1	0.2	10	1,000	32	$285–435
3DR IRIS+	0.9	0.2	16	800–1,000	40	$720–865
DJI Phantom 2 Vision +	1.2	0.2	25	600	33	$1,150–1,730
DJI Phantom 3 Professional	1.2	0.3	28	1,900	35	$1,440–1,730
Walkera Scout X4	1.7	0.5–1.0	25	1,200	40–50	$1,010–1,300
Yuneec Q500 Typhoon	1.1	0.5	25	600	54	$1,300–1,590

Source: Abbott et al., *Hostile Drones*, 5.

Depending on the type of target and desired end state, these factors differ in relative importance. Terrorist targets fall into three distinct categories: long-term static targets, temporary static targets, and mobile targets (Abbott et al. 2016, 15). Lone wolves in the United States have plotted against or attacked each type of target. Several variables influence suitability of different drone models and likelihood of success. As these characteristics continue to evolve for optimal drone configuration and utility and capabilities continue to improve, these factors will alter how terrorists may employ a consumer drone in an attack.

Long-term Static Targets

Based on characteristics and trends of past lone wolf attacks within the United States, likely long-term static targets include prominent government facilities, sports stadiums, chemical plants and facilities, natural gas pipelines, and similar infrastructure. Depending on the desired effect, drones provide terrorists few advantages in targeting some structures, such as bridges, sports stadiums and some government facilities, due to the close proximity they can attain through vehicles and other means of transporting a significantly larger explosive payload. Areas with layered security and standoff, however, may be more vulnerable to drones, which can achieve greater proximity to protected sites by approaching targets via flight (Jackson et al. 2008, 28). Hence, a lone wolf terrorist could feasibly use an explosive-laden drone to cause much more damage to a chemical plant than by attempting to use another payload delivery method.

Long-term static targets are easier for a terrorist to target, due to their permanence and a terrorist's ability to conduct reconnaissance through virtual or physical means and attack on his/her own timeline. On the other hand, this permanence allows for a more robust defense, including physical standoff and obstacles, radar, and passive sensors. In targeting long-term static structures, payload is generally the most important feature, as the explosive blast may need to rupture pipes or other metallic walls to detonate protected chemicals or inflict damage on targets within a structure. Range is also vital to success, as the drone may need to traverse considerable physical standoff posed by perimeter fences, restricted areas and a lack of dead space offering concealment. The importance of flight time varies among targets, as this factor is directly proportional to physical standoff. Speed is less vital to mission success, as the likelihood of interdiction remains low, even if guards or other defense measures detect the drone.

Temporary Static Targets

Short-term, or temporary, static targets are more dynamic than long-term static targets and, though often scheduled far in advance, locations may change due to weather or other unforeseen factors. Such targets include summits, speeches by politicians and sporting events or large gatherings, often containing some degree of local security (Abbott et al. 2016, 15). Lone wolves might attack particular events for ideological reasons, but may also seek to capitalize on live media coverage and a high concentration of people. In many such instances, security is such that a terrorist might infiltrate a crowd with a larger explosive device, such as the pressure cookers in the Boston Marathon bombing of 2013. A drone, despite payload limitations, does not require prepositioning and the terrorist can guide the bomb remotely to the largest concentration of people in real-time. This method bypasses typical forms of security and detection, increasing the odds of success.

Payload is the most significant factor in an attack deliberately targeting a crowd of people, as the terrorist aims to inflict the greatest number of casualties. Small metallic objects packed around the explosives can enhance this objective, producing shrapnel that expands the kill radius. Range also contributes to success, providing adequate standoff to avoid detection and improve chances of escaping the scene. Whereas long-term static targets may have permanent fences and surveillance cameras monitoring vulnerable areas and high-traffic pathways, physical security measures protecting temporary static targets often include road barriers, access control points or inspection sites and law enforcement patrols. Drone flight ranges generally exceed the distance between such security features and protected events or venues, weakening the effects of security against lone wolves employing an explosive-laden drone. Drones with a greater maximum speed may mitigate the chance of interdiction and minimize early warning and reaction time of the crowd.

Mobile Targets

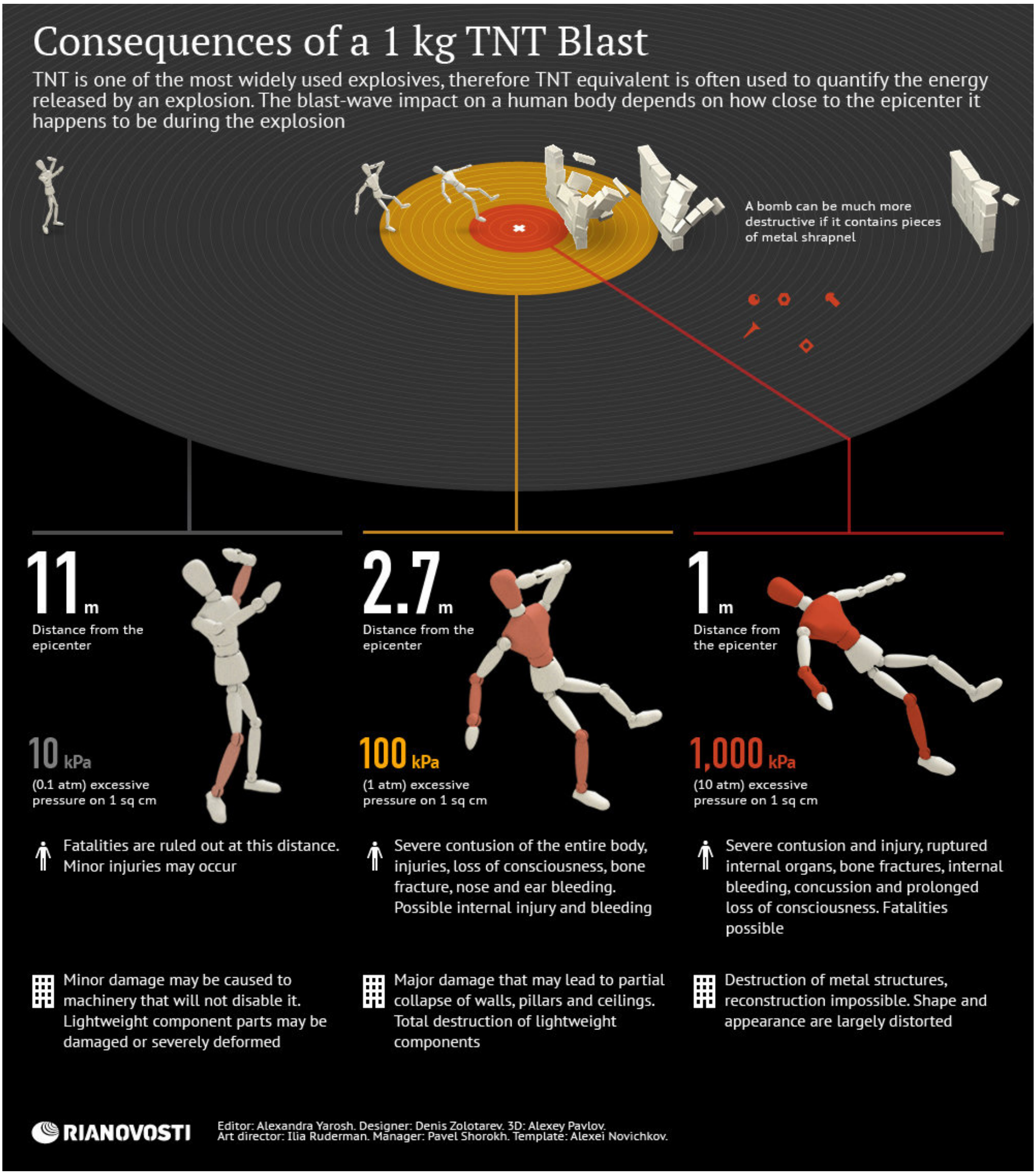
Mobile targets are usually more difficult for a lone wolf to attack, as security measures include announcing events or appearances with little time in advance and restricting knowledge of movements and routes to a small group of individuals. Mobile targets are moving targets, lacking a fixed position and constantly subject to change, such as a military convoy or the President of the United States (Abbott et al. 2016, 15). Based on trends in ideology, these targeted individuals are often prominent government authorities, heads of corporations or leaders of religious groups. Between September 11, 2001 and January 1, 2012, lone wolves targeted a person or place of interest in 8 of the 56 domestic lone wolf terrorism cases, with assassination targets ranging from abortion doctors to the President of the United States (Eby 2012, 33). Terrorists may choose to target such figures at their homes or near their workplaces, as such locations may be easier to locate than events or appearances announced with little advance notice. A lone wolf would likely employ a drone with explosives against a figure with a guard detail or similar security measures, which might interdict more common terrorist tactics such as a car bomb.

A drone's maximum speed plays a much more crucial role against a mobile target, such as in the assassination of a political leader. An increase in a target's reaction time increases his/her ability to find cover and the ability of guards to interdict the attack by shooting the drone down. Payload plays a slightly smaller role, especially if the explosive charge is equipped with small objects to produce shrapnel. Increased range can enable a terrorist to bypass physical security features protecting the mobile target and avoid surveillance cameras and media coverage sorted through in forensic investigations following an attack. Greater range also increases the probability that the terrorist can escape quickly and undetected, avoiding initial cordons or roadblocks in the wake of an attack.

Optimal Consumer Drones and Potential Effects

A drone's payload capacity is the most important feature in a terrorist attack involving an explosive-laden consumer drone. Range and maximum speed are important considerations, their relative importance depending on the type of target, while flight

Figure 1: Damage Inflicted by 1.0-kg of TNT (R.E. Factor of 1)



Consequences of a 1 kg TNT Blast

TNT is one of the most widely used explosives, therefore TNT equivalent is often used to quantify the energy released by an explosion. The blast-wave impact on a human body depends on how close to the epicenter it happens to be during the explosion

A bomb can be much more destructive if it contains pieces of metal shrapnel

11 m
Distance from the epicenter

10 kPa
(0.1 atm) excessive pressure on 1 sq cm

Fatalities are ruled out at this distance. Minor injuries may occur

Minor damage may be caused to machinery that will not disable it. Lightweight component parts may be damaged or severely deformed

2.7 m
Distance from the epicenter

100 kPa
(1 atm) excessive pressure on 1 sq cm

Severe contusion of the entire body, injuries, loss of consciousness, bone fracture, nose and ear bleeding. Possible internal injury and bleeding

Major damage that may lead to partial collapse of walls, pillars and ceilings. Total destruction of lightweight components

1 m
Distance from the epicenter

1,000 kPa
(10 atm) excessive pressure on 1 sq cm

Severe contusion and injury, ruptured internal organs, bone fractures, internal bleeding, concussion and prolonged loss of consciousness. Fatalities possible

Destruction of metal structures, reconstruction impossible. Shape and appearance are largely distorted

RIANOVOSTI

Editor: Alexandra Yarosh. Designer: Denis Zolotarev. 3D: Alexey Pavlov.
Art director: Ilia Ruderman. Manager: Pavel Shorokh. Template: Alexei Novichkov.

Source: "Potential Damage from a 1 kg TNT Explosion" 2013.

time and price are less important factors. In regards to the explosives transported by a drone, terrorists may use a variety of methods to achieve their objective, such as affixing a cluster of grenades, including small metal objects to produce shrapnel or using a homogenous substance. The relative effectiveness (RE) Factor of a material, measuring that substance's explosive properties compared to TNT (RE Factor of 1.0), is a useful factor to determine the potential effects of an explosive-laden consumer drone. Some models currently on the market can carry up to a 1.0 kg payload, which can inflict the damage described in Figure 1 if the substance's RE Factor is equal to or greater than 1.0.

Current payload limitations severely restrict the amount of potential damage resulting from an explosive-laden consumer drone flying into a building, specialized facility or crowd, but payload capacities will likely increase in the future. Existing drone models can feasibly carry the sufficient amount of explosives to assassinate an individual, injure dozens in a dense crowd, trigger a larger explosion at a chemical facility or cause minor damage to buildings, depending on the proximity of the blast. The government has not established constraints for payload weight, so that capacity will likely increase over time as companies manufacture larger and more robust drones. The prospect of heavier payloads seems more realistic as companies like Amazon experiment with drones to deliver packages.

Evaluation of Defense Mechanisms

Similar to the defense-in-depth concept for physical security practiced by government agencies and corporations, a series of defense mechanisms improves the odds of detection and interdiction. Many technical assets can defend long-term static targets, but it is unfeasible to implement such costly defense mechanisms for temporary static targets or mobile targets. Unfortunately, "drones can easily bypass many of the security measures implemented since 9/11," including many sophisticated defense assets, yet some can potentially mitigate the likelihood or severity of a drone attack (Maddox and Stuckenberg 2015). The most viable detection methods include acoustic sensing, radar and the human eye, while the most efficient interdiction methods are geofencing and kinetic defense. Additional interdiction methods include command link jamming and global navigation satellite system (GNSS) jamming, but these are less feasible options as "jamming the radio signal of a drone (or cellphone or anything else) is illegal in the United States under long-standing federal law," because it may interfere with emergency services (Ripley 2015, 70). These countermeasures must continue to evolve as consumer drone features improve and become more effective in overcoming and bypassing existing security measures.

Acoustic Sensing

Consumer drone models produce distinct noises difficult to replicate. Acoustic sensors can detect nearby drones by these unique sound signatures generated by drone motors (Sathyamoorthy 2015, 88). One such sensor, called a DroneShield, can quickly detect a drone by model and send out a text-message alert to nearby guards for monitoring and interdiction (Ripley 2015, 67). Although the tool is passive and only serves to detect when a drone flies nearby, the automated text mechanism increases the chances of interdiction by alerting guards who can shoot down the drone. The DroneShield is equipped with a database of "common UAV acoustic signatures," reducing the chance for false alarms and increasing precision detection rates (Sathyamoorthy 2015, 88). This detection mechanism is more affordable than most and is easily installed and transportable. While the DroneShield may be most effective in defending long-term static targets and less so defending some temporary static targets, due to increased ambient noise, it was implemented at the 2015 Boston Marathon and it can protect mobile targets, as the tool is available for vehicles, such as a VIP convoy (Abbott et al. 2016, 17; Sathyamoorthy 2015, 88). Unlike some visible defense mechanisms, it is unlikely a lone wolf would detect or become aware of acoustic sensors near a target prior to the attack. One significant challenge with this technology is the internal sound database, which will require updates as companies manufacture new drone models. Nonetheless, the DroneShield's ability to identify specific drone models may cue security forces to recurring instances of a unique drone flying nearby, possibly probing the perimeter and testing security responses or conducting reconnaissance for a future attack.

Radar

Radar is one of the most effective methods to detect and track aerial threats, but this defense mechanism encounters unique challenges when applied to consumer drones. Air surveillance radar in the United States is ineffective against consumer drones, as these systems detect and track, but do not interdict, planes moving at high speeds, as opposed to smaller drones moving at relatively slow speeds (Sathyamoorthy 2015, 88). Installation and maintenance of radar systems can be very costly, explaining their limited presence in the United States. Some sophisticated radar systems "can see something as small as a bird flying," presenting false positives or distinguishing small drones from birds using precision radar and analytics (Elias 2016, 20; Maddox and Stuckenberg 2015). Such systems can provide early warning to long-term static targets, especially with physical standoff in the form of clearings between a facility and its perimeter fence, but a cost–benefit analysis yields poor results in defending temporary static or mobile targets. Furthermore, drone operators may fly at low altitudes, below 100 ft, to capitalize on inter-visibility lines created by surrounding terrain to block line-of-sight required for radar detection (Elias 2016, 20). Radar systems are not the most feasible or easily implemented methods to defend against lone wolves operating an explosive-laden drone, providing a false sense of security for sites protected by a dense array of radar systems.

The Human Eye

The naked eye remains the most reliable and practical defense against an explosive-laden drone. Ironically, no technical asset detected or brought down the consumer drone that landed on the White House lawn; instead, "a Secret Service officer standing guard" spotted the drone (Leonnig and Whitlock 2015). A combination of human senses provide a redundant means to identify and locate drones, such as seeing a drone's shadow on the ground or hearing a drone overhead. In Iraq, where radars "intentionally eliminate slow-flying targets on or near the ground" to prevent overtaxing tracking systems, human eyes are also "the most effective means of detecting such slow-flying threats," such as consumer drones (Gormley 2003, 8–9). Proving to be especially effective in warzones, the human eye also has a history of identifying drones in recreational settings. After experimenting with various technical defense assets tailored to drone detection, Major League Baseball security officials concluded, "One of the best ways to detect drones is simply to deputize the crowd [because] when it comes to spotting small drones, 80,000 eyeballs are better than radar" (Ripley 2015, 72). Although this may not be the best defense for long-term static targets, where a small guard force would likely patrol access points and areas with few physical barriers, the human eye is the optimal defense for a temporary static target, such as a large crowd at an event. Complacency may detract from effectiveness, as drones become more common in the skies and operators disregard flight restrictions. While observant crowds may provide early warning, they offer little in the form of interdiction.

Geofencing

Geofencing is one of the most cost-effective and viable methods to mitigate the chance of a terrorist using a consumer drone in an attack. Invented by DJI and first implemented in April 2014, GPS geofencing is a technique where a manufacturer designates no-fly zones in coded form, imbedded in firmware, to prevent drones from entering certain areas (Poulsen 2015). Within the United States, DJI currently has no-fly zones around airports and the White House, but DJI and other drone manufacturers should include additional no-fly zones in future firmware or as updates to protect vital infrastructure and other potential terrorist targets.

Individuals with technical and sophisticated knowledge of firmware could potentially bypass or disable such security measures, but such knowledge and skills are not a common trait among lone wolves in the United States. Geofencing could, therefore, convince a potential lone wolf to abandon a target or select a different target unprotected by this security feature. Alternatively, it might force a lone wolf to seek expertise or technical assistance through the internet, Dark Web or other means, delaying an attack and increasing the likelihood of interdiction by the Intelligence Community. If the terrorist is unaware of geofencing features, the defense mechanism might interdict the drone during the actual attack. These no-fly zones would be most effective in defending long-term static targets, but manufacturers can implement and push updates to include temporary static targets.

Kinetic Defense

Shooting down a drone with small arms fire is the most likely and feasible form of drone intercept in an area not geofenced or if a drone bypasses geofencing restrictions. In urban areas, where most of lone wolf temporary static and mobile targets exist, retired Air Force Major General Frederick F. Roggero stated, "it would be tough to detect and tough to defeat kinetically without shooting it down and causing collateral damage" (Leonnig and Whitlock 2015). Faster drone speeds and smaller dimensions certainly contribute to potential collateral damage caused during interdiction attempts. Additionally, "shooting down drones is usually illegal," and may carry costly fines, so citizens and members of law enforcement are unlikely to do so (Ripley 2015, 70). Law enforcement and defense agencies in other countries have experimented with other kinetic defense mechanisms to mitigate collateral damage and increase likelihood of interdiction. Such mechanisms include a net gun, similar to a net shot to catch feral animals, and net-equipped drones that can fly over a nefarious drone and snag it in a net, but these methods are not very reliable (Ripley 2015, 67; Sathyamoorthy 2015, 93). New kinetic defense methods will likely evolve as consumer drones become more versatile over time.

Recommendations

Federal Restriction of 5-pound Payload Capacity for Consumer and Commercial Drones

Due to the relatively recent dawn of consumer drones, regulatory measures and policies in the United States remain underdeveloped and behind the curve. Currently, the FAA requires users to register drones weighing more than 0.55 lbs, which includes the drone models in Table 1 and most drones with payload capacities ("Frequently Asked Questions" 2015). Empirical evidence and qualitative data reflects that payload is the most significant factor influencing drone suitability for terrorist attacks involving explosive-laden drones, yet existing laws do not regulate payload capacities. The FAA delegates the majority of drone regulation to state and local authorities, but the FAA and Congress should establish guidelines and restrictions limiting payloads for future models, enforceable in all states. Senator Booker (D-NJ) introduced the Commercial UAS Modernization Act (S. 1314) in the Senate on May 13, 2015, which would establish "barriers to allowing payload carriage" on drones, but the bill has yet to move beyond the Senate ("S.1314—Commercial UAS Modernization Act" 2016, 24). Such proposed legislation works in stark contrast of developments in drone delivery systems. Amazon's Prime Air program, for instance, involves a drone capable of transporting a 5-pound payload (Weatherby 2016). Policies governing drone utilization lag behind Amazon's progress in drone research and development. For now, circumstances of utility drive drone design and payload in industry and commercial sectors to remain below a 5-pound weight capacity, as most of Amazon's products weigh less than 5 pounds, but this weight capacity may increase in the future (Weatherby 2016). The FAA and Congress should establish a maximum payload at or near five pounds to mitigate effects in the instance of a terrorist attack employing such drones, restricting the use of drones capable of transporting heavier payloads to the military and specialized industries. Hackers have already demonstrated that delivery drone prototypes are vulnerable to hijacking through sophisticated means (Wagstaff 2013). Although most lone wolves lack the knowledge to hijack one of these drones, the capability exists and the payoff of employing a drone with five pounds of explosives instead of two pounds yields significantly more damage.

Legislation and Increased Collaboration for Geofencing Firmware

To date, no United States laws require drone manufacturers to incorporate geofencing into their firmware. Following the quadcopter incident on the White House lawn in 2015, DJI emphasized geofencing and pushed a "mandatory firmware update" but even then, its geofenced areas only include airports and the White House (Poulsen 2015). This cost-effective method to restrict drone flight can greatly contribute to protection of long-term static targets, but may also protect short-term static and mobile targets through proper coordination. Senator Chuck Shumer (D-NY) introduced an amendment to the FAA Reauthorization bill last year stating, "If geo-fencing technology were mandated in every drone sold in America," it would "effectively fence off drones from sensitive areas like airports, the Pentagon and major sporting events like the United States Open and more" (Laing 2015). The bill failed, but politicians should continue to investigate the benefits of geofencing and push for requirements in newly manufactured drone models, such as firmware and mandatory periodic updates to incorporate new geofences, as this passive feature can slow down or prevent attacks conducted by unsophisticated lone wolves unable to bypass or circumvent firmware.

Drone manufacturers are responsible for most of the recent progress in geofencing efforts. DJI recognizes the utility of this feature and plans to implement as many as 10,000 no-fly zones for airports and some national borders in the future, but the United States Government should collaborate with DJI for additional no-fly zones over other sensitive locations (Poulsen 2015). Geofencing can mainly benefit long-term static targets, but government agencies have failed to feed information to drone manufacturers developing firmware and constructing geofences. The Department of Homeland Security's Protective Security Coordination Division, which conducts vulnerability assessments for sites of 16 different critical infrastructure sectors, should collaborate with DJI and other drone manufacturers to implement new no-fly zones over these sensitive sites ("Critical Infrastructure" 2016). Such collaboration can significantly enhance the security of long-term static targets across the United States in a relatively short amount of time.

Increased Focus in Academia

There is certainly potential for further research and analysis on this looming threat. Between September 2013 and the January 2015 quadcopter incident at the White House, the National Counterterrorism Center's working group on drones grew from four members to 65, reflecting its concern for terrorists' use of drones (Schmidt and Shear 2015). Similarly, some academic institutions developed specific groups to investigate and analyze drones, such as the Center for the Study of the Drone at Bard College, but there is room for continued growth in this new field of study. Lt. Col. (Ret.) Mitchell [last name withheld], former Chief of MQ-1 Training for a USAF Special Operations Squadron, suggested, "a study should be considered where they hire someone and say—"Go buy one [a drone] and see what you can do." This kind of practical study will fill in gray areas very quickly" (Maddox and Stuckenberg 2015). DHS and other governmental agencies should collaborate with universities to promote and endorse such research. Students are ideal candidates to conduct such experiments. They can go through the unfamiliar process of targeting by conducting reconnaissance by visiting the site or through open source intelligence collection. They can then research and purchase a drone through the same unclassified mediums a lone wolf would use, learn how to fly and program the drone and attempt an attack with mock explosives in a controlled setting under approved conditions. Such experimentation can transform theoretical studies into practical application, aiding refinement of defense mechanisms and exploring the possible terrorist applications of consumer drones.

Conclusions and Recommendations for Additional Research

For less than $1,600, anyone can acquire a ready to fly, GPS-enabled and camera-equipped consumer drone that can carry a small amount of weight. This offers terrorists new capabilities in executing attacks, particularly the ability to bypass traditional security measures and gain unprecedented access to a vulnerable target. Lone wolves in the United States break the mold of global terrorism, motivated by anti-governmental ideologies more than religious or other principles. Innovators among these lone wolves may use consumer drones to target a number of long-term static, temporary static or mobile targets in the coming years.

Consumer drones currently on the market offer a diversity of capabilities, of which payload, maximum range and maximum speed are most important. None of these can carry more than 1.0 kg of a substance, significantly limiting the destructive capacity of an explosive-laden drone; even so, a precision attack can render devastating effects against a vulnerable target. It is very likely that lone wolves will continue to use firearms and bombs in attacks rather than explosive-laden consumer drones due to a much higher probability of inflicting more casualties and causing more damage.

A variety of sophisticated defense mechanisms exist which can detect small drones at low altitudes, but there are few mechanisms capable of interdicting a drone in flight toward a target. Collaboration between government agencies and drone manufacturers may improve security conditions by implementing no-fly zones over sensitive sites through firmware, potentially delaying or deterring many attacks. Such defenses can help secure long-term static targets, but temporary static targets and mobile targets remain vulnerable, generally reliant on the human eye for detection with no reliable interdiction mechanisms.

Legislation limiting payload capacity of consumer drones can curtail future challenges associated with this type of terrorist attack. Additionally, legislation requiring geofencing firmware in drones offers a viable defense mechanism that drone manufacturers can quickly implement. Much of this new field remains unexplored, especially terrorist applications of drones, as most research is theoretical, without practical experiments or trials. Academia can hedge the risks of nefarious innovators by exploring the bounds of consumer drones before lone wolves, enhancing defense efforts by exposing vulnerabilities.

This field remains the subject of many fictional plotlines and alarmist articles, but there is a general lack of academic research detailing the feasibility of consumer drones in attacks. Researchers can further explore general terrorist applications of consumer drones, such as reconnaissance of otherwise inaccessible targets or drones as delivery agents for chemical or biological agents. Studies can also investigate other types of payloads, such as fragmentary grenades and various explosive substances. Researchers should actually run trial runs for drones carrying such payloads to demonstrate feasibility and probable damage. A study of international responses may yield useful approaches for the United States to follow in defending against drone threats. Some defense studies detail strategies and defense practices in the United Kingdom, Ireland, Japan, and Malaysia, but researchers can continue to investigate conditions in other countries to gauge effectiveness of different defense methods and assess vulnerabilities on a global scale. Such studies may also reveal how the United States Congress compares with other nations in passing relevant legislation and restrictions and how this might weaken security. Researchers may look into the research and development behind new drone models and features to assess possible terrorist applications and prepare defense measures.

References

Abbott, Chris, Matthew Clarke, Steve Hathorn, and Scott Hickle. 2016. *Hostile Drones: The Hostile Use of Drones by Non-state Actors Against British Targets*. London: Remote Control Project.

“Critical Infrastructure Vulnerability Assessments.” 2016. *Department of Homeland Security*. https://www.dhs.gov/critical-infrastructure-vulnerability-assessments (accessed May 28, 2016).

“Diffusion of Innovations Theory.” 2016. University of Twente. https://www.utwente.nl/cw/ theorieenoverzicht/Theory%20clusters/Communication%20and%20 Information% 20Technology/Diffusion_of_Innovations_Theory/ (accessed May 28, 2016).

Eby, Charles A. 2012. *The Nation that Cried Lone Wolf: A Data-driven Analysis of Individual Terrorists in the United States Since 9/11*. Master’s Thesis, Naval Postgraduate School.

Elias, Bart. 2016. *Unmanned Aircraft Operations in Domestic Airspace: U.S. Policy and the Regulatory Landscape* (CRS Report No. R44352). Washington, DC: Congressional Research Service. https://www.fas.org/sgp/crs/misc/R44352.pdf.

Finn, Peter. 2011. “Mass. Man Accused of Plotting to Hit Pentagon and Capitol with Drone Aircraft.” *The Washington Post*, September 28. https://www.washingtonpost.com/national/national-security/mass-man-accused-of-plotting-to-hit-pentagon-and-capitol-with-drone-aircraft/2011/09/28/gIQAWdpk5K_story.html (accessed May 16, 2016).

“Frequently Asked Questions.” 2015. Know Before You Fly. http://knowbeforeyoufly.org/ frequently-asked-questions/ (accessed October 20, 2016).

Gallagher, Sean. “German Chancellor’s Drone ‘Attack’ Shows the Threat of Weaponized UAVs.” *Ars Technica*, September 18. http://arstechnica.com/informationtechnology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/ (accessed October 16, 2016).

Gormley, Dennis M. 2003. *UAVs and Cruise Missiles as Possible Terrorist Weapons* (Occasional Paper No. 12). Monterrey, CA: James Martin Center for Nonproliferation Studies.

Hamm, Mark, and Ramon Spaaj. 2015. *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies*. Terre Haute, IN: Indiana State University.

Hughes, Matthew A. 2016. *The Islamic State’s Influence on Lone Wolf Terrorism in the United States*. Master’s Thesis, American Military University.

Jackson, Brian A., David R. Frelinger, Michael J. Lostumbo, and Robert W. Button. 2008. *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*. Santa Monica, CA: RAND Corporation.

Laing, Keith. 2015. “Schumer Moves to Require Geo-fencing on Drones.” *The Hill*, September 14. http://thehill.com/policy/transportation/253565-schumer-moves-to-require-geo-fencing- on-drones (accessed May 6, 2016).

Leonnig, Carol D., and Craig Whitlock. 2015. “Drone Incident at White House Highlights Long- Studied, Still-Unsolved Security Gap.” *The Washington Post*, January 26. https://www.washingtonpost.com/politics/drone-incident-at-white-house-highlights-long-studied-still-unsolved-security-gap/2015/01/26/ed2e7f9e-a594-11e4-a7c2- 03d37af98440_story.html (accessed May 3, 2016).

Maddox, Stephen, and David Stuckenberg. 2015. “Drones in the U.S. National Airspace System: A Safety and Security Assessment.” *Harvard National Security Journal*, February 24. http://harvardnsj.org/2015/02/drones-in-the-u-s-national-airspace-system-a-safety-and- security-assessment/ (accessed April 28, 2016).

"Man Sentenced in Boston for Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Detonation Devices to Terrorists." 2012. *Federal Bureau of Investigation*. https://archives.fbi.gov/archives/boston/press-releases/2012/man-sentenced-in-boston-for-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-detonation- devices-to-terrorists (accessed October 12, 2016).

McKelvey, Nigel, Cathal Diver, and Kevin Curran. 2015. "Drones and Privacy." *International Journal of Handheld Computing Research* 6 (1): 44–57. (accessed April 23, 2016). doi: 10.4018/IJHCR.2015010104.

"Potential Damage From a 1kg TNT Explosion." 2013. *Sputnik*, August 13. http://sputniknews.com/infographics/20130813/182605201/Potential-Damage-From-a-1kg- TNT-Explosion.html (accessed May 7, 2016).

Poulsen, Kevin. 2015. "Why the US Government is Terrified of Hobbyist Drones." *Wired*, February 5. http://www.wired.com/2015/02/white-house-drone (accessed April 22, 2016).

Quan, Douglas. 2014. "Terrorists' Use of Drones on RCMP's Radar; Intelligence Assessment." *The Province*, December 30. (accessed April 21, 2016). Proquest (1640950854).

Ripley, Amanda. 2015. "To Catch a Drone." *The Atlantic Monthly* 316 (4): 66–68, 70, 72–74. Proquest (1726692327).

"S.1314 – Commercial UAS Modernization Act." 2015. *Library of Congress*. https://www.congress.gov/bill/114th-congress/senate-bill/1314/actions (accessed May 14, 2016).

Sathyamoorthy, Dinesh. 2015. "A Review of Security Threats of Unmanned Aerial Vehicles and Mitigation Steps." *The Journal of Defence and Security* 6 (1): 81–97. Proquest (1768942810).

Schmidt, Michael S., and Michael D. Shear. 2015. "Drones Spotted, but Not Halted, Raise Concerns." *The New York Times*, January 29. http://www.nytimes.com/2015/01/30/us/for-super-bowl-and-big-games-drone-flyovers-are-rising-concern.html?_r=0 (accessed May 28, 2016).

Wagstaff, Keith. 2013. "Could Prime Air Drones be Hacked? Probably, but Amazon Might not Care." *NBC News*, December 4. http://www.nbcnews.com/technology/could-prime-air-drones-be-hacked-probably-amazon-might-not-2d11691755 (accessed December 19, 2016).

Weatherby, Lea. 2016. "Amazon Drone Delivery: 30 Minutes and 5-Pound Limits for 'Prime Air.'" *Inverse*. https://www.inverse.com/article/10330-amazon-drone-delivery-30- minutes-and-5-pound-limits-for-prime-air (accessed October 23, 2016).