Section II: Creativity and Complications: The Dark Side of UAS Use and Emerging Technologies

The accessibility of commercial drones has led to an explosion in use of the devices by private citizens. It has also contributed to the fairly rapid development of new ways to use UASs, from fighting forest fires and assisting search-and-rescue missions to delivering packages and racing for sport. There is an obvious benefit to society from these developments, as in many ways UASs can be used to gain efficiencies and to contribute to the public good. Indeed, as noted by Paul Scharre, "uninhabited systems can not only save human lives by undertaking dangerous missions in their place, they can enable new concepts of operation that would not be possible were human lives at risk."[292]

While private-sector drone makers and software developers are providing the tools to enable UAS exploration, the decentralization of UAS technology has created a playing field in which individual users are limited only by their own imaginations and the various government regulations to which they choose to abide—if the regulations even exist. In this way, when it comes to innovation in UAS use, creativity is king. A number of emerging technologies like autonomy, miniaturization and swarms, and further advancements and increased accessibility of sensors (e.g., forward looking infrared, known by the acronym FLIR) and software (e.g., terrain mapping) will only perpetuate these UAS use trends and extend the realm of the possible.

The dark side to all of this is that innocuous UAS use demonstrated by one person could be exploited by those with more sinister motives. To that end, and to demonstrate more fully what already lies within the realm of the possible for a terrorist group, this section catalogs a number of creative ways that drones have been used by private individuals who did not have terror intent, but whose UAS use could be mimicked or repurposed by others to inflict harm. By focusing on what private citizens have already achieved, we avoid the pitfalls associated with unconstrained brainstorming and "what-if" scenario development about how drones can be used, and limit our discussion to those incidents to which "proof of practicality" applies.[293] The section concludes with a brief review of emerging technology trends, and discusses how they will complicate future terrorists' use of drones, and the threat potential as a delivery or attack mechanism they hold.

Creativity and Additional Capability

> *For example, the first thing many people often ask is: "What weapon should I use in my operation?" But the answer to this question—and it's an important question—is not as difficult as it may seem. The Mujahid Brother Nidal Hasan used firearms in his assault on Fort Hood, but the fact is, today's Mujahid is no longer limited to bullets and bombs when it comes to his choice of a weapon. As the blessed operations of September 11th showed, a little imagination and planning and a minimal budget can turn almost anything into a deadly, effective and convenient weapon which can take the enemy by surprise and deprive him of sleep for years on end.*
>
> *—Adam Gadahn, 2010*[294]

As the 2010 quote from the late al-Qa`ida operative Adam Gadahn makes clear, sometimes all that is required to shock the system in a terrorist campaign is just a little imagination. Thus, to round out our analysis about the current and future threat potential of drones, this subsection focuses not on what

292 Paul Scharre, *Robotics on the Battlefield, Part 1: Range, Persistence and Daring*, (Washington, D.C.: Center for a New American Security, May 2014), p. 27.

293 I would like to thank Brian Jackson for his helpful thoughts, and suggested language, as to how best to frame this section, especially for the "proof of practicality" language that he recommended.

294 Adam Gadahn, "A Call to Arms," *al-Sahab*, January 2010.

terrorists have done, but on what private citizens have. All that would be required from the terrorist side is a little imagination; for that reason, it is equally important that the West's response to the UAS threat be proactive and imaginative as well.

Surveillance

The principal way drones have been used by terrorist groups to date has been for surveillance and strategic communications purposes. Commercially available drones have also been used by private citizens for a range of snooping purposes, including spying on backyard neighbors or stealing trade secrets via industrial-corporate espionage.[295] UAS flights have also been observed over strategic military installations in the United States, such as those that have taken place over Naval Base Klitsap.[296]

Given the array of sensors and other add-ons that are available, the surveillance potential of today's commercially available drones is not limited to aerial intelligence or line-of-sight reconnaissance. The actions taken by two security consultants at the Black Hat security conference in 2011 demonstrate what can be accomplished with a little know-how and ingenuity. Armed with several thousand dollars and using "off-the-shelf electronics" the two experts created (in their garage) the Wireless Aerial Surveillance Platform, or WASP, a UAS with unique capabilities.[297] As noted by *Forbes*:

> The WASP, built from a retired Army target drone converted from a gasoline engine to electric batteries, is equipped with an HD camera, a cigarette-pack sized on-board Linux computer packed with network-hacking tools including the BackTrack testing toolset and a custom-built 340 million word dictionary for brute-force guessing of passwords, and eleven antennae…
>
> On top of cracking wifi networks, the upgraded WASP now also performs a new trick: impersonating the GSM cell phone towers used by AT&T and T-Mobile to trick phones into connecting to the plane's antenna rather than their carrier, allowing the drone to record conversations and text messages on 32 gigabytes of storage. A 4G T-mobile card routes the communications through voice-over-Internet or traditional phone connections to avoid dropping the call.[298]

That was nearly five years ago, and while security services are aware of these vulnerabilities, the ability to mimic and re-create the WASP system exists. As noted by Jane's:

> Fully functional drone systems that require no assembly are already available for purchase by the general public. The AR Parrot Drone, for example, costs USD300, is controlled using a smartphone and sends back real-time video feed to the operator's smartphone or tablet computer. When modified with a lightweight computer running Linux, a broadband connection, a GPS receiver and two WiFi cards, the Parrot can be turned into a drone that is capable of hacking into WiFi systems and carrying out rudimentary signals intelligence.[299]

Accessing Sensitive Locations and VIPs

The potential of violent actors to access sensitive sites has been demonstrated by a number of cases that involve private citizens who were able to fly drones into or over a number of hard-to-access, restricted locations. One of the most famous examples occurred in January 2015 when an off-duty U.S. government employee "lost control of a friend's DJI Phantom quadcopter, which then crashed onto

295 For corporate security linkages, see "New Threat: Drones Banned for Fear of Espionage," *White Sparks* 7:145 (March 10, 2015); see also Michael Condon, "Feedlots Concerned about Industrial Espionage from Drones," ABC Rural, April 2, 2013.

296 "Navy Looking for Drone Operator Flying Device around Washington State Base," Fox News, February 27, 2016.

297 Pierluigi Paganini, "Wireless Aerial Surveillance Platform, the DIY Spy Drone," Security Affairs, December 17, 2014.

298 Andy Greenberg, "Flying Drone Can Crack Wi-Fi Networks, Snoop on Cellphones," *Forbes*, July 28, 2011.

299 "Attack of the Drones—the Dangers of Remote-Controlled Aircraft," *Jane's Intelligence Review*, December 16, 2011.

the White House lawn." The individual who was flying the UAS was intoxicated at the time and is believed to have flown the UAS onto the White House grounds by accident. The trouble for the Secret Service was that the incident appears to have motivated someone else to try to pull off the same stunt intentionally in May of that same year. In this incident, "a man was arrested for trying to fly a Parrot Bebop drone over the White House fence."[300] UAS flights over sensitive locations by private citizens have also been an issue in France, as "unidentified drones have been flown over the US embassy, the Eiffel Tower, the Invalides military museum, the submarine communications base at Sainte-Assise, the Place de la Concorde, the Elysee Palace and multiple nuclear power stations."[301] As noted in section I, Maynard Hill also made headlines in 2003 for flying a UAS across the Atlantic Ocean on less than a gallon of gas.[302]

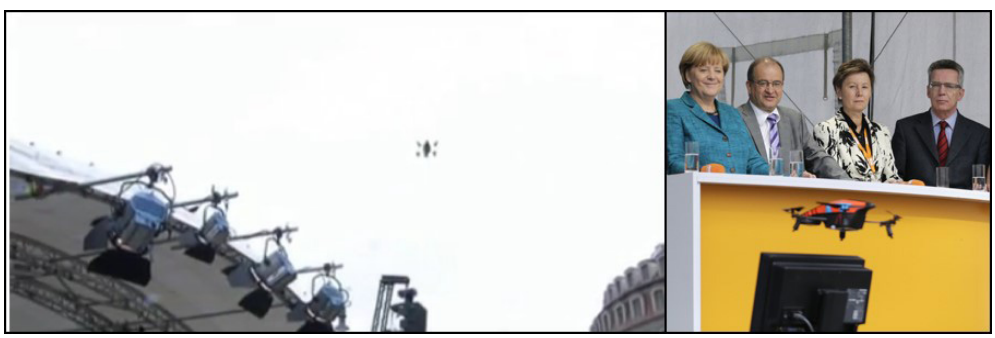

Photo Credit: Screen grab of Pirate Party UAS at Angela Merkel press event

Commercially available drones also have the potential to provide greater access to political leaders and other VIPs. For example, in September 2013 activists from the German Pirate Party made news after they successfully flew "a small Parrot quadcopter drone up to the stage" where German chancellor Angela Merkel was speaking to a rally of supporters.[303] The activist controlling the UAS was able to hover the UAS over her head and in front of her before he was arrested.[304] "Commentators noted that if the drone been equipped with even a small explosive device, it could have been an effective weapon."[305]

The boldest and perhaps most troublesome incident to date occurred in August 2015, when a Japanese activist, protesting Japan's nuclear policy, successfully flew and landed a UAS "carrying trace amounts of radiation" onto the roof of the Japanese prime minister's residence.[306] While the activist conducted the stunt for publicity and not to inflict harm on the prime minister, the incident still speaks to what lies within the same realm of possibility for a group that has violent intentions.

Drones have also been used to smuggle drugs across borders, to deliver material into entry-control-restricted locations, such as prisons, and to conduct corporate espionage. According to estimates provided by the U.S. Drug Enforcement Agency (DEA), in 2014 there were "in excess of 150 cross-border smuggling flights" involving drones that flew across either the U.S.-Mexico or U.S.-Canada borders.[307] While the DEA and other agencies have been aware of this issue, U.S. officials seized their first ship-

300 Abbott et al., "Hostile Drones.

301 Ibid.

302 Sohn, "Model Airplane Flies the Atlantic."

303 Timothy B. Lee, "Watch the Pirate Party Fly a Drone in Front of Germany's Chancellor," *Washington Post*, September 18, 2013; Dan Gettinger, "A Pirate Drone in Germany," Center for the Study of the Drone, September 19, 2013.

304 Lee, "Watch the Pirate Party Fly a Drone in Front of Germany's Chancellor."

305 Gettinger et al., *The Drone Primer*, p. 9.

306 Scott Mitchell, "Someone Flew a Drone Carrying Radioactive Material on to the Japanese PM's Office," Vice, April 22, 2015.

307 Friese et al., "Emerging Unmanned Threats," p. 47; for additional background, see Kristina Davis, "Two plead guilty in border drug smuggling by drone," *Los Angeles Times*, August 12, 2015.

ment of drugs delivered via cross-border drone only in August 2015.[308] Prison officials in numerous countries have faced similar challenges. For example, in 2012 "a $600 remote-controlled quadcopter [was flown] over a Brazilian prison fence to deliver cell phones to the incarcerated."[309] Drones have also been used to deliver contraband, pornography, weapons and food to inmates, and by kidnappers to pick up a ransom payment.[310] Although their platforms have not been that capable, a number of DIY hobbyists have used UAS technology to build systems large enough and with a sufficient amount of lift to transport a person.[311] These examples speak to the broader utility of drones for terrorist organizations, and illustrate how—just like Amazon's plan to use drones to deliver packages—terrorists might be eyeing drone platforms to deliver sensitive matériel or to function as couriers.

Weaponize

As outlined in the typology presented in section I, there are several ways to weaponize a UAS. They include piloting a UAS to a target; using a UAS to deliver an explosive or to disperse chemical, biological or radiological material; and mounting a weapon to a UAS. Like the examples earlier in this subsection, a variety of incidents involving private citizens demonstrate what is already in the realm of possibility when it comes to using commercially available drones in a violent, weaponized way.

Pilot to Target

Akin to Japan's use of kamikaze pilots during World War II, a terrorist can pilot a UAS directly to his or her target. There are two main threat angles associated with this type of attack. The first involves the piloting of an explosive-laden UAS into an intended target. Some have dubbed this type of approach, which Iran has declared its intent to use, the "kamikaze or suicide drone."[312] The second attack method involves the piloting of a UAS into a target that could have catastrophic consequences if hit in the right location, such as a large commercial airliner's engine (i.e., a "birdstrike" scenario), precluding the need for explosives.[313] In this type of attack, the UAS itself functions as the weapon, and the "explosive" lies in the creative and sinister way in which the drone is used. Naturally, both of these attack methods can be used in combination with one another, and in the future the threat potential of this approach will be complicated by UAS swarms (for further detail, see later in this paper), whereby a commercial airliner or other target needs to avoid not one UAS but many, with the potential to overwhelm a particular system. For example, UAS controllers could position themselves along the final route of approach used by lower- and slower-flying incoming aircraft at Newark Liberty International Airport. The danger potentially caused by a last-minute landing problem at Newark could be amplified, considering that one of the airport's runways runs adjacent to a major (and heavily trafficked) highway.

AeroVironment's small, backpack-portable Switchblade UAS, which the U.S. military is in the process of fielding, illustrates the potential of "kamikaze" UAS systems.[314] The device also provides a glimpse into how small "kamikaze"-style UASs are bound to significantly alter the tactics, techniques and procedures of conventional militaries, insurgents and terrorists alike. The value of the Switchblade lies in its transportability, weight and destructive potential. As noted by *Gizmodo*, the device:

> Carries a small explosive charge equivalent to a 40mm grenade, allowing it to target lightly ar-

308 Ibid.

309 Marc Goodman, "Criminals and Terrorists Can Use Drones Too," *Time*, January 31, 2013.

310 Mary Emily O'Hara, "Another Drone was Used to Smuggle Contraband into a Prison," Vice, August 1, 2014; Kevin Poulson, "Drones and Spyware: The Bizarre Tale of a Brutal Kidnapping," *Wired*, July 24, 2015.

311 For example, see "Self flying drone is powerful enough to carry a person," *Daily Mail* (Video), no date.

312 "Iran Helping Hamas, Hezbollah Build Fleet of Suicide Drones," *Jerusalem Post*, April 9, 2015.

313 For background on this issue, see Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles*, pp. 26–28.

314 Even more lightweight than the Switchblade, Prioria's Maveric UAS also illustrates this potential.

> mored vehicles and embedded (or otherwise inaccessible) infantry positions, such as on rooftops or ridge lines. What's more, the Switchblade's electric propulsion system and small stature make is a sneaky little bastard, difficult to track and able to glide silently in a window before detonating.[315]

The U.S. military is also using even smaller, hand-launched drones like the Wasp or Raven to enhance the field surveillance capabilities of operational units. The size and cost of these UAS allows them to be purchased in the thousands, and as technology advances, future drones will get even smaller.

These drones are beyond the accessibility of terrorist groups, but that does not mean that creative terror actors will not seek to replicate the Switchblade's key features, even if done in an ad hoc or jerry-built way. For example, as noted by *Newsweek*, "*Wired* magazine editor Chris Anderson built a version of the military's hand-tossed Raven surveillance drone for $1,000, while an Arizona-based anti-immigrant group instituted its own pilotless surveillance system to monitor the U.S.-Mexico border for just $25,000."[316] Another potential way to create a "kamikaze" UAS on the cheap would be for a terrorist group to cobble together existing resources, such as outfitting a small fixed-wing aircraft like a Cessna with autopilot or GPS guidance and remote-control features, and then loading that heavier-payload-capable craft with explosives. When drones were in short supply in the first decade of the twenty-first century, this approach was something the U.S. military considered as a cheap, stopgap measure to get more reconnaissance and armed drones into the sky.[317]

As has been well reported, a steady stream of close encounters between private drones and commercial airliners has taken place in flight over the last several years. To gain analytical purchase into this issue, the Center for the Study of the Drone at Bard College released a report in 2015 that analyzed 921 incidents in the United States over a nearly two-year period during which a UAS either was sighted by "a pilot or an air traffic controller… [who observed the UAS] flying within or near the flight paths of manned aircraft" or when a UAS came in close enough proximity to a manned aircraft that the potential for a "near midair collision" existed.[318] In their report, Dan Gettinger and Arthur Holland Michel found that 35.5 percent of the 921 incidents were close enough to be deemed "close encounters."[319] Further, the authors

> counted 158 incidents in which a drone came within 200 feet or less of a manned aircraft (two-thirds of all Close Encounters in which a concrete drone-to-aircraft proximity is given), 51 incidents in which the proximity was 50 feet or less, and 28 incidents in which a pilot maneuvered to avoid a collision with a drone. One hundred and sixteen of the Close Encounters involved multiengine jet aircraft, 90 of which were commercial aircraft (the majority of which have the capacity to carry 50 or more passengers). We also counted 38 Close Encounter incidents involving helicopters. The reports do not always clearly identify the type of drone involved in incidents, but of the 340 drones that were identified in the reports, 246 were multirotors (i.e. quadcopters, hexacopters, etc.) and 76 were fixed-wing. The locations with the highest number of incidents were large metropolitan areas.[320]

315 Andrew Tarantola, "America's Kamikaze Drone Makes the Skies Way Less Friendly," Gizmodo, September 5, 2013; see also Sam Biddle, "These Drones Transform into Suicide Bombs," Gizmodo, September 9, 2011.

316 Newsweek Staff, "Will Foreign Drones One Day Attack the U.S.?," *Newsweek*, February 25, 2010.

317 Dave Moniz, "Old Planes Eyed as Drones," *USA Today*, February 4, 2002; for additional background, see Gormley, "UAVs and Cruise Missiles as Possible Terrorist Weapons," p. 7; and Dennis Gormley, "Unmanned Air Vehicles as Terror Weapons: Real or Imagined?" NTI, July 1, 2005.

318 Dan Gettinger and Arthur Holland Michel, *Drone Sightings and Close Encounters: An Analysis*, (New York: Center for the Study of the Drone, December 11, 2015), http://dronecenter.bard.edu/drone-sightings-and-close-encounters/.

319 Ibid.

320 Ibid. For additional background, see Craig Whitlock, "Near-Collisions between Drones, Airliners Surge, New FAA Reports Show," *Washington Post*, November 26, 2014; Jonathan Vanian, "Close Calls between Drones and Airliners Are Sky-High," *Forbes*, December 11, 2015.

The frequency of these "close encounters," and specifically the near-miss incidents, has concerned the Federal Aviation Administration. The potential for a UAS to make direct contact with a jet engine or other critical system on a sizable commercial aircraft loaded with passengers while on final approach to an airport and potentially over a densely populated urban area is real. The likelihood of such an event, however, is a matter of debate.[321]

The problem, which Gettinger and Michel also note, is that, with a few exceptions, such as the work being done through the CRASH Lab at Virginia Tech, little testing has been done.[322] There is a paucity of empirical, physical test-driven data to evaluate just how much risk exists.[323] The computer simulations run by Virginia Tech's lab suggest that, depending on the strike location and the size of the UAS, a UAS collision with an airliner has the potential to cause "critical damage."[324]

A factor that complicates this issue slightly is an open-source "zombie drone" software-hardware package that allows one to hack into, "hijack" and then take control of a nearby commercially available UAS. This approach would allow violently motivated actors to potentially repurpose UAS already in flight.[325] Although a matter of dispute, Iran claims that in 2011 it was able to hack into and take over the controls of an RQ-170 Sentinel, a super-stealthy and advanced military-grade U.S. UAS, which, if true, would illustrate that there is precedent for this type of action on a much larger scale.[326]

Deliver or Drop Explosive

While a UAS loaded with explosives can be piloted directly to its objective, a UAS can also be modified to drop an explosive over a target, such as a VIP gathering or a stadium full of people. UAS hobbyists looking for a thrill, a good aerial shot or to make the news have already flown drones over stadiums. Indeed, drones have been spotted over college and NFL football games, professional soccer matches in a number of countries and the U.S. Open. During that latter event, which occurred after the U.S. Federal Aviation Administration prohibited UAS flights over stadiums in the fall of 2014, a UAS "whizzed above players Flavia Pennetta and Monica Niculescu before slamming into an empty area at Louis Armstrong Stadium."[327]

Facilitating the delivery or the dropping of an explosive is commercial off-the-shelf technology designed to initiate the release of a payload, which already exists. The availability of such tools suggests that the "jump" for terrorists employing this type of tactic is not far away. As noted by the defense consultancy Jane's in late 2011:

---

321 According to Fred Roggero, the "potential for catastrophic damage is certainly there." His perspective carries some weight, as he is "a retired Air Force major general who was in charge of aviation safety investigations for the service and now serves as a consultant to companies seeking to fly drones commercially." For background, see Whitlock, "Near-Collisions between Drones, Airliners Surge." While a number of experts agree with Roggero or have similar views, other specialists believe the threat potential is much less and that the risk associated with a UAS–commercial airliner collision is overblown. "We've been flying into birds for how long?" noted John Goglia, a former National Transportation Safety Board member. In his view, a drone isn't "going to bring an airplane down. . . . That's a little bit of baloney." See "Former NTSB Official Says Drone Isn't Going to Bring Airplane Down," *New York Post*, May 8, 2016.

322 Gettinger and Michel, *Drone Sightings and Close Encounters: An Analysis*.

323 Ibid.

324 Ibid.

325 For background, see http://samy.pl/skyjack/.

326 Scott Peterson, "Exclusive: Iran Hijacked US Drone, Says Iranian Engineer," *Christian Science Monitor*, December 15, 2011.

327 Julia Talanova, "Drones Crashing Big Sporting Events, Including U.S. Open, College Football," CNN, September 6, 2015. Russian separatist forces operating in Ukraine in 2014 reportedly outfitted a commercial UAS with a homemade "grenade dropping" mechanism, which they tried to use—unsuccessfully—to attack Ukrainian soldiers from the air. According to the Ukrainian soldiers involved in the incident, the separatists were able to release the grenade over their position, but the grenade failed to detonate for reasons that are unclear. While investigating this issue further, Larry Friese also found a "photograph uploaded to a social media platform [that] shows an improvised assembly configured to drop an RGO or RGN type hand grenade, potentially with additional fragmentation material, from a small UAV." For background see, Friese et al., "Emerging Unmanned Threats," p. 38–39.

> For only USD16.95 anyone can buy the Chinese-made Quanum "bomb" drop system for remote control aircraft. This 23.5 cm long case splits open to release a 103 g payload of the user's choice. It can be installed in just seconds by connecting the bomb with a radio channel so that it can be released on demand. Although sold as a leisure accessory, when used with a drone equipped with GPS navigation and video feed, this type of device could effectively and accurately deliver a pernicious payload on any desired target. The Quanum bomb system, and the many more like it that will surely follow, make it far easier for any terrorist to turn a remote-controlled plane into an aerial bomber.[328]

While attractive to potential terrorist actors, using a UAS in this capacity is not without its own limitations. First, a 103-gram payload, which is roughly equivalent to a quarter of a pound, is not a sizable amount of explosives. Second, as noted by RAND, "conventional bombs are much more effective when employed indoors. An open-air nail-bomb delivered to a crowded outdoor event would, if all went as planned, probably produce effects similar to the Boston marathon attacks."[329] This isn't to say that such an attack should be written off—it shouldn't—but rather that the scale of devastation caused by such an incident might not be higher than that produced by a single suicide bomber. The use of multiple drones or a fleet of autonomous drones could enhance the level of destruction, though.

Weapon Mount

Another attack modality that will likely be explored by terror groups is mounting a weapon directly to a UAS. This wouldn't be that surprising, as some private citizens have been interested in doing the same for quite some time. For example, in December 2008, Jim Simmons, a DIY UAS hobbyist, successfully attached and remotely fired "a Springfield 1911-A .45 caliber weapon with a digital camera gun sight for accurate shooting" to a "Bergen Gasser EB mini-helicopter."[330] The event, a potential first, wasn't just bluster, because Simmons filmed his stunt and posted it online.[331] Few major news outlets reported it, though.

328 "Attack of the Drones."

329 Davis et al., "Armed and Dangerous.

330 As cited ibid. Originally reported by Gizmodo; see Jesus Diaz, "RC Helicopter Modded 45 Caliber Handgun will Probably End in Disaster," Gizmodo, December 10, 2008.

331 For video of the RC helicopter in flight, see www.liveleak.com/view?i=4cd_1228911752.

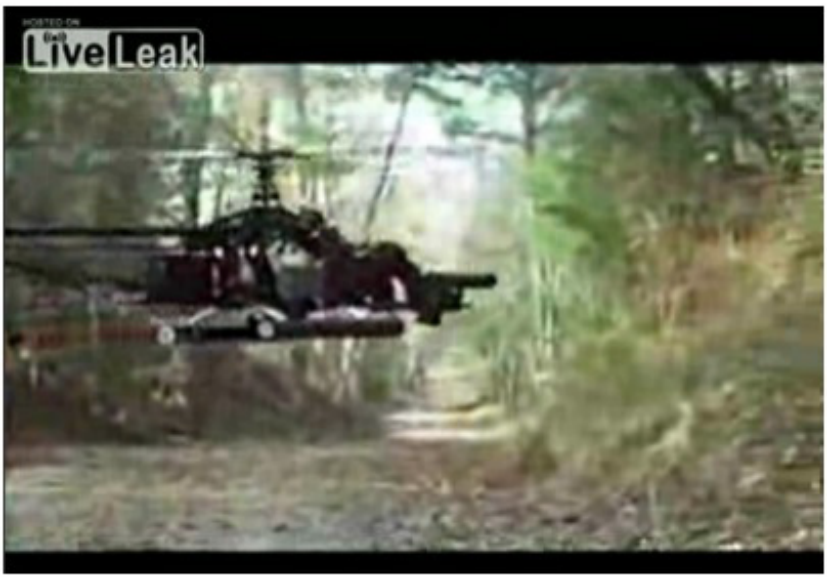

Photo Credit: Screen grab of Jim Simmons's 2008 Live Leak video

Six and a half years later, in July 2015, a Connecticut teenager, Austin Haughwout, made major new headlines after he posted a video to YouTube that showed him mimicking the stunt, and successfully firing a handgun that he mounted to a commercial UAS variant that he had modified.[332] The video shows the teen remotely firing the handgun while the UAS is in flight through a trigger mechanism he installed.[333] While the teen's accomplishment was certainly novel and noteworthy, the video also shows the jerry-rigged "handgun UAS" bouncing in the air between shots as a result of gun's kickback, indicating that stability and accuracy were central problems affecting the usability and reliability of the platform.[334] (Simmons's device also appears to have faced this problem.) Since the contraption was made by a teenager in the United States, it is almost certain that a terror organization with more resources and expertise would at least be able to mimic the effort, if not improve on it, for potential use in assassination-type scenarios.

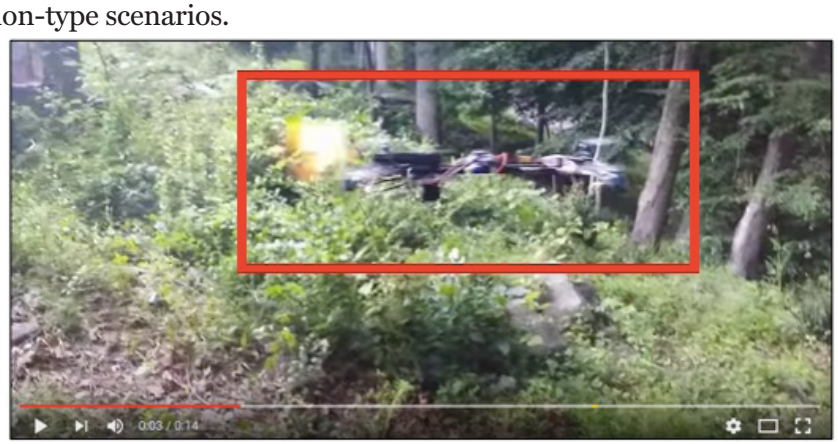

Photo Credit: Screen grab of "Flying Gun" YouTube video posted by user Hogwit in 2015

Then, less than six months after his initial media splash, Haughwout made headlines again with another DIY UAS invention. This time he upped the ante and the shock value by creating a UAS-mount-

332 Dan Corcoran and Bob Connors, "Father Says 'Flying Gun' Drone Broke No Laws," NBC Connecticut, July 22, 2015.

333 Ibid.

334 Ibid.

ed flamethrower, which he again successfully demonstrated in another YouTube video posted online.[335] The interesting thing about Haughwout's second invention is that by using a flamethrower instead of a handgun, he was able to improve the weapon's accuracy. In creating this device, Haughwout has not only illustrated the "flamethrower UAS" proof of concept, which he advertised to the world, but he has also shown how easy it is to weaponize a UAS with basic materials.

Photo Credit: Screen grab of "Roasting the Holiday Turkey" YouTube video posted by Hogwit

The actions of Simmons and Haughwout have demonstrated what lies within the realm of possibility in terms of weapon-mounted UAS capability, given a little ingenuity and craftiness.

"Blade" Drone

Although less of a concern, UAS rotator blades also hold a small amount of threat potential due to the high-speeds at which they spin. Accidents involving commercially available drones in 2003, 2005, 2008 and two in 2013, all of which resulted in deaths due to contact made with UAS rotor blades, illustrate the danger.[336] In one unfortunate episode, a UAS flight instructor was struck in the neck by an out-of-control UAS that his student was flying, and the instructor ended up bleeding to death.[337] Another tragic case from 2013 involved an experienced UAS pilot whose head was partially severed after he also lost control of his UAS. Based on what can be learned from news accounts, most if not all of these episodes involved—as one might suspect—larger remote-control helicopters with large and strong blades.[338]

Even smaller drones, however, have caused problems. For example, in November 2015 a UAS blade on a smaller device accidently made contact with a toddler's left eye, and the damage was significant enough to leave the child blind in that eye.[339] To evaluate some of these claims, and the potential for harm, the popular U.S. television show *Mythbusters* conducted an experiment whereby its hosts intentionally flew UAS blades into a chicken carcass to see what would happen, and the damage that would result.[340] The show's hosts were surprised to find that the plastic UAS blades easily sliced into the chicken, leaving them to conclude that if used in close range the blades could inflict some bodily

335 See www.youtube.com/watch?v=lmD3rXUR1Tw.

336 For background on 2003 incident, which resulted in the death of Ronald Kyle, see, www.rcgroups.com/forums/showthread.php?t=165680; for 2005 incident, which reportedly resulted in death of a child in South Korea, see http://rc.runryder.com/helicopter/t169336p1/. Other blade injuries are chronicled at www.heliguy.com/nexus/dangers.html.

337 See www.rcgroups.com/forums/showthread.php?t=165680.

338 Dan Nosowitz, "Remote-Controlled Helicopter Kills 19-Year-Old in Brooklyn," *Popular Science*, September 5, 2013.

339 "Toddler's Eyeball Sliced in Half by Drone Propeller," BBC News, November 26, 2015.

340 Andrew Liptak, "Can a Home Drone Kill You? The Mythbusters Test with a Chicken Says Yes," io9, July 25, 2015.

harm and be dangerous.[341] More damage could probably be done if the blades were metal and the UAS was flown by a skilled operator who could navigate to a target successfully at close range. Even with these modifications, the threat of "blade" drone use still remains low and is more of a potential nuisance than anything else. Given other options, a terrorist actor would likely only select this type of approach to highlight its ability to get close to a VIP or to embarrass a government, rather than inflict a maximum number of casualties.

WMD Delivery

Given their desire for publicity and commitment to violence, a diverse range of terrorist groups have been attracted to the high-lethality potential associated with the use of chemical and biological weapons. The groups that have shown an interest in this type of material range from the Japanese religious cult Aum Shinrikyo to al-Qa`ida to the Covenant, Sword and the Arm of the Lord. Chemical, biological, radiological and nuclear material has been attractive to a number of groups because of the fear and chaos it would inspire and the potential it has to produce many casualties. Yet while a good number of terrorist outfits have experimented with weapons of mass destruction, very few have successfully deployed chemical or biological agents, and most have backed away after experimenting with them. And with one possible exception, none have had success using radiological or nuclear material.[342] Attacks like Aum Shinrikyo's 1994 successful sarin gas attack on the Japanese subway, or the Islamic State's reported use of chemical agents in Syria, are the exception and not the rule. This is because even though WMDs are attractive, acquiring, producing and successfully weaponizing or dispersing these types of agents presents a number of significant technical and logistical hurdles. As noted by RAND:

> The effectiveness of modes for dispersing an attack agent in the air above a target relies on the ability to place sufficient amounts of the weapon in the desired position, its probability of arriving there successfully and at the time designated for the attack, and the chance of successfully dispersing the material in the manner desired.… Particularly for UAVs, the systems' ready availability and ability to fly in most areas that would represent attractive targets appear to be significant advantages. However, they have significant disadvantages in payload size and the probability of successfully deploying the agent at the position and time desired.[343]

Thus, even if they are initially interested, most terror groups soon find out that they do not possess the resources or the level of expertise required to make the investment in WMDs worth it. This is especially the case when they evaluate their WMD options, which add complexity and increases costs (both financial and security, due to the risk associated with being caught trying to acquire or produce this type of material), in relation to the much lower costs of producing and deploying conventional explosives. For most terrorist groups, it doesn't take them long to figure out that the "juice just isn't worth the squeeze" and that it is more effective and efficient to go with more-conventional attack options. For example, instead of using a UAS for the 1993 plot described earlier in this report, Aum Shinrikyo decided to use a spray truck.[344] Given the openness of Western societies, other actors have found it to be more efficient to use the U.S. Postal Service as their delivery mechanism for weaponized anthrax, as the cost of delivery was not more than one or several stamps.[345]

Despite the hurdles terror groups have consistently faced in relation to WMDs, concerns about the

341 Ibid.

342 "To date, the only confirmed case of attempted nuclear terrorism occurred in Russia on November 23, 1995, when Chechen separatists put a crude bomb containing 70 pounds of a mixture of cesium-137 and dynamite in Moscow's Ismailovsky Park. The rebels decided not to detonate this "dirty bomb," but instead informed a national television station to its location." See Graham Allison, "Nuclear Terrorism: How Serious a Threat to Russia," *Russia in Global Affairs*, September–October 2004.

343 Jackson et al., *Evaluating Novel Threats to the Homeland*, p. 25.

344 Danzig et al., "Aum Shinrikyo: Insights into How Terrorists Develop Biological and Chemical Weapons."

345 For background, see "Timeline: How the Anthrax Terror Unfolded," NPR, February 15, 2011.

potential for commercially available drones to be used as platforms to disperse chem-bio material have been around for quite some time. As the cases associated with Aum Shinrikyo and the Islamic State in section I make clear, that concern is not unfounded. During "a 1994 meeting to discuss the future of counter-proliferation in a post-Soviet world, Senator Sam Nunn, the then chairman of the U.S. Senate Committee on Armed Services, laid out three 'out of the box' terrorism scenarios."[346]

> One involved terrorists flying a small UAV loaded with two 40 lb canisters of weaponised Anthrax spores into the Capitol building on the night of the president's State of the Union address to Congress. In Nunn's scenario, terrorists remotely flew the drone from a short distance away and were able to kill hundreds of lawmakers and senior government officials. While the president survived, the government was left paralyzed and a huge, densely populated area was biologically contaminated.[347]

Nearly two decades later, planners in charge of the 2012 summer Olympic Games in London were concerned about a number of aerial threats, including a UAS being used to deliver biological agents. As noted by Brian Fahy, an officer in the UK army, "The range of threats varies in size and capability. It could be a commercial airliner hijacked by somebody with malicious intentions or a protest group using a microlight to get their name in the papers."[348] He added that "it was 'feasible' that remote-controlled aircraft filled with poison and small enough to fit into a backpack could be used as a biological weapon in the capital."[349] The threat was taken seriously enough that the UK armed forces stationed a number of surface-to-air missiles on the tops of high-rise buildings around key Olympic venues.[350] While the surface-to-air missiles likely would not have been used to take down a UAS, a comprehensive plan, which involved other disruption methods, was also developed to ensure people's safety.[351] UK authorities took these precautions based on threat reporting that indicated that the Islamic State was training foreign fighters, including those with links to Britain, to produce toxic material.[352]

The concern about terror use of drones to distribute chem-bio materials has also picked up added steam because UAS platforms are now so much more capable, accessible and affordable. One industry that is now using drones in an analogous way (to disperse chemicals or other pesticides) is the agriculture, as farmers have found drones to be useful for cost savings and to spray wider areas. For example, "a video posted online shows how one Japanese farmer, tired of working in the sweltering heat, turned his remote-controlled helicopter into a crop-duster." As noted by RAND:

> If a terrorist were to use this same concept to spread a lethal agent over a crowd instead of pesticides over rice fields, the potential for harm could be enormous.
>
> One study showed that if 900 g of weapons-grade anthrax was dropped from a height of 100 m upwind of a large US city, an estimated 1.5 million people would become infected, with more than a 100,000 dying. Another study showed the consequences of dispersing a radiological weapon consisting of 2 kg of plutonium and 50 g of cesium over San Diego could lead to an 8 km area being contaminated and thousands of people exposed.[353]

Farmers aren't the only ones who have shown an interest in using drones for dispersion purposes. A

346 "Attack of the Drones."

347 Ibid.

348 Stephanie Condron and Christopher Leake, "Poison Drones Carrying Biological Weapons Are New Olympic Threat, Warns Colonel in Charge of Keeping London Calm," *Daily Mail Online*, May 5, 2012.

349 Ibid.

350 Ibid.

351 Ibid.

352 For background, see Mark Nicol, "MoD Tests Defences against High-Street Drones as MI5 Braces Itself for Jihadi Chemical Attack on UK," *Daily Mail*, September 12, 2015.

353 "Attack of the Drones—the Dangers of Remote-Controlled Aircraft."

graffiti artist in New York City also made news in April 2015 after he successfully attached and used a spraying mechanism to deface a prominently placed billboard of Kendall Jenner in New York City. Both of these cases—of the farmer and graffiti artist—show what one can achieve with a little dedication and ingenuity, and they illustrate that we might not be that far away from someone using a UAS to disperse a chem-bio agent to maim and kill, even if on a small scale.

Complicating Factors

Given the accessibility of commercial drones, the fast pace of technological change and a number of emerging UAS-related technologies, the terrorist UAS threat over the next five to ten years is bound to become more complicated. A cross-cutting challenge, as discussed earlier, is that many of the technological advancements we are seeing and likely will continue to see are being driven not by the military, but by the commercial sector.[354] This means that companies will be motivated and more inclined to open the sale of their technologies to a wider pool of potential buyers. This includes emerging technologies that are going to enhance UAS performance, and add new dimensions to UAS systems. As noted by Paul Scharre:

> Many of the game-changing innovations that enable swarming—low-cost uninhabited systems, autonomy and networking—are driven by commercial sector, not military, innovation. They will be widely available to a range of actors, and many states and non-state groups may be more eager to embrace them than the U.S. military, which is invested heavily in current operational paradigms.[355]

Another complicating issue is that over the course of the next decade, advancements will be made to the hardware and other core factors that currently limit the threat potential of commercially available drones. For example, it is predictable that future off-the-shelf drones will be able to carry heavier payloads, fly and loiter longer, venture farther from their controller, survive in more difficult weather and be able to do so via more-secure communications links (i.e., links that are less prone or susceptible to disruption). Indeed, as noted by Jane's, "the weight of modern onboard navigation equipment and sensors is dropping steadily due to advances in information technology and miniaturization. This allows drone pilots to do more with less."[356] Advancements in power will be a key driver of these developments, and will serve as a barometer of just how quickly UAS payload, range and endurance capabilities change.[357] When compared with advances in software, advances in hardware likely will be more modest.

The speed of small drones, as already illustrated by drone racing variants, and advancements in sensors and UAS add-on technology, such as infrared and night-vision cameras, light detection and ranging (LiDAR) systems and terrain- or facility-mapping tools, will compound these problems, as will things like decentralized manufacturing processes facilitated by 3-D printing, which will make field UAS production and related repairs easier.[358] That does not mean that new commercial UAS variants will be infallible or that the pace of change associated with the various subtechnologies that support drones will be steady, but that even without emerging technology, they will be more capable.

This naturally also means that the tools to counter, disable or defeat UASs will be more capable too. The broader use of commercial drones, as we have already seen, will also be accompanied by regulatory

354 "Joint Doctrine Note 2/11," p. 6–13; Scharre, *Robotics on the Battlefield, Part 2*, p. 42.

355 Scharre, *Robotics on the Battlefield, Part 2*, p. 42.

356 "Attack of the Drones—the Dangers of Remote-Controlled Aircraft."

357 I thank Paul Scharre for this point.

358 For example, see Kit Eaton, "The Perfect Tech Storm: 3-D Printed, Self-Assembling Drone Swarms," *Fast Company*, July 31, 2013; see also Emma Bryce, "This Ultraviolet Printer is 100X Faster than Ordinary 3D Printers," *Wired*, August 13, 2015; and Jordan Golson, "A Military-Grade Drone That Can Be Printed Anywhere," *Wired*, September 16, 2014.

changes that will likely lead to a further rationalization of airspace and export-control restrictions; factors that could make it harder for terrorist actors to acquire specific technology or fly drones when and where they want to.[359] The evolution of defensive tactics will pose challenges for terrorists as well.

Emerging technologies that have disruptive potential complicate things even more. Some of the most significant technologies that will drive changes in UAS capabilities include artificial intelligence, autonomous systems and robotics; miniaturization and swarming; nanoexplosives and directed-energy weapons; enhanced processing power and data mining; and cyber tools.[360] Advancements in autonomy, which are occurring rapidly, are bound to create new opportunities for terrorists and state agents alike, as changes in this area allow for a person or group to simultaneously operate multiple drones and potentially cause more destruction as a result.[361] While each of these technologies will present its own set of counterterrorism challenges, future terrorist threats, specifically those involving drones, likely will be tied to the combined use of several of these technologies as a system.

For example, imagine a scenario in which a terrorist group is able to design and print its own micro-drones by the thousands using a commercially available 3-D printer, a feat that researchers at Harvard University have already accomplished.[362] Powered by new and smaller energy sources, these micro-drones could then be programmed to fly autonomously as part of a large, networked swarm, whereby they would aim to overwhelm "enemy defense by their sheer numbers."[363] A terrorist group could develop several of these UAS swarms, some as general deception (to distract and confuse authorities) and others with larger and more capable UASs loaded with chemical or biological weapons hidden within the UAS swarm clouds. Using software that will enable the discovery of large collections of people (perhaps based on their mass, heat or digital signatures) in an urban environment, these larger drones would hunt down these high-density groups and release their toxic agents via air delivery so they could inflict the most harm. (Researchers affiliated with Central European University have already developed software for UASs that evaluates the size of crowds.[364])

The accompanying microswarms could be programmed to achieve three supporting tasks: (1) to protect the larger drones (i.e., by defeating local UAS countermeasure systems) and to ensure the successful delivery of the toxic agents; (2) to film and broadcast the attack; and (3) to fly through the dispersion area immediately after chem-bio release, and then to other nearby areas so the zone of contamination could be extended.[365] Borrowing a style of attack that is already popular with today's terrorist groups, the attack could be designed as a phased or multipronged operation, just like LeT's

359 I thank Brian Jackson for highlighting this point.

360 For background on these issues, see Ben FitzGerald, Kelley Sayler and Shawn Brimley, "Game Changers: Disruptive Technology and U.S. Defense Strategy," Center for a New American Security, September 27, 2013; see also James Manyika et al., "Disruptive Technologies: Advances That Will Transform Life, Business and the Global Economy," McKinsey Global Institute, May 2013. See also "Joint Doctrine Note 2/11," pp. 62–71; T. X. Hammes, "In an Era of Cheap Drones: US Can't Afford Exquisite Weapons," Defense One, January 16, 2016; T. X. Hammes, "Technologies Converge and Power Diffuses: The Evolution of Small, Smart, and Cheap Weapons," *Policy Analysis* (CATO Institute), no. 786, January 27, 2016. Autonomy "refers to a specific action that a machine can take independently, without human intervention." See Samuel J. Brannen, *Sustaining the U.S. Lead in Unmanned Systems: Military and Homeland Considerations through 2025* (Washington, D.C.: Center for Strategic and International Studies, February 2014), p. 5; for background on robots and robotics see Scharre, Robotics on the Battlefield, Part 2, p. 11.

361 I thank Paul Scharre for his suggestions related to this issue.

362 For background, see Scharre, *Robotics on the Battlefield, Part 2*, p. 20; Radhika Nagpal, "The Kilobot Project," www.eecs.harvard.edu/ssr/projects/progSA/kilobot.html; see also Eaton, "The Perfect Tech Storm;" for other threat-scenario variations involving potential future terrorist use of UASs, see Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles*, pp. 28–33.

363 As noted by Paul Scharre: "The point of building large numbers of lower cost systems is not to field forces on the battlefield that are qualitatively inferior to the enemy. Rather, it is to change the notion of qualitative superiority from an attribute of the platform to an attribute of the swarm. The swarm, as a whole, should be more capable than an adversary's military forces." See Scharre, *Robotics on the Battlefield, Part 2*, p. 10, 21.

364 For background, see Austin Choi-Fitzpatrick's "Drones for Good" project at www.austinchoifitzpatrick.com/dronesforgood/.

365 The Naval Postgraduate School is already experimenting with UAS swarm–fighting scenarios. See "Dogfighting Drones—Swarms of Unmanned Battle-Bots Take to the Skies," airforce-technology.com, July 23, 2012.

devastating November 2008 attack in Mumbai, which involved the terrorists attacking four targets simultaneously.

An attack like this one may never materialize, but the introduction of these new technologies will create additional system-based options for terrorist groups, a trend that will favor the creative and make counterterrorism harder. This is a future that will require agile, outside-the-box thinking, as terrorists, as they always do, will seek to outwit their opponents and level the asymmetric playing field through a mix of cunning and bold operations. Even though the United States and other Western countries are the principal agents developing this technology, it is not clear if they are prepared for this future and what it might mean in the counterterrorism domain, as these technologies are shifting strength from hard power and conventional weapons to the artistic—solutions that involve the combined use of inputs that are small, fast and many. The Islamic State's use and manipulation of Twitter is one good example of this. Indeed, as noted by Paul Scharre, "the history of revolutions in warfare has shown they are won by those who uncover the most effective ways of using new technologies, not necessarily those who invent the technology first or even have the best technology."[366] The immediate danger posed by terrorist use of UAS lies in human-machine teaming, and it is in that area that the world will get a glimpse of the future potential—and complexities—that emerging technologies hold.

366 For background see Scharre, *Robotics on the Battlefield, Part 2*, p. 42.