



# Defending Against UAVs Operated by Non-State Actors

Final Thesis, GMAP 16

David Kovar

Introduction .....	4
Background .....	6
Types of UAVs .....	6
UsUAS Deployment Examples .....	9
Defining a Win.....	13
Counter-UAV Systems.....	14
Counter-UAV Challenges.....	15
Attack surface .....	15
Legal Challenges Facing Civilian Counter-UAV Systems .....	16
Detection and Classification .....	17
Possible Criminal Charges .....	20
Physical/Kinetic .....	22
Radio Frequency Jamming .....	22
Radio Frequency Hacking.....	23
Legal Challenges Summary .....	24
Technical Counter-UAS Challenges.....	26
UsUAS Detection.....	26
UsUAS Neutralization – Technical Challenges.....	28
Geofencing .....	28
Physical/kinetic .....	30
Jamming.....	31
Hacking.....	32
Technical Challenges Summary .....	34
Dual Use and Open Source Technology.....	34
CanberraUAV and the Outback Challenge.....	35
Microsoft and UAV Simulation Software .....	36
Conclusion.....	37
Further research .....	40
Bibliography .....	42

## Acknowledgement

This thesis and my success in Fletcher's GMAP program would not have been possible without the support of many people. First and foremost to my mother, Mary Grace Kovar, who taught me to appreciate knowledge, trusted me to make mistakes and survive, and who made attending Fletcher possible.

Christopher Korody, Ross Stapleton-Gray, and several of my fellow Fletcher students provided significant support, research, and insights, all very much appreciated.

Finally, many thanks to my wife, Hilary Justice, for demonstrating the value of education and academic discourse in large ways and small throughout our lives and for supporting the academic duckling that she married through this very challenging year.

## Introduction

A technical revolution over the past decade brought unmanned aerial vehicle (UAV) capabilities once available only to well-funded militaries into the hands of anyone with a credit card and basic technical skills. These low cost, easily modified, and consumer friendly UAVs extend threats familiar to civilians and non-state actors in conflict zones to civilians in the Western world.

The perils of dual use technology – technology that can be used for civilian and military purposes - are very familiar to Western nations. In the past, such technology was often developed in the U.S. and, through export controls, relatively easy to contain, at least with respect to non-state actors. Cyberspace and globalization radically changed this dynamic. While military UAVs certainly were born in the United States, China is responsible for leading the development and export of consumer UAVs.

Qiao and Wang were senior colonels in the Chinese military writing in 1999 in one of the most influential publications for future military leaders of the time, *Unrestricted Warfare*. “ ... (they) are great believers in the imminence of an RMA (Revolution in Military Affairs), but they see the key elements of it emerging from the commercial sector, where China is surging forward. ‘The new concept of weapons will cause ordinary people and military men alike to be greatly astonished at the fact that commonplace things that are close to them can also become weapons with which to engage in war.’ They go on to add, “We believe that some morning

people will awake to discover with surprise that quite a few gentle and kind things have begun to have offensive and lethal characteristics."<sup>1</sup>

They were not only prophetic, they were writing from the country that is leading the commercial sector that is selling those commonplace things to civilians, militaries, and non-state actors.

Are the technical counter measures and the associated regulatory environments available to western military, law enforcement organizations, and civilians sufficient to prevent attacks by non-state actors using commercial UAVs? This paper will demonstrate that counter-UAV technology is, and will continue to be, unable to meet the full scope of the potential threat posed by non-state actors due to costs, insufficient capabilities, deployment challenges, and regulatory issues.

The author hopes to help readers understand the potential impact of consumer UAVs in the hands of non-state actors as well as the technical and regulatory challenges present in the United States that we face so that they can make informed decisions about public policy choices, investments, and risk.

A combination of articles, white papers, and military theses will be used to document the current threats posed by consumer and commercial UAVs. Vendor white papers, trade articles,

---

<sup>1</sup> P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (Penguin Press, 2009), pg 247

and research papers will be used to document the current state and cost of counter-UAV systems. Finally, a review of the U.S. legal and regulatory environment will demonstrate that counter-UAV capabilities face significant deployment challenges off of the battlefield.

## Background

Unmanned Aerial Vehicles (UAVs) are more commonly known as drones as well as a variety of other names depending on context and environment. The term broadly covers any aerial vehicle that is flown by someone outside of the aircraft or by an autonomous system, a computer. The term covers all such systems without regard for size, weight, payload capacity, or purpose. A UAV is the aircraft component of an Unmanned Aerial System (UAS) that also includes a ground control station, often a mobile device for consumer UAVs, and communications equipment.

## Types of UAVs

The United States Department of Defense divides UAVs into five different groups<sup>2</sup>:

---

<sup>2</sup> “Unmanned Aircraft System Airspace Integration Plan” (Department of Defense, March 2011), pg 42, [http://www.acq.osd.mil/sts/docs/DoD\\_UAS\\_Airspace\\_Integ\\_Plan\\_v2\\_\(signed\).pdf](http://www.acq.osd.mil/sts/docs/DoD_UAS_Airspace_Integ_Plan_v2_(signed).pdf).

UAS Groups	Maximum Weight (lbs) (MGTO)	Normal Operating Altitude (ft)	Speed (kts)	Representative UAS	
Group 1	0 – 20	<1200 AGL	100	Raven (RQ-11), WASP	
Group 2	21 – 55	<3500 AGL	< 250	ScanEagle	
Group 3	< 1320	< FL 180		Shadow (RQ-7B), Tier II / STUAS	
Group 4	>1320		> FL 180	Any Airspeed	Fire Scout (MQ-8B, RQ-8B), Predator (MQ-1A/B), Sky Warrior ERMP (MQ-1C)
Group 5		Reaper (MQ-9A), Global Hawk (RQ-4), BAMS (RQ-4N)			

The United States Federal Aviation Administration uses a much simpler classification based on the aircraft's weight – those 55lbs or less in one category and those over 55lbs. Those under 55lbs are roughly equivalent to the Group 1 and Group 2 military UAVs.

This paper addresses the use of Group 1 & 2 UAVs by non-state actors. These UAVs are of interest for this thesis because:

- They can be purchased anonymously over the Internet in most developed nations
- They generally cost less than \$1,500 and extremely capable ones less than \$5,000
- The registration and regulatory requirements in most countries are extremely lax
- They can easily be modified to provide capabilities similar to Group 1 & 2 military UAVs

Military Group 1 & 2 UAVs generally support ISTAR capabilities - information, surveillance, target acquisition, and reconnaissance. To date, onboard offensive capability was only available on Group 3, 4, & 5 military UAVs.

Non-state actors have deployed Commercial Off the Shelf (COTS) UAVs in all of the ISTAR roles. In this past year, non-state actors have also modified these UAVs to provide offensive capabilities.

For the purposes of this paper we will define an Unconventional Small Unmanned Aerial System (UsUAS) as an unmanned aircraft plus supporting ground control systems with the following characteristics:

- Group 1 UAV (0-20 lbs. maximum weight, less than 1200 ft. AGL operating altitude, less than 100 knots)
- Available to civilians without a license or other documentation
- Priced below \$5,000
- Used for military purposes – ISTAR plus offensive actions
- Operated by non-state, criminal, or activist actors

We will also define an attacker as the operator of a UsUAS and a CUAS operator as the operator of a counter-UAV system who is responsible for defending a site against UsUAS attacks.

## UsUAS Deployment Examples

A number of non-state actors have employed UsUAS on the battlefield. This paper focuses on their use by ISIS to demonstrate the capability of the platforms in the hands of an organized actor. According to a report by the Center for the Study of the Drone at Bard, of the one hundred ninety-four reported UAV sightings in Syria and Iraq since 2014, sixty one of those were consumer UAVs.<sup>3</sup>

In 2014, ISIS first deployed UsUAS in a role for which they were designed – producing video for propaganda films.<sup>4</sup> Later that year they released another video documenting their use of UsUAS in a surveillance role.<sup>5</sup> In 2015 an ISIS propaganda film demonstrated UsUAS performing command and control and artillery spotting missions<sup>6</sup>. In October of 2016, ISIS achieved their first kill with a UAV configured as a SVBIED<sup>7</sup>. By November of 2016 ISIS was regularly using modified DJI Phantom UAVs to drop grenades on military and civilian targets.<sup>8</sup>

---

<sup>3</sup> “Drones Operating in Syria and Iraq,” *Center for the Study of the Drone*, December 13, 2016, <http://dronecenter.bard.edu/drones-operating-in-syria-and-iraq/>.

<sup>4</sup> John Hall, “Latest ISIS Video Shows Drone View of Kobane’s Battle-Ravaged Streets,” *Mail Online*, December 12, 2014, <http://www.dailymail.co.uk/news/article-2871389/ISIS-propaganda-Call-Duty-style-Latest-footage-shows-drone-s-view-battle-ravaged-streets-Kobane-swooping-gun-battles-ground.html>.

<sup>5</sup> Peter Bergen and Emily Schneider, “Now ISIS Has Drones?(Opinion) - CNN.com,” accessed February 2, 2017, <http://www.cnn.com/2014/08/24/opinion/bergen-schneider-drones-isis/>.

<sup>6</sup> Caleb Weiss, “Islamic State Uses Drones to Coordinate Fighting in Baiji,” *FDD’s Long War Journal*, April 17, 2015, <http://www.longwarjournal.org/archives/2015/04/islamic-state-uses-drones-to-coordinate-fighting-in-baiji.php>.

<sup>7</sup> Michael S. Schmidt and Eric Schmitt, “Pentagon Confronts a New Threat From ISIS: Exploding Drones,” *The New York Times*, October 11, 2016, <https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html>.

<sup>8</sup> “US Commander Hails Iraqi Forces Beating ISIS Drones and VBIEDs,” *Rudaw*, accessed February 7, 2017, <http://www.rudaw.net/english/middleeast/iraq/110120171>.

The article documenting UAVs used to deliver munitions also offered several important facts:

- “The drones have not been used to deliver chemical weapons as of yet, Sylvia noted...”

As we will demonstrate, this capability is well within the reach of ISIS even if the chemical weapons are not.

- “They (allied forces) have brought down at least a dozen (ISIS UAVs), Sylvia noted.”

When a new DJI Phantom costs approximately as much as an AK-47 in Iraq, ISIS can afford to lose dozens.<sup>9</sup>

In two years, ISIS went from using an occasional UsUAS for propaganda purposes to losing dozens of them a month in late 2016 in weapons delivery operations.

Recent investigations show that ISIS developed a well-supported UsUAS program complete with user guides<sup>10</sup>, requisition forms, operations checklists, and after action reports to gauge operational effectiveness.<sup>11</sup> The collection of documents provided several other important insights that bear on our hypothesis:

- “Iraqi officials said bombs dropped by the drones, which were primarily quadcopters, had killed about a dozen government soldiers and injured more than 50.”

---

<sup>9</sup> “AK-47 and Other Guns on the Black Market - Havocscope,” accessed February 7, 2017, <http://www.havocscope.com/black-market-prices/ak-47/>

<sup>10</sup> ...السلام عليكم ورحمة الله وبركاته رسالة عاجلة الى الشخص الذي يدير طائرات الدولة الاسلامية الاستطل“ - Justpaste.it,” accessed February 7, 2017, <https://justpaste.it/jnabi7>.

<sup>11</sup> Michael S. Schmidt and Eric Schmitt, “Pentagon Confronts a New Threat From ISIS: Exploding Drones,” *The New York Times*, October 11, 2016, <https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html>.

- The UsUAS are lethal and effective
- “It poses a threat to troops on the ground, and it has value as a propaganda technique”
  - In addition to being lethal, the propaganda value on the battlefield must be considered, and all the more so if deployed against domestic targets
- Some documents were feature requests. “For example, to protect the transmission of their drone video feeds, members of the group wanted to acquire encrypted video transmitters and receivers, the assessment said.”
  - ISIS is investigating modifications to consumer UAVs designed to mitigate possible UsUAS counter measures
- “So it shows consistency and standardization, certainly with some sort of chain of supply in place,” he said.’
  - The program is well organized, on par with what we would expect from a Western commercial operation.
- “In the short term, we should expect the Islamic State to refine its drone bomb-drop capability,” the assessment concluded. “It is likely that the Islamic State’s use of this tactic will not only become more frequent, but more lethal as well.”
  - The effectiveness and capability of these UsUAS will likely increase in lethality and in operational capabilities
- These captured documents were from 2015.
  - The program has matured at least a year beyond what is recorded in the captured documents.

Highly capable UsUAS are not limited to well established non-state terrorist organizations.

Criminal cartels utilize long range, large payload UsUAS for drug delivery. “The drone was used to carry cocaine to Panama, it had the capacity to transport 10 kilograms (22 pounds) per journey and it traveled a 100-kilometer (62 mile) distance,” Acevedo said.<sup>12</sup>

And solo activists have used them to deliver radioactive payloads to the roof of the Japanese Prime Minister’s office.<sup>13</sup>

Dan Goure sums up the problem in two statements. First, “The U.S. and its Coalition allies no longer have sole use of the air domain. Drones provide our adversaries with the ability to conduct aerial ISR, mission command, targeting and even precision strike -- all capabilities that were, until recently, solely the province of wealthy militaries.”<sup>14</sup> And secondly, “... the U.S. has a similar capability consisting of dozens of manned airborne sensors and command and control aircraft, .... However, the U.S. capability requires thousands of people and costs many billions of dollars.” ISIS is providing the same capabilities, albeit on a tactical rather than strategic level, with dozens of people and less than \$20,000.

---

<sup>12</sup> Ananya Bhattacharya, “Colombia’s Narcotics Smuggling Is Going Hi-Tech with Drone Deliveries,” *Quartz*, November 19, 2016, <http://qz.com/841327/colombias-narcotics-smuggling-is-going-hi-tech-with-drone-deliveries/>.

<sup>13</sup> David Kravets, “Man Lands Drone Carrying Radioactive Sand on Japanese Prime Minister’s Office,” *Ars Technica*, April 25, 2015, <https://arstechnica.com/tech-policy/2015/04/man-arrested-for-flying-drone-carrying-radioactive-sand-in-tokyo/>.

<sup>14</sup> Goure, Dan. "Drone Wars: Defeating the Unmanned Threat Will Require A Firestorm Of Energy." *The National Interest*. July 27, 2016. Accessed December 23, 2016. <http://nationalinterest.org/blog/the-buzz/drone-wars-defeating-the-unmanned-threat-will-require-17144>.

## Defining a Win

Our hypothesis is that Western nations are not prepared to defend civilian populations against the use of small UAVs by non-state actors. This can be proved false by:

- Identifying counter-UAV technology that can be deployed to effect a “win” against currently available UAVs that meet the UsUAS definition
- Identifying the regulations that allow the technology to be utilized within the borders of the United States and at sites not covered by “no fly zones”.
- Demonstrating that the solutions are capable of being deployed at sufficient scale to protect all possible targets, not just major events

The defenders are at a classical asymmetric warfare disadvantage – they need a nearly 100% success rate, and if they can demonstrate that success, even better. This is essentially an impossible victory condition to meet. If the scope is limited to critical infrastructure, and if the rules of engagement are adjusted, the odds increase dramatically for the defenders but are still daunting.

Attackers win if they can conduct a single terror attack using a UsUAS against any civilian target, one of thousands of Friday night high school football games for example.

A successful attack need not injure or kill civilians. It may not even make major headlines. It just needs to demonstrate enough capability to generate sufficient public outcry to slow consumer and commercial UAV sales and deployment. Lawmakers already show a great deal of interest in

responding to requests for greater regulation and the industry has demonstrated little effective lobbying power to hold off these regulations. A notable hostile use of a consumer UAV could result in regulation that would have significant impact on the civilian industry predicted to be worth \$2 billion by 2020.<sup>15</sup>

## Counter-UAV Systems

The military first coined the phrase “kill chain” but it has crept into civilian use, particularly in cyber security where corporations are under constant cyberattack. A Sandia National Labs report<sup>16</sup> defined a three step kill chain model:

1. Detection – The collection of some phenomenological information captured by a sensor. This step does not necessarily denote classification (that is, differentiation of nuisance alarm versus target).
2. Classification – Analysis of data received in the detection phase, with the goal being to separate real targets from highly cluttered, noisy background data. When this step is performed solely by a human, considerable care must be taken to understand how nuisance alarms affect classification performance.

---

<sup>15</sup> B. I. Intelligence, 2016 Oct. 2, and 092 2, “THE DRONES REPORT: Market Forecasts, Regulatory Barriers, Top Vendors, and Leading Commercial Applications,” *Business Insider*, accessed February 15, 2017, <http://www.businessinsider.com/2016-10-2-uav-or-commercial-drone-market-forecast-2016-9>.

<sup>16</sup> Gabriel Birch, John Griffin, and Matthew Erdman, “UAS Detection, Classification, and Neutralization: Market Survey 2015” (Sandia National Laboratories, 2015), <http://prod.sandia.gov/techlib/access-control.cgi/2015/156365.pdf>.

3. Neutralization – Once a target is positively identified in the previous step, additional action must be taken to deny mission success, including the potential for target neutralization.

An effective counter-UAV system must successfully execute each step in the chain in order. It must detect a very small flying object against a complex visual, audio, and radio frequency background. It then must determine that the UAV's operator has malicious intent and possibly determine the risks associated with that intent to select the most appropriate response. Then, and only then, must the system effectively neutralize the malicious UAV without causing collateral damage. Failure to detect or neutralize UsUAS will result in a successful attack. Failure to correctly classify a UAV may result in a false positive and the neutralization of a benign UAV.

## Counter-UAV Challenges

Successful deployment of counter-UAV systems must overcome a variety of challenges, chief among them the size of the attack surface, the legal and regulatory environment, the technical capabilities on both sides, and the nature of dual use technology.

### Attack surface

On the battlefield, only military units and installations must be defended. These are generally already equipped with a wide range of detection equipment and defensive weapons, along with the personnel, procedures, and rules of engagement to determine if a UAV is a threat and to deploy weapon systems against it.

When the battlefield includes civilian populations the attack surface expands greatly even if combatants do not intentionally target civilians. But, as it is still a combat zone, equipment, personnel, procedures, and rules of engagement are still available.

The United State's greatest challenge in combating UsUAS is the theatre of operations – domestic soil. When a UsUAS could be used to drop incendiary flares on Western forests, or agricultural toxins on Midwest farm fields, or tear gas on East Coast high school football games, the defenders face insurmountable odds as nearly all sites, infrastructure, and events are possible targets.

To make matters worse, the military's effectiveness in responding is greatly curtailed. The number of military units per capita is very low, the units generally lack offensive and defensive systems ready for deployment, and the military's rules of engagement on domestic soil preclude any form of immediate response without specific government decree.

Finally, if a 100% effective detection and deterrent system could be developed and made available at a reasonable cost, the financial and logistic expense would exceed the nation's capability and willingness to deploy it at all possible targets.

## [Legal Challenges Facing Civilian Counter-UAV Systems](#)

Consumer/commercial unmanned aerial vehicles sales and operations are increasing rapidly according to sales figures, media reports, and various studies. So too are unconventional uses of these drones by non-state actors and criminals, as well as perceived privacy violations by regular operators. The result is a well-funded rush to develop UAV detection and counter measure systems for military and civilian use. At present, someone employing a counter-UAV system may be engaged in more serious criminal activity than the operator of the UAV. If the legal challenges affecting the deployment of these systems are not addressed, not only will those investments be put at risk but our nation may be exposed to greater risk of malicious UAV operations.

The technical challenges and efficiency of the solutions are often shrouded behind intellectual property protection at various startup companies. The legal challenges, however, are clearly defined in existing public law and regulation. We all have a vested interest in working with local, state, and federal lawmakers to enact new regulations that will enable individuals, corporations, and law enforcement agencies to effectively and legally defend against malicious UAVs.

#### Detection and Classification

Simply detecting a UAV and classifying it as a UsUAS faces legal challenges. In the United States there are very few areas where aircraft crossing a perimeter may automatically be treated as hostile or at least malicious. A declared National Defense Airspace as was used for the 2017

Presidential Inauguration is the most recent example.<sup>17</sup> In addition to civil and criminal charges, “the United States government may use deadly force against the airborne aircraft, if it is determined that the aircraft poses an imminent security threat.” These are the only areas within the United States borders where deadly force is authorized against aircraft, which includes UsUAS. Recent incursions into the airspace over the White House by UsUAS<sup>18</sup> and by small aircraft<sup>19</sup> illuminate both the difficulty of detecting incursions by these types of aircraft and the perceived unwillingness to engage them even over the most critical building in the United States.

Temporary Flight Restrictions (TFRs) issued by the FAA provides for temporary control of the airspace by other agencies and allows them to administratively control access to the airspace. Access violations are addressed through civil and criminal charges, if the operator can be located. Deadly force used against the aircraft is not authorized under the Federal Aviation Regulations or their underlying statutes.

For several years agencies fighting wildfires in the western part of the United States have engaged in an ongoing dance with UAV operators who violate the TFRs established to enable

---

<sup>17</sup> “FLIGHT ADVISORY NATIONAL SPECIAL SECURITY EVENT 2017 PRESIDENTIAL INAUGURATION FESTIVITIES” (Federal Aviation Administration, December 2016), [https://www.faa.gov/files/notices/2016/Dec/2017\\_Inauguration\\_Advisory.pdf](https://www.faa.gov/files/notices/2016/Dec/2017_Inauguration_Advisory.pdf).

<sup>18</sup> Michael S. Schmidt and Michael D. Shear, “A Drone, Too Small for Radar to Detect, Rattles the White House,” *The New York Times*, January 26, 2015, <https://www.nytimes.com/2015/01/27/us/white-house-drone.html>.

<sup>19</sup> “Florida Mailman Lands a Gyrocopter on Capitol Lawn, Hoping to Send a Message,” *Washington Post*, accessed January 30, 2017, [https://www.washingtonpost.com/local/florida-mailman-lands-a-gyrocopter-on-capitol-lawn-hoping-to-a-send-message/2015/04/15/3be11140-e39a-11e4-b510-962fcfab310\\_story.html](https://www.washingtonpost.com/local/florida-mailman-lands-a-gyrocopter-on-capitol-lawn-hoping-to-a-send-message/2015/04/15/3be11140-e39a-11e4-b510-962fcfab310_story.html).

aviation assets to safely operate near the wildfires. “Twenty-one drones were spotted at the scenes of wildfires nationwide in 2014-2015, and aircraft were grounded six times. And there have been at least two occasions when firefighting aircraft have had to take evasive actions to avert a collision with drones.”<sup>20</sup> Few operators have been located or charged. One operator who was located was charged with a misdemeanor for interfering with firefighting operations and fined \$1,000. A stricter law with harsher punishments was introduced in California assembly but failed to pass.

The legal opportunities to challenge UsUAS operations over most federal lands open to the public as well as private or commercial property are even more limited. The debate hinges around two core issues: Who controls the airspace and privacy.

It is generally accepted that the Federal Aviation Administration controls all of the National Airspace (NAS). Many jurisdictions are attempting to write laws that depend on their ability to regulate local airspace, something they have no legal authority to do. Orlando, FL recently crafted an ordinance that may be more successful in defending against challenges by addressing the use of city land rather than the airspace. “It is prohibited to cause an unmanned aircraft to launch or land, or for any person to operate or assist in the operation of any

---

<sup>20</sup> Jeff Daniels, “Feds Turn up the Heat in Fight against Drones Interfering in Wildfires,” *CNBC*, July 26, 2016, <http://www.cnbc.com/2016/07/26/feds-turn-up-the-heat-in-the-fight-against-drones-interfering-in-wildfires.html>.

unmanned aircraft system out of doors unless permitted to do so by the City of Orlando, when that person is on city property.”<sup>21</sup>

The vast majority of citizens in the United States desire to be free from surveillance by the government and by other citizens. Unfortunately, there are essentially no laws that protect an individual’s privacy outside of the walls of their homes. Any effective law would need to apply to all forms of aerial surveillance including helicopters, airplanes, and satellites. UAVs reignited and fueled debate and possible regulations addressing privacy protection from aerial surveillance but there are no broad laws in place that provide for civil or criminal redress, and particularly no laws that provide for shooting, netting, jamming, or hacking into an UsUAS.

#### Possible Criminal Charges

Non-military UAVs are susceptible to a variety of attacks that may disable them in flight, cause them to return to the launch point, or grant the attacker control over their operation. Methods range from shotguns to GPS jammers to nets and even to birds. Unfortunately, utilizing any of these methods in most domestic situations is illegal.

The following legal options for charging the CUAV operator will be referenced for each type of counter-UAV technique available. In addition to these criminal charges, other criminal charges and a variety of civil charges could be filed.

#### *State criminal offenses*

---

<sup>21</sup> “ORDINANCE NO. 2016-87” (The City Council of Orlando, Florida, December 7, 2016), [http://www.mynews13.com/content/dam/news/images/2017/01/4/Drone\\_UAS\\_Ordinance\\_-\\_12\\_7\\_2016.pdf](http://www.mynews13.com/content/dam/news/images/2017/01/4/Drone_UAS_Ordinance_-_12_7_2016.pdf).

- Larceny - The unlawful taking and carrying away of someone else's property without the consent of the owner; and with the intent to permanently deprive the owner of the property.<sup>22</sup> (state or local)
- Criminal mischief - Intentionally or knowingly damaging someone else's property (state or local)
- Reckless endangerment - Carelessness which is in reckless disregard for the safety or lives of others, and is so great it appears to be a conscious violation of other people's rights to safety (state or local)

*Federal criminal offenses*

- Destruction of aircraft - Sets fire to, damages, destroys, disables, or wrecks any aircraft in the special aircraft jurisdiction of the United States or any civil aircraft used, operated, or employed in interstate, overseas, or foreign air commerce. (18 U.S. Code § 32)
- Jamming – The use of devices designed to intentionally block, jam, or interfere with authorized radio communications is a violation of federal law.<sup>23</sup> (The Communications Act of 1934, 18 U.S.C. § 1362, 18 U.S.C. § 1367(a))
- FCC Violation – Operating an unlicensed transmitter or interfering with the legal operation of another transmitter. (The Communications Act of 1934, Sections 301 and 333)
- CFAA – “Knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without

---

<sup>22</sup> "Definition of Larceny." Findlaw. Accessed February 09, 2017.

<http://criminal.findlaw.com/criminal-charges/definition-of-larceny.html>.

<sup>23</sup> “Jammer Enforcement,” *Federal Communications Commission*, March 3, 2011, <https://www.fcc.gov/general/jammer-enforcement>.

authorization, to a protected computer” (Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

### Physical/Kinetic

A physical attack on a UsUAS is intended to cause the aircraft to cease operating. Example attacks include firearms, nets, and birds. A successful attack will cause the aircraft to fall to earth in an uncontrolled manner. Any attack that causes the aircraft to stop operating in a normal manner opens the CUAV operator up to being charged with criminal mischief if the UAV or property on the ground is damaged as a result. Any attack that causes the aircraft to cease operating will add opportunities to charge the CUAV operator with larceny, reckless endangerment, and destruction of aircraft due to the likelihood that the aircraft will strike the ground in an uncontrolled manner.

Discharging a firearm against an offending aircraft could result in injury or death to individuals other than the operator and is almost always a crime. Deadly physical force may only be legally used to counter deadly physical force.

The UsUAS operator can attempt to counter such an attack by flying erratically, either manually or via an automated flight path. Other defenses would require modifications to the aircraft that would likely be out of proportion to its value.

### Radio Frequency Jamming

Most commercial UAVs are configured to “fail safe” in the event of unexpected loss of signal or interference. An attacker can jam the GPS signal, causing the UsUAS to lose one of the guidance options. This normally results in erratic or fail safe behavior. A very careful GPS attack could force a UsUAS to land. An attacker can also jam either the control link used to operate the aircraft or the data link used to receive sensor data from the aircraft or both. Jamming the control link will result in a normally configured UAV to return to home and land.

A malicious operator can acquire a UAV capable of operating without a GPS signal or manually fly a standard UAV that has lost the GPS signal. This capability exists to allow indoor and other obstructed operations. The operator can disable the “return to home” function in the event of a control link loss and enable the UAV to continue operating in an autonomous mode.

The CUAV operator could be charged with larceny, criminal mischief, reckless endangerment, and destruction of aircraft depending on the outcome. The person could be charged a FCC violation for operating an illegal transmitter as well as a FCC violation for jamming. Some attacks, and specifically GPS jamming attacks, have the potential to create safety risks far beyond the offending aircraft and could result in other significant charges.

### Radio Frequency Hacking

Most commercial UAVs depend on a radio frequency communication link to enable the operator to control the aircraft either directly or through a ground control station that enables

semi-autonomous flight. This communication link is poorly secured in most cases and exploits are available for all major commercial UAVs. A CUAS operator can detect the frequencies in use and send signals on those frequencies to take control of the aircraft from the original operator. The CUAS operator will then attempt to land the aircraft either to terminate the operation or to seize physical control of the UsUAS.

It is difficult to configure most off the shelf commercial UAVs to operate without any control link. However, there are some off the shelf UAVs equipped with flight controllers that can easily be configured to shut down the radio link and then operate in a fully autonomous mode. Once configured in this manner, the UsUAS is impervious to radio frequency counter measures. It is also possible to utilize non-standard radio link systems or cellular network links to control the aircraft and thus complicate an attack on the control link. Such a configuration would still be detectable through radio frequency scans and possibly susceptible to jamming attacks.

The CUAS operator could be charged with larceny, criminal mischief, reckless endangerment, and destruction of aircraft depending on the outcome. The person could be charged with a FCC violation for operating an illegal transmitter as well as a FCC violation for jamming. And, in addition to all of the above, the CUAS operator is now remotely accessing a computer system without permission, a violation of the Computer Fraud and Abuse Act.

### [Legal Challenges Summary](#)

The vendors of one counter-UAV solution state the challenges clearly on their web site.

“This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased in the United States, other than to the United States government and its agencies, until authorization is obtained. Under current law, the DroneDefender may be used in the United States only by authorized employees of the Federal government and its agencies, and use by others may be illegal.”<sup>24</sup>

Technical issues aside, there is insufficient broad legal support to enable a CUAS operator to determine that the behavior of a commercial UAV is malicious and thus subject to actions to cease such operations or charge the attacker. Further, existing and frequently applied local, state, and Federal laws make almost all of the options available to counter malicious UAV operations illegal. These laws apply to civilians and law enforcement alike, and either group would require exemptions to deploy any of the known counter-UAV systems.

We must face the fact that there are very limited circumstances where physical force or electronic countermeasures are authorized against aircraft, including UsUAS. In all other circumstances, the legal options for defending against a UsUAS are all after the fact measures that require identifying and locating the operator. These are not significant barriers against non-state terrorists and criminal actors.

---

<sup>24</sup> “Counter-UAS Technologies,” accessed February 19, 2017, <https://www.battelle.org/government-offerings/national-security/tactical-systems-vehicles/tactical-equipment/counter-UAS-technologies>.

Our investment in counter-UAV technology should be matched with investment in updated laws and regulations to enable the deployment of these systems by organizations charged with defending our infrastructure and airspace. Failure to do so may put the public at risk. Failure to do so may also result in reactionary regulations passed immediately after a malicious event that would negatively impact an industry already challenged by overly burdensome regulations.

## Technical Counter-UAS Challenges

An effective counter-UAS system must overcome technical challenges relating to the environment, physics, and capabilities of both the defensive and offensive systems. Dual use technology and the nature of asymmetric warfare underscore many of these challenges.

### UsUAS Detection

Dan Goure provides a good summary of the detection challenges on the battlefield. "Defeating this new offset capability is going to be a challenge. The typical drone being used by ISIS, Hamas and Hezbollah are small, fly low and slow and can employ GPS-based automated guidance. Detecting them is a challenge. Most air surveillance radars don't even see them. Those that do can usually be fooled if the drone merely hovers. These drones are extremely quiet and have a low infrared signature."<sup>25</sup> A civilian environment serves to further complicate the detection component due to numerous benign aircraft operating and a busier radio frequency spectrum.

---

<sup>25</sup> Goure, Dan. "Drone Wars: Defeating the Unmanned Threat Will Require A Firestorm Of Energy." The National Interest. July 27, 2016. Accessed December 23, 2016. <http://nationalinterest.org/blog/the-buzz/drone-wars-defeating-the-unmanned-threat-will-require-17144>.

A Sandia National Labs report<sup>26</sup> provides the following summary of the effectiveness of current detection options against three possible commercially available small UAVs:

Detection scheme	Glider	Quadcopter	Jet
Radar			
Passive optics (i.e., cameras)			
Active optics (i.e., LIDAR)			
Acoustics			
EM emissions			
B-field detection			

Green – good. Yellow – mild. Red – poor.

There are no good options for any of the UAVs and a jet turbine based UAV, which is commercially viable, is particularly difficult to detect and also requires an extremely fast response time.

Commercial detection systems are often constrained by cost, effectively eliminating radar, active optics, and magnetic detection systems as viable options. Acoustic systems are relatively low cost but require an extremely large and regularly updated library of signatures. Acoustic

<sup>26</sup> Gabriel Birch, John Griffin, and Matthew Erdman, “UAS Detection, Classification, and Neutralization: Market Survey 2015” (Sandia National Laboratories, 2015), <http://prod.sandia.gov/techlib/access-control.cgi/2015/156365.pdf>.

performance in an urban environment is very poor with a high rate of false positives. Simple physical modifications to a UsUAS can significantly alter its acoustic signature. Radio frequency detection is the most common and most effective system against commercial UAVs but can easily be defeated by turning off all transmitters and flying autonomously.

The Sandia report summarizes the detection challenges facing the defenders.

- No sensor type alone is able to provide sufficient tracking and identification capability to offer a reliable and effective defense against the LSS (low, slow, and small) threat.
- To provide a satisfactory performance, the use of an adequate mix of sensors will be crucial, increasing the cost and complexity of the system

### UsUAS Neutralization – Technical Challenges

Once a UAV has been detected and determined to be malicious it must be neutralized. Forcing it to stop functioning and crash to the ground is the simplest outcome but the resulting damage may compromise useful forensic evidence. Collateral damage to people and property must also be considered. Techniques that prevent a UsUAS from crossing a boundary or force it to return to the launch point may prevent the current attack but also reduce the defender's ability to collect intelligence about the attack. Techniques with a high probability of success that also enable the defender to capture the UsUAS intact are the most desirable and do exist.

### Geofencing

The broadest, most effective deterrent to, not defense against, UAVs operating in restricted areas is geofencing – the establishment of a virtual border around an area that is encoded in the UAV’s flight controller and prevents the UAV from entering the area. It is nearly 100% effective against accidental incursions. Unfortunately, it is essentially useless against intentional incursions.

- It is available many major vendor’s products but not on home or kit built products
- Hardware is available for most DJI models that defeats the geofence without interfering with the GPS
- DJI admits that the geofence database can be defeated. “Even if it (geofencing) did ban flights there (Syria and Iraq), DJI says that the ban could theoretically be circumvented, since Phantoms aren’t shipped with military-grade encryption that would prevent a user from tampering with the restrictions.”<sup>27</sup>

By tweaking the data, Michael Robinson did just that. He was able to make his Phantom ignore the manufacturer-set no-fly zones. “I very easily downloaded the database and started just changing entries, which I found very interesting,” he said.<sup>28</sup>

---

<sup>27</sup> Kate Conger, “How Consumer Drones Wind up in the Hands of ISIS Fighters,” *TechCrunch*, accessed February 2, 2017, <http://social.techcrunch.com/2016/10/13/how-consumer-drones-wind-up-in-the-hands-of-isis-fighters/>.

<sup>28</sup> “Chuck Schumer’s No-Fly-Zone Rule for Drones Won’t Work,” *Defense One*, accessed February 12, 2017, <http://www.defenseone.com/technology/2015/08/chuck-schumer-no-fly-zone-drones/119389/>.

Geofencing depends on onboard GPS navigation. Civilian radio control (RC) model airplane pilots have been conducting long range first person view (FPV) flights for nearly a decade without GPS equipment. These are the platforms and electronic systems upon which modern consumer UAVs were built. Add a GPS for location awareness and a flight controller for automation and you transform a ten-year-old RC aircraft into a UAV. Conversely, if GPS system is removed from a modern UAV the operator can continue to conduct accurate long range missions. Geofencing is effective, but only against operators utilizing UAVs sold by a single vendor.

#### Physical/kinetic

Physical counter measures are designed to cause the UsUAS to physically cease operations and in some circumstances capture the aircraft. The most common forms of physical systems are firearms and nets though birds have been trained to attack UsUAS<sup>29</sup>. Net guns have been used for years to trap birds and they have been successfully deployed against UsUAS in controlled situations. Firearms are very prevalent in the United States and have been successfully deployed against UsUAS by civilians<sup>30</sup> and by law enforcement<sup>31</sup>.

---

<sup>29</sup> Kelsey Atherton, "Trained Police Eagles Attack Drones On Command," *Popular Science*, February 1, 2016, <http://www.popsci.com/eagles-attack-drones-at-police-command>.

<sup>30</sup> David Morris, "A Drone, a Shotgun, and the Future of Airspace Rights," *Fortune*, September 25, 2016, <http://fortune.com/2016/09/25/drone-shotgun-airspace-rights/>.

<sup>31</sup> Lauren Sigfusson, "Drone Pilot and FAA Comment on Drone Shooting at North Dakota Pipeline Protest | Drone360 Magazine," *drone360mag.com*, December 5, 2016, <http://drone360mag.com/news-notes/2016/10/drone-pilot-and-faa-comment-on-drone-shooting-at-north-dakota-pipeline-protest>.

Unfortunately, all physical counter measures can easily be evaded by the UsUAS operator. Net guns and firearms require skilled operators to use effectively and have very limited range, particularly against a rapidly moving or evading target. Trained birds are in limited supply, hard to train and operate, and can be injured in counter-UAV operators.

### Jamming

Radio frequency jamming is the most effective method for neutralizing a broad range of consumer or commercial UAVs and has been an effective military counter measure against many threats since the early days of radio. Typical consumer UAVs depend on signals on two frequencies for normal operations – GPS signals for navigation and command and control (C2) signals for flight controls, telemetry, and manual operations. These UAVs are designed to cease operations if either signal is lost or unreliable though they can be switched to manual mode and flown without a GPS signal by a proficient operator. If the C2 signal is jammed the UAVs are designed to return to home (RTH) and land or to hover in place until the power supply is exhausted.

Battelle's DroneDefender<sup>32</sup> is the most common example of an effective counter-UAV jamming system capable of interfering with both the C2 link and the GPS signal. Reports suggest that it is

---

<sup>32</sup> "Counter-UAS Technologies," *Battelle*, accessed February 13, 2017, <https://www.battelle.org/government-offerings/national-security/tactical-systems-vehicles/tactical-equipment/counter-UAS-technologies>.

successfully being deployed in the United States by authorized Federal agencies and abroad in combat zones by the United States military<sup>33</sup>.

Jamming is effective against any non-military UAV that is designed to fail safe in the event of a loss of GPS or C2 signal. It will be less effective or completely ineffective against UsUAS configured to operate in GPS denied areas or in a fully autonomous mode. The available systems are relatively inexpensive and easy to operate, enabling broad domestic deployment *if they are legal to operate in the United States*.

However, they can be defeated by using a combination of non-standard communications frequencies, manual control, or visual recognition guidance systems. These counter measures increase the cost and complexity for the attacker and have not been observed in the field though captured ISIS documentation suggests that they are being explored<sup>34</sup>.

## Hacking

Similar to jamming techniques, hacking requires knowledge of the UsUAS's frequencies but goes further in that it also requires knowledge of the communication protocols used on those frequencies. With this knowledge, it is possible to insert malware into the onboard flight controller though this technique has not been demonstrated publicly. Demonstrated hacks of

---

<sup>33</sup> Oriana Pawlyk, "Air Force Zaps ISIS Drone with Electronic Weapon," *Defensetech*, October 24, 2016, <https://defensetech.org/2016/10/24/air-force-zaps-isis-drone-with-electronic-weapon/>.

<sup>34</sup> Eric Schmitt, "Papers Offer a Peek at ISIS' Drones, Lethal and Largely Off-the-Shelf," *The New York Times*, January 31, 2017, <https://www.nytimes.com/2017/01/31/world/middleeast/isis-drone-documents.html>.

UAVs that purported to be malware attacks<sup>35</sup> were actually attacks on the C2 link that are designed to break the link between the original operator and the UsUAS so that the defender can capture the C2 link and take control of the UsUAS. If successful, this enables the defender to safely land the UsUAS, reducing damage to the aircraft and collateral damage. It also preserves valuable forensic evidence.

A cybersecurity researcher demonstrated what is known as a timing attack that works against the C2 link on all consumer UAVs as they share a common weakness. One of the researchers explains – “The issue is that all the RC systems from ALL the manufacturers count on frequency hopping obfuscation to "hide" their broadcasts which are easily gathered en masse and reversed with an SDR (software defined radio)<sup>36</sup>, or by using a logic analyzer on their transmitters, there is no cryptographically secure authentication layer on any of the current systems.”

The broad impact of this technique is very appealing but two more factors enhance the appeal – it is very inexpensive to implement, requiring approximately \$100 worth of parts, and the C2 link technology is so prevalent that it is prohibitively difficult and expensive to replace.

---

<sup>35</sup> Samy Kamkar, “Samy Kamkar - SkyJack: Autonomous Drone Hacking,” accessed February 13, 2017, <http://samy.pl/skyjack/>.

<sup>36</sup> The issue is that all the RC systems from ALL the manufacturers count on frequency hopping obfuscation to "hide" their broadcasts which are easily gathered en masse and reversed with an SDR, or by using a logic analyzer on their transmitters, there is no cryptographically secure authentication layer on any of the current systems.

This counter-UAS technique can be defeated. A malicious operator cannot easily replace the C2 link electronics on consumer UAVs. However, a variety of options exist for kit and home built systems. The most appealing communications link solution is cellular<sup>37</sup>. Cellular C2 links are very appealing to malicious actors for several reasons:

- Years of effort aimed at securing cellular communication makes cellular links very difficult to hack.
- Cellular links are designed to operate in challenging environments and are resistant to jamming.
- Cellular signals are extremely common in domestic environments and a UsUAS utilizing cellular C2 links will be much harder to pick out from all of the other signals.

### Technical Challenges Summary

If a UsUAS can be detected, and if it depends on either a radio frequency link or a GPS signal to operate successfully, it can be neutralized via relatively inexpensive and easily operated equipment. However, if a UsUAS is capable of operating fully autonomously and without dependence on GPS signals, neutralizing it would depend on long range firearms in the hands of a skilled marksman, a decidedly non-technical solution of limited effectiveness that scales poorly.

### Dual Use and Open Source Technology

---

<sup>37</sup> “Cellular Drone Communication,” *Qualcomm*, August 31, 2016, <https://www.qualcomm.com/invention/technologies/lte/advanced-pro/cellular-drone-communication>.

The fundamental challenge facing counter-UAS operators may be the nature of the technology it is dual use and predominantly open source technology. Counter-UAS legal and technical challenges are shaped, defined, and constrained by the very nature of consumer and commercial UAVs – they are extremely popular for recreational activity and are the instruments of rapid economic growth in industries ranging from real estate to agriculture to public utilities to film making. Regulations designed to restrict malicious activity, flight over crowds for example, would also restrict media and commercial applications. No reasonable technical restrictions on their capabilities could be brought to bear on Chinese firms and open source developers.

Modern consumer UAVs grew out of a combination of hobby or kit radio controlled aircraft combined with the development of open source software and hardware designed to enable anyone with sufficient motivation to build their own UAVs and collectively extend and enhance the capabilities of the entire consumer UAV ecosystem. There are two superb examples of this ecosystem at work, creating great benefit for society while simultaneously providing more capabilities to a malicious actor. One example highlights the contributions by open source and academics, the other by one of the world's largest corporations.

### Canberra UAV and the Outback Challenge

The stated goals of the Outback Challenge – Medical Express<sup>38</sup> competition were:

---

<sup>38</sup> “What Are the Aims of Medical Express?,” *UAV Challenge*, September 23, 2016, <https://uavchallenge.org/2016/09/23/what-are-the-aims-of-medical-express/>.

- Improved search algorithms (that can locate a person that is standing and is wearing normal clothes – i.e. a non-high visibility shirt).
- Cheap and reliable ground-to-ground communications (between a GCS and a remotely landed unmanned aircraft) over a distance of at least 5.4 nautical miles.
- Unmanned aircraft that can transit long distances and land and take off in a constrained area that is surrounded by obstacles. New hybrid platforms that are neither pure fixed-winged aircraft nor pure multi-rotors are likely to be required to complete the mission.
- Fully automatic takeoff and landing systems that can operate in a remote location – not only at the GCS end.
- On-board situational awareness of remote landing locations that are largely unknown to aircraft operators before a mission commences.

Each one of these goals furthers UAVs ability to benefit society while also enabling malicious actors to conduct more effective military and terrorist missions. A UAV capable of meeting these goals could target an individual on a rural estate, operate at very long ranges, land and take off without human intervention, and land or operate in an unfamiliar environment.

CanberraUAV met all of these goals, and more using off the shelf equipment and open source tools and software.<sup>39</sup>

## Microsoft and UAV Simulation Software

---

<sup>39</sup> “CanberraUAV Outback Challenge 2016 Debrief,” *ArduPilot Discourse*, accessed February 19, 2017, <http://discuss.ardupilot.org/t/canberrauav-outback-challenge-2016-debrief/12162>.

Microsoft just published and made available at no cost a simulation environment designed to speed the development of UAVs. "... an open source simulator, the Aerial Informatics and Robotics Platform, that helps designers test and train autonomous machines in realistic conditions without wrecking expensive prototypes."<sup>40</sup>

Malicious actors generally do not need to determine if their vision system can dodge a branch, one of the system's use cases. But they would certainly benefit from another use case – "It's more of a complement that can either account for hard-to-reproduce circumstances ...." (ibid)

Circumstances such as a flight over a major sporting event or through the urban canyons of New York City. If a malicious actor can model, fly, and tune their intended mission virtually in advance they will greatly increase their odds of mission success.

## Conclusion

At the present time, the ease of access to the capabilities of consumer UAVs for non-state actors to wage asymmetric warfare or engage in terror attacks cannot be offset by current technical and regulatory solutions.

Non-state actors have demonstrated the ability to use off the shelf consumer UAVs to conduct information, surveillance, target acquisition, and reconnaissance missions as well as offensive SVBIED and aerial bombardment missions against United States and allied forces. Criminal organizations have deployed kit built UAVs capable of flying in excess of 60 miles while carrying a 20lbs payload. Individual activists have delivered radioactive samples to the roof of

---

<sup>40</sup> "Microsoft Drone Simulator Helps You Prevent Real-World Crashes," *Engadget*, accessed February 19, 2017, <https://www.engadget.com/2017/02/15/microsoft-drone-simulator/>.

government buildings. The capability clearly exists to use consumer UAVs to deliver payloads that would incite terror if deployed against domestic targets.

Technically, the vast majority of consumer off the shelf UAVs can be detected and neutralized due to their dependence on well known, very standardized radio frequency equipment used for the command and control links required for their normal operation. The equipment required to defeat this class of UAVs is relatively inexpensive to produce and operate and thus could be broadly deployed by law enforcement agencies, corporations, and individuals to protect critical infrastructure or commercial or residential sites with sufficient funding and risk analysis to justify counter-UAV systems.

Unfortunately, a major challenge prevents the United States and other western nations from deploying effective counter-UAV solutions – the techniques utilized by these solutions violate multiple federal laws and regulations. Further, even if the counter-UAV techniques were legal, there is no legal framework to enable defenders to determine that a UAV is malicious and then to engage it. The only legal action that can be taken against a UAV operator who flies outside of a very small number of restricted zones is a fine, if the operator can be located. Any action taken against a UAV is almost certainly subject to more serious criminal charges than faced by the operator of the UAV.

The larger problem is that there is no low cost, effective solutions to counter a UAV built and operated by a moderately technical determined adversary. For under \$4,000 an off the shelf

commercial UAV can be purchased that is capable of carrying a 2.2 lbs. payload for 100 minutes at 29 mph, giving it a 44-mile range. With a simple, well documented change to the software running on the onboard flight controller, the UAV will operate fully autonomously and with no radio frequency emissions. The flight controller can be programmed to operate a simple servo mechanism at a predetermined location or time, releasing the payload.

Such a UAV cannot be detected by radio frequency emissions and it has an extremely low radar cross section and acoustic signature. Flying at 300 feet above ground level, it is very hard to visually detect. Even if detected, it would be hard to neutralize. At that altitude and speed, firearms would be difficult to deploy effectively against it. Jamming the GPS signal could disable the GPS guidance but the UAV could be configured to continue to operate based on bearing and speed.

The United States is unprepared to counter the threats posed by consumer UAVs in the hands of non-state actors desiring to conduct terror attacks on domestic targets. Dual use technology ensures that the attackers will have sufficient capability to effect attacks using UAVs capable of evading or mitigating any reasonable counter-UAV solution. The United States legal environment that enshrines personal liberty and property rights along with criminal codes that prohibit the deployment of counter-UAV solutions prevents effective solutions from being deployed by all except a select few members of Federal agencies at very select sites.

## Further research

This paper briefly touched on the challenges facing anyone wishing to defend against consumer UAVs deployed against domestic targets by non-state actors. There is much more research that can be done on the topic, now and as technology, tactics, and laws evolve. Some possible future efforts include:

- Interview military staff, vendors, and others to explore offensive and defensive options which do not appear in open source literature
- Examine proposed regulatory changes to determine possible impact
- Explore other unmanned options, including fully autonomous robotics
- Get funding and support to conduct a demonstration exercise
- Investigate the impact of additive technology (3D printing) and other disruptive technologies

Also, this paper addressed our ability to domestically respond to UAVs operated by non-state actors domestically which doesn't allow for exploration of possible changes in the U.S. military's thinking based on UAV threats on the battlefield. The paper opened with Chinese references to Revolution in Military Affairs (RMA). "A Revolution in Military Affairs (RMA) is a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational

concepts, fundamentally alters the character and conduct of military operations."<sup>41</sup> Our military adversaries are embracing disruptive technologies with great success. This is not only forcing disruptive counter measures but it is also contributing to the U.S. military's consideration of using identical COTS UAV technology. We are in a period where major military forces are not just reacting to adversary's techniques, they are reacting to adversary's technologies and even adopting it. We are certainly entering an RMA period and this is worthy of further research.

Finally, international humanitarian agencies are exploring possible applications of UAVs to their work. When adversaries, the U.S. military, and aid agencies are all using the same platforms, how do all of the operators in the airspace identify unknown UAVs and react accordingly? Faine Greenwood and others at Harvard are doing interesting research on this topic.

---

<sup>41</sup> Stephen Biddle, "Assessing Theories of Future Warfare", Paper presented to the 1997 International Studies Association Annual Convention, Toronto, 19 March 1997

## Bibliography

- Singer, P. W. *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*. Penguin Press, 2009. <https://books.google.com/books?id=AJuowQmtbU4C>.
- "Unmanned Aircraft System Airspace Integration Plan." Department of Defense, March 2011. [http://www.acq.osd.mil/sts/docs/DoD\\_UAS\\_Airspace\\_Integ\\_Plan\\_v2\\_\(signed\).pdf](http://www.acq.osd.mil/sts/docs/DoD_UAS_Airspace_Integ_Plan_v2_(signed).pdf).
- "Drones Operating in Syria and Iraq." *Center for the Study of the Drone*, December 13, 2016. <http://dronecenter.bard.edu/drones-operating-in-syria-and-iraq/>.
- MailOnline, By John Hall for. "Latest ISIS Video Shows Drone View of Kobane's Battle-Ravaged Streets." *Mail Online*, December 12, 2014. <http://www.dailymail.co.uk/news/article-2871389/ISIS-propaganda-Call-Duty-style-Latest-footage-shows-drone-s-view-battle-ravaged-streets-Kobane-swooping-gun-battles-ground.html>.
- Bergen, Peter, and Emily Schneider. "Now ISIS Has Drones?(Opinion) - CNN.com." Accessed February 2, 2017. <http://www.cnn.com/2014/08/24/opinion/bergen-schneider-drones-isis/>.
- Weiss, Caleb. "Islamic State Uses Drones to Coordinate Fighting in Baiji." *FDD's Long War Journal*, April 17, 2015. <http://www.longwarjournal.org/archives/2015/04/islamic-state-uses-drones-to-coordinate-fighting-in-baiji.php>.
- Schmidt, Michael S., and Eric Schmitt. "Pentagon Confronts a New Threat From ISIS: Exploding Drones." *The New York Times*, October 11, 2016. <https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html>.
- "US Commander Hails Iraqi Forces Beating ISIS Drones and VBIEDs." *Rudaw*. Accessed February 7, 2017. <http://www.rudaw.net/english/middleeast/iraq/110120171>.
- "AK-47 and Other Guns on the Black Market - Havocscope." Accessed February 7, 2017. <http://www.havocscope.com/black-market-prices/ak-47/>.
- "السلام عليكم ورحمة الله وبركاته رسالة عاجلة الى الشخص الذي يدير طائرات الدولة الاسلامية... - Justpaste.it." Accessed February 7, 2017. <https://justpaste.it/jnabi7>.
- Bhattacharya, Ananya. "Colombia's Narcotics Smuggling Is Going Hi-Tech with Drone Deliveries." *Quartz*, November 19, 2016. <http://qz.com/841327/colombias-narcotics-smuggling-is-going-hi-tech-with-drone-deliveries/>.
- Kravets, David. "Man Lands Drone Carrying Radioactive Sand on Japanese Prime Minister's Office." *Ars Technica*, April 25, 2015. <https://arstechnica.com/tech-policy/2015/04/man-arrested-for-flying-drone-carrying-radioactive-sand-in-tokyo/>.
- Goure, Dan. "Drone Wars: Defeating the Unmanned Threat Will Require A Firestorm Of Energy." *The National Interest*. July 27, 2016. Accessed December 23, 2016. <http://nationalinterest.org/blog/the-buzz/drone-wars-defeating-the-unmanned-threat-will-require-17144>.
- Intelligence, B. I., 2016 Oct. 2, and 092 2. "THE DRONES REPORT: Market Forecasts, Regulatory Barriers, Top Vendors, and Leading Commercial Applications." *Business Insider*. Accessed February 15, 2017. <http://www.businessinsider.com/2016-10-2-uav-or-commercial-drone-market-forecast-2016-9>.

Gabriel Birch, John Griffin, and Matthew Erdman, "UAS Detection, Classification, and Neutralization: Market Survey 2015" (Sandia National Laboratories, 2015), <http://prod.sandia.gov/techlib/access-control.cgi/2015/156365.pdf>.

"FLIGHT ADVISORY NATIONAL SPECIAL SECURITY EVENT 2017 PRESIDENTIAL INAUGURATION FESTIVITIES" (Federal Aviation Administration, December 2016), [https://www.faa.gov/files/notices/2016/Dec/2017\\_Inauguration\\_Advisory.pdf](https://www.faa.gov/files/notices/2016/Dec/2017_Inauguration_Advisory.pdf).

Michael S. Schmidt and Michael D. Shear, "A Drone, Too Small for Radar to Detect, Rattles the White House," *The New York Times*, January 26, 2015, <https://www.nytimes.com/2015/01/27/us/white-house-drone.html>.

"Florida Mailman Lands a Gyrocopter on Capitol Lawn, Hoping to Send a Message," *Washington Post*, accessed January 30, 2017, [https://www.washingtonpost.com/local/florida-mailman-lands-a-gyrocopter-on-capitol-lawn-hoping-to-a-send-message/2015/04/15/3be11140-e39a-11e4-b510-962fcfab310\\_story.html](https://www.washingtonpost.com/local/florida-mailman-lands-a-gyrocopter-on-capitol-lawn-hoping-to-a-send-message/2015/04/15/3be11140-e39a-11e4-b510-962fcfab310_story.html).

Jeff Daniels, "Feds Turn up the Heat in Fight against Drones Interfering in Wildfires," *CNBC*, July 26, 2016, <http://www.cnbc.com/2016/07/26/feds-turn-up-the-heat-in-the-fight-against-drones-interfering-in-wildfires.html>.

"ORDINANCE NO. 2016-87" (The City Council of Orlando, Florida, December 7, 2016), [http://www.mynews13.com/content/dam/news/images/2017/01/4/Drone\\_UAS\\_Ordinance\\_-\\_12\\_7\\_2016.pdf](http://www.mynews13.com/content/dam/news/images/2017/01/4/Drone_UAS_Ordinance_-_12_7_2016.pdf).

"Definition of Larceny." Findlaw. Accessed February 09, 2017. <http://criminal.findlaw.com/criminal-charges/definition-of-larceny.html>.

"Jammer Enforcement," *Federal Communications Commission*, March 3, 2011, <https://www.fcc.gov/general/jammer-enforcement>.

"Counter-UAS Technologies," accessed February 19, 2017, <https://www.battelle.org/government-offerings/national-security/tactical-systems-vehicles/tactical-equipment/counter-UAS-technologies>.

Gabriel Birch, John Griffin, and Matthew Erdman, "UAS Detection, Classification, and Neutralization: Market Survey 2015" (Sandia National Laboratories, 2015), <http://prod.sandia.gov/techlib/access-control.cgi/2015/156365.pdf>.

Kate Conger, "How Consumer Drones Wind up in the Hands of ISIS Fighters," *TechCrunch*, accessed February 2, 2017, <http://social.techcrunch.com/2016/10/13/how-consumer-drones-wind-up-in-the-hands-of-isis-fighters/>.

"Chuck Schumer's No-Fly-Zone Rule for Drones Won't Work," *Defense One*, accessed February 12, 2017, <http://www.defenseone.com/technology/2015/08/chuck-schumer-no-fly-zone-drones/119389/>.

Kelsey Atherton, "Trained Police Eagles Attack Drones On Command," *Popular Science*, February 1, 2016, <http://www.popsci.com/eagles-attack-drones-at-police-command>.

David Morris, "A Drone, a Shotgun, and the Future of Airspace Rights," *Fortune*, September 25, 2016, <http://fortune.com/2016/09/25/drone-shotgun-airspace-rights/>.

Lauren Sigfusson, "Drone Pilot and FAA Comment on Drone Shooting at North Dakota Pipeline Protest | Drone360 Magazine," *drone360mag.com*, December 5, 2016, <http://drone360mag.com/news-notes/2016/10/drone-pilot-and-faa-comment-on-drone-shooting-at-north-dakota-pipeline-protest>

Oriana Pawlyk, "Air Force Zaps ISIS Drone with Electronic Weapon," *Defensetech*, October 24, 2016, <https://defensetech.org/2016/10/24/air-force-zaps-isis-drone-with-electronic-weapon/>.

Eric Schmitt, "Papers Offer a Peek at ISIS' Drones, Lethal and Largely Off-the-Shelf," *The New York Times*, January 31, 2017, <https://www.nytimes.com/2017/01/31/world/middleeast/isis-drone-documents.html>.

Samy Kamkar, "Samy Kamkar - SkyJack: Autonomous Drone Hacking," accessed February 13, 2017, <http://samy.pl/skyjack/>.

"Cellular Drone Communication," *Qualcomm*, August 31, 2016, <https://www.qualcomm.com/invention/technologies/lte/advanced-pro/cellular-drone-communication>.

"What Are the Aims of Medical Express?," *UAV Challenge*, September 23, 2016, <https://uavchallenge.org/2016/09/23/what-are-the-aims-of-medical-express/>.

"Canberra UAV Outback Challenge 2016 Debrief," *ArduPilot Discourse*, accessed February 19, 2017, <http://discuss.ardupilot.org/t/canberra-uav-outback-challenge-2016-debrief/12162>.

"Microsoft Drone Simulator Helps You Prevent Real-World Crashes," *Engadget*, accessed February 19, 2017, <https://www.engadget.com/2017/02/15/microsoft-drone-simulator/>.

Stephen Biddle, "Assessing Theories of Future Warfare", Paper presented to the 1997 International Studies Association Annual Convention, Toronto, 19 March 1997