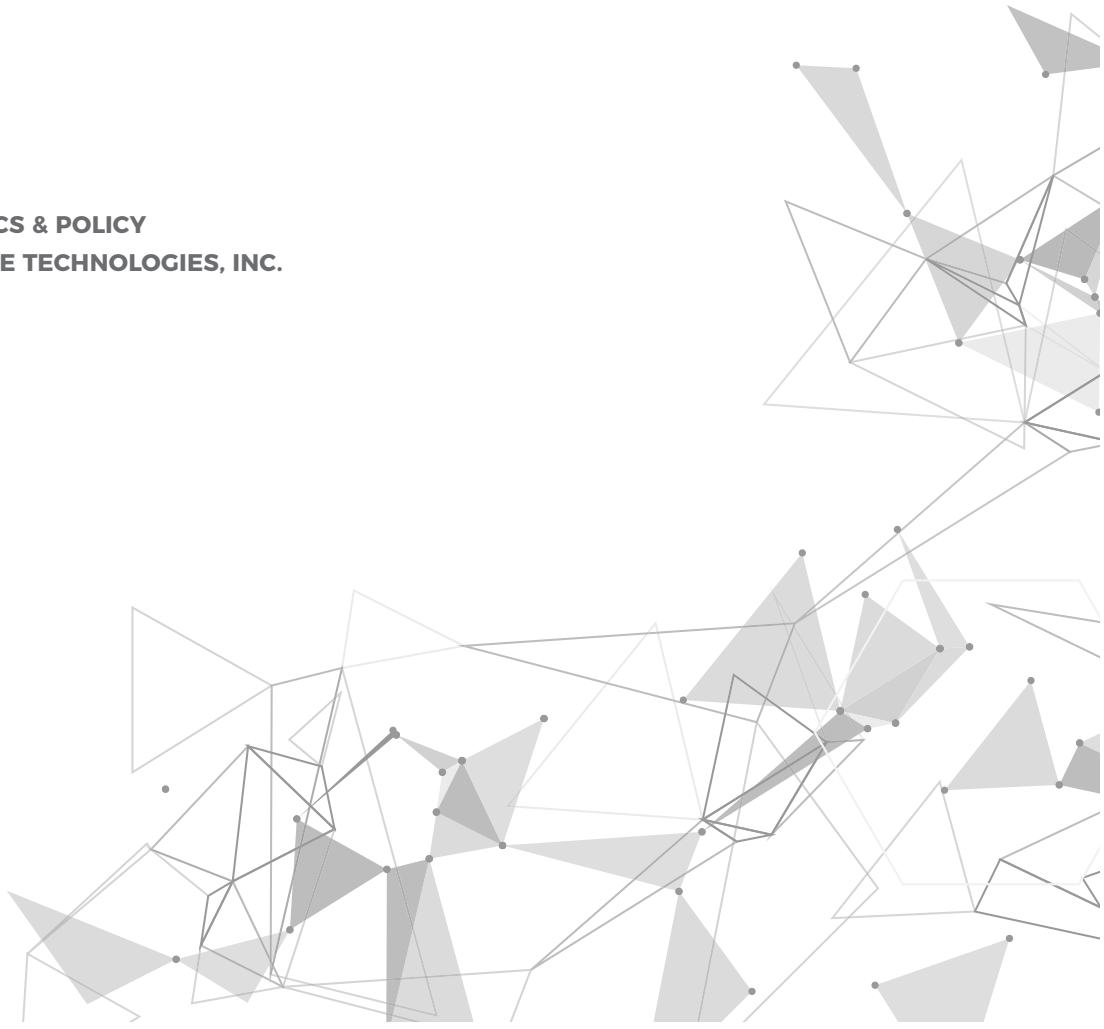
How to evaluate counter-drone products

DR. RYAN JENKINS
DIRECTOR OF ETHICS & POLICY
WHITEFOX DEFENSE TECHNOLOGIES, INC.



Introduction

KEY POINTS

- All counter-drone solutions have advantages, limitations, and drawbacks that must be considered based on the application.
- Counter-drone solutions must detect, identify and, when appropriate, mitigate hostile drone threats.

Drones are one of the most exciting technological platforms to arrive in a decade or more, promising benefits to agriculture, consumers, law enforcement, healthcare, and other sectors. But capitalizing on the benefits of drones requires enabling their positive uses while discouraging or preventing their dangerous ones. As drones are increasingly introduced and integrated into the national airspace, consumers, industry, and regulators agree that we need powerful, smart solutions to prevent potential harms from abuse and negligence.

This paper examines counter-drone solutions and suggests that a satisfactory solution is one that is **successful at detecting, identifying, and, if appropriate, mitigating a wide range of hostile drones with minimal human oversight**. This paper then evaluates the landscape of counter-drone technologies to examine their benefits and drawbacks. While no counter-drone solution is a silver bullet, this paper ultimately endorses **non-kinetic, low-power, "smart jamming"** counter-drone solutions as supreme.

Drones pose emerging threats in many different contexts. Perhaps the most spectacular threat is on the battlefield, where ISIS now almost daily threatens US and allied forces with "flying IEDs" [improvised explosive devices] (Vann, 2017). Drones already have dozens of near-collisions per year with aircraft at airports, "where such incidents are both most common and most dangerous" (Michel, 2018, p. 2). A single collision with a jetliner could be catastrophic, costing hundreds of lives. Drones are small and difficult to detect, which makes them an attractive choice to threaten VIPs or politicians (BBC, 2015). They can also be used to surveil or bring payloads into critical infrastructure like power plants (Hersh, 2015) or to help prisoners escape by smuggling in contraband (Hennigan, 2018). They have interfered with crucial firefighting efforts (Grossman, 2016) and harassed law enforcement in the line of duty (Murdock, 2018). In one alarming and revealing incident, a drone pilot on a "drunken lark" even crashed a drone onto the lawn of the White House (Shear & Schmidt, 2015).

But while solutions have proliferated at a dizzying speed[1], the Center for the Study of the Drone found that "there is a wide variance in the effectiveness and reliability of [counter-drone] systems" (Michel, 2018, p. 1). Reducing the harms from drones requires a multi-pronged response, including appropriate regulation and a cultural shift among drone pilots that enforces accountability. But a powerful technological component is also undoubtedly required as a last line of defense against hostile or negligent pilots. The best technological solution must allow an entity to detect, identify, and mitigate drones with a single, simple package.

1 The Center for the Study of the Drone measured an increase in counter-drone products from 10 in 2015 to over 230 in 2018 (Michel, 2018).

Components of a Satisfactory Counter-Drone Solution

KEY POINTS

- Counter-drone solutions must be powerful enough to detect and identify a wide range of hostile drones and intelligent enough to reliably separate friend from foe.
- Counter-drone solutions should operate with minimal human involvement and oversight, acting as a force multiplier for defense.
- Counter-drone solutions should be able to mitigate hostile drones when appropriate, considering relevant legal constraints and safety concerns. Some methods of drone mitigation are illegal, though some solutions are technically capable of mitigating drones today.

We can evaluate the *technical virtues* of a counter-drone solution by examining its purpose. Counter-drone solutions are adopted to detect, identify, and, when appropriate, mitigate drone threats.[2] Solutions are superior, then, to the extent they are powerful enough to detect, identify, and mitigate hostile drones.

Drones rely on many different modes of communication for navigation and control, including GPS, WiFi, and radio frequency (RF). Superior solutions will be effective against a wide range of drone threats.

But identifying drones also requires a delicate touch, nimble enough to separate friend from foe, and allowing its operators to intercept drones, when appropriate, in ways that protect people and property from harm. The solution should also avoid inflicting collateral damage to drones that are friendly or benign, such as those operated by civilians, law enforcement, or for commercial use. Moreover, it should be so capable of accomplishing this as to earn the trust of its operators, able to operate in semi- or fully autonomous modes, to function as a force multiplier for threat mitigation.

POWER: KEY POINTS

- A satisfactory counter-drone solution should allow its operator to detect and identify hostile drones with minimal human oversight.
- Counter-drone solutions should provide operators with a forensic threat assessment, including the drone's location, telemetry, make and model.

Counter-drone solutions should be **powerful**: they must be able to detect, identify, and mitigate hostile drones. A satisfactory solution would maximize true positives and minimize false negatives. It would do this with minimal human oversight and it would scale effectively against numerous or sophisticated threats, like drone swarms. Ideally, it would require only one portable device (or 'node') to accomplish all of these functions. A solution should allow for **arbitrary precision**, allowing the user to designate an arbitrary area to monitor and, if appropriate, defend against intrusion.

2 Operators who wish to mitigate drones should take note of relevant legal constraints and safety concerns.

A counter-drone solution should be **trustworthy** enough to require minimal human oversight. It should be reliable enough to function autonomously or semi-autonomously as a force multiplier.[3] Indeed, a satisfying solution would be reliable enough that its operator could "set it and forget it." Solutions that require their operators or manpower to scale along with the size of the threat are impractical for use against sophisticated adversaries.

All-in-one counter-drone solutions that allow the operator to detect, identify, and mitigate drones in one fell swoop are superior in their simplicity and integration. Combining multiple technologies for detection, identification, and mitigation introduces product interactions and potential points of failure.

To earn the trust of its human operator, a counter-drone solution should be **transparent and revelatory**. It should be able to identify the location and trajectory of the drone, i.e. it would be able to intercept and decipher its telemetry data. It should be able to decode UAS data, accurately identify drones, and make this information available to its operator. BlueForce, a drone technology consultant, calls this feature "intelligence" and identifies the following information as crucial to decode and display: make and model, speed and height, precise GPS location, and dynamic track (Fentiman & Domoney, 2017, p. 4).

3 The ideal counter-drone solution, in fact, would have a *practically infinite* range. But: such a system is prohibitively technically complex and conflicts with other values we hold dear by raising serious concerns about privacy.

PRECISION: KEY POINTS

- Counter-drone solutions should be able to distinguish friend from foe, so that friendly drones are unaffected.
- Counter-drone solutions should minimize collateral damage to authorized drones and harm to people from falling drones.

A second requirement of counter-drone solutions is **precision**: a satisfactory solution should **minimize collateral damage**. It must be able to distinguish between authorized uses of drones and unauthorized drone flights. For example:

> ...at a large sporting event, the airspace may be crowded with legitimate aerial cinematography drones that do not pose a security risk; an effective C-UAS [counter-unmanned aerial system] system must be able to tell the difference between those drones and a single rogue drone that is operating with malicious intent. (Michel, 2018, p. 6)

A satisfying counter-drone solution would not interfere with friendly or benign drones and would not interfere with authorized law enforcement or civilian activities. It would not endanger critical infrastructure or the performance of vital or emergency services.

BlueForce adds that the ideal solution would "effectively control the threat while not causing any interference to other drones or wireless communications devices in the area," including interference with other protocols like WiFi, BlueTooth, and GPS (Fentiman & Domoney, 2017, p. 4).

One way of minimizing collateral damage is to take control of and safely land a hostile drone and turn that control over to an operator. In theory, an ideal solution would minimize the potential for collateral damage by allowing an operator "to disconnect the original pilot controller from the drone and prevent reconnection; [and] allow an authorized operator to decide the safe course of action for a 'captured' drone" (Fentiman & Domoney, 2017, p. 4). In the

absence of being able to take control of and safely land a drone, the next best thing is to initiate the drone's failsafe mode. While this is valuable for area denial, it is not a perfect solution for drone mitigation. All parties who have a stake in sophisticated counter-drone solutions await a change in the regulatory landscape to be able to more effectively neutralize hostile drones.

Counter-drone solutions should also be attractive in their physical specifications. They are superior to the extent they are small and light enough to be mobile, affordable, and with a long-lasting power source.

KEY POINTS

- Counter-drone solutions should be able to disrupt a wide range of hostile drones, distinguish friend from foe, and minimize collateral damage.
- Counter-drone solutions should be powerful enough to act as a force multiplier against sophisticated threats, and they should be able to do all this in a portable, lightweight, long-lasting design.

Solutions for Drone Detection and Identification

KEY POINTS

- Drone detection and identification technologies offer a range of benefits and costs, and no single solution can detect and identify all drone models.
- Omnidirectional RF detection offers the best profile in terms of power, precision, and manpower required to operate successfully.

The naked eye. Many times an operator can simply *see* a drone threat without needing any assistance from technology. The unassisted naked eye, while attractive for its affordability and wide availability, is nonetheless an unsatisfying solution. Beyond close ranges of just a few hundred feet, the eye becomes unreliable. Operators require special training to distinguish friend from foe at a distance — or even to distinguish a drone from a bird — and using sight to identify drones does not scale effectively against sophisticated threats. As BlueForce says, "for longer range detections and for areas not conducive to physical 24-hour surveillance, RF detectors and RADAR are needed" (Fentiman & Domoney, 2017, p. 2).

Notice these weaknesses also undermine any drone mitigation solution that relies on the naked eye, including many kinetic solutions and jammer guns discussed below.

Radio frequency direction finding. Some products are able to identify the location and telemetry of a drone by intercepting its radio frequency (RF) signal. While drones can conceivably be modified to cease broadcasting RF signals, for the time being, nearly all drones rely on RF signals for communication with a controller. However, RF direction finding products can require multiple nodes to successfully triangulate the location of a drone and can "suffer from inaccuracies caused by signal reflections" (Fentiman & Domoney, 2017, p. 2). Only the most sophisticated RF counter-drone systems can operate with a single-node, requiring omnidirectional RF detection.

RADAR. Radar is an initially enticing technology for its wide availability and integration into other area denial and defense systems. Radar systems can detect objects from several kilometers away and can also help the operator infer telemetry data for these objects. However, radar is not a complete standalone counter-drone solution: radar systems have difficulty classifying targets, e.g. distinguishing birds from drones, and must be paired with another technology to identify the make and model of a drone (iHLS, 2018). Radars that are calibrated to be sensitive to small objects will risk returning so many false positives that operators become desensitized or frustrated.

Moreover, drones are small, comparatively slow, and low-flying, whereas "military anti-aircraft radars are mostly designed to detect large, fast moving objects" (Michel, 2018, p. 2). Thus, radar systems can be expected to struggle significantly against continuing advances in the miniaturization of drones (iHLS, 2018).

Combined sensors. Some technologies combine multiple sensors, such as optical sensors (i.e. cameras), infrared, and acoustic detectors. The rationale behind these approaches is that drones have characteristic signatures — appearances or

sounds — that can be detected and classified by a suite of connected technologies. Ultimately, though, all sensors have drawbacks. For example, optical sensors suffer from many of the same drawbacks as the naked eye: they can only operate during the daytime when drones are visible and they must have a line of sight to the target.

Moreover, these solutions rely on a library of known drone signatures, which must be continually updated to stay current as new models are released onto the market. This cat-and-mouse game is a challenge for many counter-drone approaches. These approaches, especially, seem doomed to stay one step behind malicious actors who need only tweak their drones slightly to avoid detection by sight or sound. The hope in combining sensors is that the various detectors will counterbalance the weaknesses and gaps in one another. Instead, the opposite often happens and the operator is left to interpret multiple sensors giving conflicting reports or false positives.

Solutions for Drone Mitigation

Once a drone has been detected and classified as a threat, it remains to mitigate or neutralize the drone. A wide variety of products exist for mitigating drones, but they can be grouped into two general categories: **kinetic** and **non-kinetic**. Kinetic solutions use physical force to neutralize a drone — often called a "hard kill" in which drones are damaged, destroyed, or rendered inoperable. Non-kinetic solutions are able to mitigate drones without directly damaging the drone, typically by intercepting or interfering with the communications signals that drones rely on for guidance and control.

KINETIC OPTIONS: KEY POINTS

- Kinetic counter-drone solutions rely on physically damaging or interfering with drones, scaling one-to-one against drone threats. They are extremely challenging to execute because drones are small and nimble.
- Kinetic counter-drone solutions cause significant collateral damage when missing a drone or when damaged or disabled drones fall from the sky.

Kinetic counter-drone products attempt to mitigate a drone by physically damaging or interfering with that drone. A principle advantage of kinetic mitigation solutions is that they work against drones that have been modified not to broadcast RF, WiFi, or other common protocols (though these threats are very rare).

However, the prime attraction of drones is that they are small, fast, and agile, which means that kinetic mitigation methods are inherently challenging. The legendary slugger Ted Williams said that hitting a baseball is "the single most difficult thing to do in sport" — and this is not surprising given that the goal is to hit something very small and fast-moving with something else relatively small (Bowen, 2011). Kinetic counter-drone solutions attempt something similar.

Kinetic weapons pose a significant risk of collateral damage. Because they knock a drone from the sky, they often render it inoperable and uncontrollable.[4] Thus, using a kinetic counter-drone solution in a heavily populated area, like during a concert or a sporting event, risks injuring innocent people.

Finally, many kinetic options fail to scale effectively against threats. Instead, many of them scale *linearly*, in a one-to-one relationship. Since, by nature, each drone threat needs to be met and physically intercepted, and since physical objects can only be in one place at a time, you would need as many of these interceptors as there are threats. For every hostile drone, you need another eagle, net, or counter-drone drone. It is hard to take seriously the suggestion to use solutions like eagles to protect critical infrastructure or other sensitive targets that could be harassed by dozens or hundreds of drones in a near-future sophisticated attack.

Counter-drone drones. Some companies suggest that the best solution to a bad guy with a drone is a good guy with a drone. Accordingly, they have used their own drones with claws or nets to down hostile drones. The weakness of these approaches is that they scale one-to-one with drone threats. And, at several hundred dollars per drone, amassing an

4 There are exceptions to this, including kinetic solutions that maintain control over a drone. Some companies are developing drones that will capture a hostile drone with a net or claw, presumably maintaining control of the hostile drone. Using eagles as a counter-drone weapon may accomplish the same thing. But these solutions still have considerable drawbacks, as are discussed in this paper.

army of counter-drone drones to defeat a swarm or sophisticated threat quickly becomes exorbitant.

Another clear problem with such solutions is that they could result in collateral damage by undermining public safety. If a drone is disrupting emergency services or firefighting operations, for example, then tracking and intercepting it with an *additional* drone exacerbates the problem.

Eagles. Some companies have made headlines by training eagles — natural predators — to intercept drones. But there are many problems with this approach. Eagles can be seriously harmed by trying to capture a drone with their talons, and some malicious actors have attached razors to the blades of their drones to mangle the birds further. Using these animals for such dangerous operations, then, puts their wellbeing at risk, even if it makes for a sensational picture. It also presents a challenge to train eagles or other birds of prey to tell apart friendly from hostile drones, which would be necessary during a chaotic scenario involving many friendly and hostile drones.

Nets or net-guns. Some companies have deployed nets to intercept hostile drones. This improves over other solutions by increasing their area of effect, i.e. it is easier to catch a drone with a large net than it is to catch it with another drone. Still, a reliable implementation of this approach is elusive. Though nets have a wide area of effect, drones are small and agile, and they are notoriously difficult to hit. It is extraordinarily difficult to catch a drone with a net-gun, even from a close distance — and at hundreds of feet away, this becomes practically impossible.

Projectiles. Projectiles are objects fired at a drone to try to destroy it. They can be guided projectiles, like missiles, or unguided, like bullets. Some countries have successfully demonstrated the use of missiles to annihilate hostile drones. One recent example includes Israel firing a Patriot missile at a hostile drone (Hawkins, 2017). While this solution may be effective, it is also prohibitively expensive: a Hellfire missile costs around $115,000 and a Patriot missile costs a remarkable $3 million — meaning that it costs several thousand times as much as a typical off-the-shelf drone (Osborne, 2012; Michel, 2018; Hawkins, 2017).[5] The cost proposition, then, of using missiles to down cheap and nimble drones is unrealistic. Moreover, it goes without saying that few have access to these weapons and that they are out of the question as a counter-drone solution to safeguard public areas or critical infrastructure.

Militaries have also experimented with using machine guns to counter hostile drones. But this turns out to be extraordinarily difficult. Hitting a small object traveling 50 miles per hour with a smaller object traveling hundreds of feet per second is enough of a challenge that, in one demonstration, seventy gunners firing fully automatic machine guns at once could not down a single drone a few hundred feet away (National Geographic, 2017).

Lasers. Militaries have also demonstrated the ability to down a drone with a high-powered laser, using directed energy to destroy critical parts of the drone and cause it to crash. (Lasers can be considered kinetic mitigation options because they directly damage or destroy a drone.) But because they fire in a straight line, lasers can only take out drones in a line of sight. They also take tremendous power to operate — as such they are relatively immobile. They are also a one-to-one solution, since a laser can only fire at one drone at a time. Finally, like many kinetic solutions, once a laser has destroyed a drone, it simply falls from the sky, endangering whatever might be below it, including sensitive infrastructure or innocent people.

---

5 What's more, even these sophisticated traditional systems have been unsuccessful at bringing down drones: "in July 2016, a simple Russian-made fixed wing drone that flew into Israeli airspace from Syria survived two Patriot missile intercepts, as well as an air-to-air missile attack from an Israeli fighter jet" (Michel, 2018, p. 2). The cost of this failed interception must have totaled several million dollars.

NON-KINETIC SOLUTIONS: KEY POINTS

- Jamming counter-drone solutions risk collateral damage and interfering with critical communications.
- "Spoofing," a non-jamming counter-drone approach, allows an operator to take control of and safely land a hostile drone, which can be done with minimal risk of collateral damage.
- The promise of smart jamming and spoofing underscores the need for clarified regulation to enable authorized parties to defend critical assets and public safety.

Non-kinetic solutions are divided into **jamming** and **non-jamming** approaches.

Jammers. Jammers are devices that interfere with the communications link that drones rely on for navigation or control, including RF, GPS, or WiFi.[6] As a result of being jammed, drones may fall from the sky or else enter a pre-determined "failsafe" mode. Jammers improve over kinetic counter-drone technologies because the operator does not need to get close to the drone or make physical contact with it to jam its communications. Though jammers are the most common method to mitigate drones, they are still far from a satisfying solution (Michel, 2018, p. 5).

Perhaps most significantly, manufacturers are beginning to include anti-jamming technology in newer drones. As a result, many jammers are powerless against the most recent models of drones. But even when jammers are able to disrupt a drone's communications, they have serious drawbacks.

Jamming approaches fall short in terms of both power and precision. It is a challenge to use jammers effectively in order to halt hostile drone threats. Directional jammers, like jamming "guns," provide a spread of about 30° within which the jammer is effective. They require significant human involvement to mitigate the hostile drones in an area — and one at a time. These jammers also operate only temporarily, they have to be pointed in the right direction, they have to overpower the drone controller's signal, and they must transmit continuously. Jamming a signal is a challenging and delicate operation.

Jammers also cause collateral interference with other communications. They can be calibrated to different frequencies and power levels to try to avoid this problem. However, "In practice, when a drone is moving at up to 60 km/hr [37 mph], an operator doesn't have time to determine what power might be required or which band it might be operating on, so maximum power and multiple frequency bands are often used when it is deployed" (Fentiman & Domoney, 2017, p. 7).

The incentive is often to adopt what are called "barrage jammers," which jam communications at a high power output and over a wide range of frequencies. These solutions operate one-to-many and could successfully jam several drones at once. Ironically, though, these jammers are often *too* powerful: they threaten to disrupt civilian and law enforcement frequencies, RF, WiFi, BlueTooth, and consumer GPS receivers in the area.[7]

Newer and more advanced **"precision jammers"** or **"smart jammers"** can reduce collateral damage by

6 The majority of drones rely on some method of wireless communication for navigation or control. Still, "many drones can be programmed to operate autonomously without an active RF link. There is also active research to develop drones that can operate in GPS-denied environments" (Michel, 2018, p. 7).

7 "Collateral interference is an acceptable risk when broadband jammers are used to prevent the remote detonation of IEDs, but given the wide range of drone threats, the regularity of incursions into restricted airspace and our increasingly widespread reliance on wireless technology (both by civilians and law enforcement), they are not the best choice in many cases" (Fentiman & Domoney, 2017, p. 3).

narrowly targeting a range of RF frequencies and operating at low power. Still, these solutions have the aforementioned problems, e.g. having to transmit continuously and having to overpower the drone's controller signal. Still, these solutions improve significantly over many of those mentioned above.

Spoofing. A final solution worth considering is communications interception. These technologies can disrupt the signal from a controller to a drone, then "clone" that signal to *impersonate the drone's controller*, and gain control of the hostile drone.

These counter-drone technologies are exceedingly powerful, able to detect and identify multiple drones at once, with a single node, and with minimal human oversight. They do not require line of sight, can operate 24/7, and do not require physically intercepting a drone. They truly act as a force multiplier for area denial.

These counter-drone technologies also create no collateral damage. They can be operated according to white-lists, which prohibit all drones *except* for a list of known drones, or according to black-lists, which identify specific drones to mitigate. They therefore do not interfere with other civilian, law enforcement, or critical communications in an area. They are a precision tool akin to a scalpel, whereas a comparatively indiscriminate jammer could be compared to a chainsaw.

As we continue to integrate friendly drones into the airspace, a narrowly tailored drone solution, powerful enough to counter hostile threats, but intelligent enough to avoid collateral damage to friendly drones or innocent people, is required. "Spoofing" technology boasts numerous advantages. These technologies are far away the safest and "cleanest" counter-drone solutions. And they are the most impressive force multiplier, in terms of **power** and **precision**, that can be operated with minimum human oversight.[8] Some solutions are technically capable of mitigating drones today, and merely await new regulations to unlock their full potential.

- Smart jamming and spoofing are ideal counter-drone solutions for most threats and environments.

8 See, once again, BlueForce: "Precision jamming technologies allow the countermeasures operator permanent control of a drone threat and the choice of automated or manual options to force a landing at the drone's current location or in a predetermined safe zone. The drone can also be disabled and dropped immediately… While precision and targeted jammers are technically still included under the broad definition of jamming devices, there are numerous reasons, outlined above, that clearly demonstrate these tools to be a safer and "cleaner" technology" (Fentiman & Domoney, 2017, p. 9).

Conclusion

No counter-drone solution is perfect, though some of them boast undeniable advantages: they are powerful enough to detect and identify hostile drones, they are precise enough to tell friend from foe, and they are nimble enough to avoid collateral damage to civilian or critical communications.

- A fully satisfying counter-drone solution will likely involve a suite of reinforcing tools for detecting, identifying, and, when appropriate, mitigating a wide range of drone threats and will scale effectively against sophisticated threats like swarms.

It is worth reiterating, in closing, that **a technology to detect, identify, and mitigate drones is only one component of a comprehensive and mutually reinforcing set of technology, regulation, and responsible drone culture**. Integrating drones gracefully into the national airspace requires a positive regulatory component as well: a UAS traffic management (UTM) system that is currently being explored by the FAA.[9]

It is our position that these systems must thread a needle carefully through the intersecting concerns of the public and law enforcement (Jenkins, DeBruhl, & Fox, 2017). They must provide peace of mind, privacy, and ease of use for the public, balanced against real security for parties with a legitimate interest in accessing sensitive data such as a drone operator's identity. They must be cryptographically secure and required to operate a drone, much in the same way that license plates provide a token to identify the driver of a car, inscrutable to citizens in order to maintain privacy, yet assisting law enforcement by deterring or identifying bad actors.

We eagerly and optimistically await regulatory progress to enable the bright future of responsible drone operations and catalyze the benefits that would follow.

9 "An alternate form of 'counter-drone' technology is known as electronic identification, which allows one to remotely access information such as the exact location, model type, operator name, and registration number of drones operating in the vicinity. This information could be used to establish whether a drone presents an immediate threat, something that traditional C-UAS systems cannot do" (Michel, 2018, p. 7).

Works Cited

BBC. (2015, April 25). *Japan radioactive drone: Tokyo police arrest man*. Retrieved from BBC: https://www.bbc.com/news/world-asia-32465624

Bowen, F. (2011, January 19). *What's the toughest feat in sports?* Retrieved from Washington Post: http://www.washingtonpost.com/wp-dyn/content/article/2011/01/19/AR2011011906160.html

Fentiman, B., & Domoney, F. (2017, January 1). *Counter Small Unmanned Aircraft Systems (C-sUAS) Emerging Technical Solutions White Paper.* BlueForce UAV Consulting Inc.

Grossman, D. (2016, December 2). *How Aviation Became Firefighters' Best Friend—And Then Their Worst Enemy*. Retrieved from Popular Mechanics: https://www.popularmechanics.com/flight/drones/a24109/fighting-fires-and-flying-drones-a-growing-danger/

Hawkins, D. (2017, March 17). *A U.S. 'ally' fired a $3 million Patriot missile at a $200 drone. Spoiler: The missile won.* Retrieved from Washington Post: https://www.washingtonpost.com/news/morning-mix/wp/2017/03/17/a-u-s-ally-fired-a-3-million-patriot-missile-at-a-200-drone-spoiler-the-missile-won/

Hennigan, W. J. (2018, May 31). *Experts Say Drones Pose a National Security Threat — and We Aren't Ready*. Retrieved from TIME Magazine: http://time.com/5295586/drones-threat/

Hersh, M. (2015, January 30). *Commentary: Drone Threat to Nuclear Plants* . Retrieved from DefenseNews: https://www.defensenews.com/opinion/commentary/2015/01/30/commentary-drone-threat-to-nuclear-plants/

iHLS. (2018, May 30). *First Untethered Insect-Sized Flying Robot Developed* . Retrieved from iHLS: https://i-hls.com/archives/83234?mc_cid=33a339d209&mc_eid=%5BUNIQID%5D

iHLS. (2018, June 1). *Radars Will Not be Able to Tell Bird-Like Drone from Real Birds*. Retrieved from iHLS: https://i-hls.com/archives/83291?mc_cid=33a339d209&mc_eid=%5BUNIQID%5D

Jenkins, R., DeBruhl, B., & Fox, L. (2017). *UAS Traffic Management: Recommendations for Seamless Integration*. WhiteFox Defense Technologies.

Michel, A. H. (2018). *Counter-Drone Systems.* Center for the Study of the Drone.

Murdock, J. (2018, May 4). *'Drone swarm' used by criminals to disrupt an FBI hostage rescue operation*. Retrieved from Newsweek: http://www.newsweek.com/drone-swarm-used-criminals-disrupt-fbi-hostage-rescue-operation-910431

National Geographic. (2017). *Game of Drones*. Retrieved from Vimeo: https://vimeo.com/234884331

Osborne, C. (2012, October 4). *How much do smart weapons cost the military?* . Retrieved from ZDNet: https://www.zdnet.com/article/how-much-do-smart-weapons-cost-the-military/

Shear, M., & Schmidt, M. (2015, January 27). *White House Drone Crash Described as a U.S. Worker's Drunken Lark*. Retrieved from New York Times: https://www.nytimes.com/2015/01/28/us/white-house-drone.html

Vann, M. (2017, January 19). *Trump Inauguration Spotlights New Ways to Protect Crowds From Attack Drones*. Retrieved from NBC News: https://www.nbcnews.com/mach/features/trump-inauguration-spotlights-new-ways-protect-crowds-deadly-attack-drones-n708646

Zhou, L. (2018, June 18). *Chinese navy deploys drones in South China Sea missile drills*. Retrieved from South China Morning Post: http://www.scmp.com/news/china/diplomacy-defence/article/2150957/chinese-navy-deploys-drones-south-china-sea-missile