

# **COUNTER-DRONE SYSTEMS**

# 2nd Edition

# ARTHUR HOLLAND MICHEL



#### ABOUT THE CENTER FOR THE STUDY OF THE DRONE

The Center for the Study of the Drone at Bard College is an interdisciplinary research institution that examines the novel and complex opportunities and challenges presented by unmanned systems technologies in both the military and civilian sphere. By conducting original, in-depth, and inquiry-driven projects, we seek to furnish stakeholders, policy-makers, and the public with the resources to engage in a robust public debate and develop policies that best address those opportunities and challenges.

#### **ACKNOWLEDGEMENTS**

Dan Gettinger edited this publication and assisted with the development of the database. Isabel Polletta and Ariana Podesta provided editorial support. Aasiyah Ali, Lynn Barnett, Dylan Sparks, Josh Kim, John McKeon, and Lilian O'Donnell provided research support. Layout by Dan Gettinger.

Michael Blades, Vice President for Research and Consulting, Americas Region, Frost & Sullivan, provided assistance in the development of this database. Frost & Sullivan's market report on C-UAS technology is available for purchase at: <u>https://store.frost.com/global-counter-uas-market-forecast-to-2024.html</u>

The project was made possible by the Peace Research Institute Oslo under its program "Counter-Drone Systems: Implications for Norway in an EU and NATO context," which is funded by the Norwegian Ministry of Defense, as well as by general operating support provided by the Open Society Foundations.

Cover photos by Pvt. James Newsome and Senior Airman Kaylee Dubois.

Copyright © 2019 Center for the Study of the Drone at Bard College

## **OVERVIEW**

Counter-drone technology, also known as counter-UAS, C-UAS, or counter-UAV technology, refers to systems that are used to detect and/or disable unmanned aircraft. As concerns mount around the potential security threats drones may pose to both civilian and military entities, a new market for counter-drone technology is rapidly emerging. This second edition of "Counter-Drone Systems" provides background on the growing demand for C-UAS technology, describes how the technology works, presents our database of known C-UAS products from around the globe, and explains some of the challenges surrounding counter-drone technology use.

This report is based on open-source research of technical and policy reports, written testimony, news and analysis pieces, and manufacturer information; background interviews with government and law enforcement officials, industry representatives, and subject matter experts; and participation in both public and closed conferences and workshops.

# BACKGROUND

The rise of C-UAS technology is largely tied to the novel threats posed by the expanding use of dronesparticularly small, inexpensive systems-in civilian and wartime environments. In the military domain, small drones have been proliferating at a rate that has alarmed battlefield commanders and planners alike. According to our September 2019 report The Drone Databook, at least 95 countries now possess drones,<sup>1</sup> which can potentially furnish even poorly funded state actors with an aerial command of the battlespace that was previously only available to those possessing a sophisticated aircraft program. Drones are also increasingly becoming a weapon of choice for non-state groups that employ the technology for surveillance, battlespace management, propaganda, and aerial strike attacks, often to considerable effect (see insert on page 8). As a result of the proliferation of this technology, which is set to continue apace in the years ahead, counter-drone systems will become a ubiquitous weapon in all future conflicts.

In the civilian domain counter-drone systems are likewise set to figure as an important tool for security and law enforcement, as unmanned aircraft are increasingly being put to a variety of nefarious purposes. With relatively simple modifications it is possible, for example, to convert cheap "off-the-shelf" consumer drones and hobby kit aircraft into rudimentary yet potentially lethal guided missiles or other airborne attack systems—so much so that it has become common for security and law enforcement professionals who track the issue to characterize the possibility of a lethal drone attack in the U.S. or Europe as being not so much a matter of "if," but "when." Other dangerous and/or criminal uses of drones abound (see insert on page 9), which intensifies the demand for effective methods to detect rogue unmanned systems and, if necessary, bring them down.

The air defense systems that have traditionally been used to protect airspace are mostly designed with inhabited aircraft in mind—that is, they are optimized for detecting, tracking, and shooting down large fast-moving objects. As a result, they cannot always pick up small, slow, low-flying drones.\* Even formidable air defense systems have sometimes failed to bring down rudimentary unmanned aircraft; 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 attack from an Israeli fighter jet.<sup>2</sup> In civilian airspace, drones aren't yet required to carry transponders, so they cannot be detected and tracked with existing air traffic control systems. Relying on visual observation to detect drones is equally ineffective; at a distance of several hundred feet, drones can become all but invisible to the naked eye.

In light of the proliferation of unmanned aircraft that operate precisely within this gap in modern military and security defenses, the market for fit-for-purpose counter-drone systems is booming. In a market survey conducted in 2015, researchers at the Sandia National Laboratories identified a dozen dedicated counter-drone systems available for acquisition.<sup>3</sup> Today, less than five years later, we have tallied as many as 537 systems on the market. In that interim, the technology itself has also advanced considerably and the knowledge-base for how to employ it has matured. However, significant challenges remain unsolved.

<sup>\*</sup> Even though the emergence of low-flying small unmanned aircraft poses a new challenge that cannot fully be addressed with existing air defenses alone, many legacy air defense and electronic warfare weapons do figure as a component of a "layered" approach to C-UAS that many established militaries appear to be adopting. Furthermore, many dedicated counter-drone products are based on existing air defense technologies, particularly radar and counter-mortar systems.

# **C-UAS 101**

*C*-*UAS systems rely on a variety of techniques for detecting and/or intercepting drones. This section describes the main detection and interdiction methods employed by products currently available on the market, as well as the principal platform types* 

### Detection, Tracking and Identification

Radar	Detects the presence of small unmanned aircraft by their radar signature, which is generated when the aircraft encounters radio frequency pulses emitted by the detection element. These systems often employ algorithms to distinguish between drones and other small, low-flying objects, such as birds.
Radio-frequency (RF)	Detects, locates, and in some cases identifies nearby drones by scanning for the frequencies on which most drones are known to operate.
Electro-optical (EO)	Identifies and tracks drones based on their visual signature.
Infrared (IR)	Identifies and tracks drones based on their heat signature.
Acoustic	Detects drones by recognizing the unique sounds produced by their motors. Acoustic systems rely on a library of sounds produced by known drones, which are then matched to sounds detected in the operating environment.
Combined Sensors	Many systems integrate a variety of different sensor types in order to provide a more robust detection, tracking, and identification capability.



From left to right: examples of handheld, mobile, and UAV-based counter-drone systems. (See "Platform Types" on the following page. Photos by Cpl. Brian R. Domzalski, Sgt. Devon Bistarkey, and Wesley Farnsworth

### Interdiction

RF Jamming	Disrupts the radio frequency link between the drone and its operator by generating large volumes of RF interference. Once the RF link, which can include WiFi links, is severed, a drone will usually either descend to the ground or initiate a "return to home" maneuver.
GNSS Jamming	Disrupts the drone's satellite link, such as GPS or GLONASS, which is used for navi- gation. Drones that lose their satellite link will usually hover in place, land, or return to home.
Spoofing	Allows one to take control of or misdirect the targeted drone by feeding it a spurious communications or navigation link. (For our purposes, we include within this category a range of measures such as cyber attacks, protocol manipulation, and RF/GNSS Deception).
Dazzling	Employs a high-intensity light beam or laser to "blind" the camera on a drone.
Laser	Destroys vital segments of the drone's airframe using directed energy, causing it to crash to the ground.
High Power Microwave	Directs pulses of high intensity microwave energy at the drone, disabling the aircraft's electronic systems.
Nets	Designed to entangle the targeted drone and/or its rotors.
Projectile	Employs regular or custom-designed ammunition to destroy incoming unmanned air- craft.
Collision Drone	A drone designed to collide with the adversary drone.
Combined Interdiction Elements	A number of C-UAS systems also employ a combination of interdiction elements to increase the likelihood of a successful interdiction. For example, many jamming systems have both RF jamming and GNSS jamming capabilities in the same package. Other systems might employ an electronic system as a first line of defense and a kinetic system as a backup measure.

### Platform Types

Ground-based: Fixed	Systems designed to be used from either stationary positions on the ground.
Ground-based: Mobile	Systems that are designed to be mounted on vehicles and/or operated on the move.
Hand-held	Systems that are designed to be operated by a single individual by hand. Many of these systems resemble rifles or other small arms.
UAV-based	Systems designed to be mounted on drones.

Counter-drone technology can serve in a wide variety of roles. In wartime, militaries are adopting C-UAS for protecting bases, naval vessels, convoys, and ground units. In civilian environments, counter-drone technology is primarily used for securing the airspace around critical infrastructure, sensitive facilities, and large events such as party conventions and sports games, as well as for protecting VIPs and countering airborne smuggling at prisons.<sup>4</sup> Increasingly, the technology is also being adopted for private use. In any of these contexts, countering a drone is a complex multi-step process involving interaction between several distinct systems and between those systems and the human operator(s).

- 1. First, a sensor system must detect, identify, locate, and track the incoming drone. Depending on the type of system used, a sensor that makes an initial detection, such as a wide-area radar or an RF detector, may have to "cross-cue" to secondary sensors such as cameras or electronic identification elements to confirm that the detected object is in fact a drone, as well as determine its precise location and track its movements. Secondary sensors may also serve to provide additional information about the drone, which may help determine intent. For example, a camera may be able to show whether a drone appears to be carrying explosives. Certain electronic sensors may be able to additionally identify the location of the drone operator. Sensor data can often be stored for later use as evidence.
- 2. Based on the information from these sensors, a human operator must decide how to respond to the incoming drone. This may not always involve activating an interdiction system. For example, a federal law enforcement team operating a C-UAS system with mitigation capabilities at the 2019 Super Bowl found that they could usually just locate the operator of the drone and ask them to cease flying in the area.<sup>5</sup> Particularly in civilian environments, C-UAS operators often describe mitigation as a "last resort" measure. C-UAS teams may have a very limited window of time to make this decision.

- 3. A mitigation system is activated and the drone is intercepted. Depending on the technique used, this could result in a range of effects, including the drone landing on the ground or activating a "return to home" mode (in the case of jamming or spoofing), the capture of the drone (nets), or the complete or partial destruction of the drone (lasers, projectiles, collision UAVs, high powered microwaves).
- 4. Depending on the circumstances, once a drone is intercepted the device may need to be isolated and retrieved. If the drone is potentially armed, an explosive ordnance disposal team may be called in to assess and, if needed, disable the device. Unarmed drones must likewise be treated with caution. If the device is damaged, its lithium-ion battery poses a risk of combustion. If the device continues to be functional, its rotors can pose a risk of injury. Those wishing to perform forensic analysis on the device may need to follow a series of steps to ensure that the integrity of the system and the potentially valuable data it carries are not compromised.



Photo by Capt. Jason Welch

# **DATABASE OF PRODUCTS**

To better grasp the scale and form of the counter-drone market, we have assembled a database of publicly marketed counter-drone systems. The database consists of 537 products sold by 277 firms and partnerships from 38 different countries.

This database was built through open-source research of news stories, marketing materials and brochures, press releases, and other publicly available information. It includes a small number of systems that are still in active development, as well as existing products designed for other purposes that have been retooled and/or specifically marketed for C-UAS. *The full database can be found on page 18*.

### Key Analysis Points

- With 537 systems, this database is considerably larger than our original database, published with the first edition of "Counter-Drone Systems" in February 2018, which contained 235 products from 155 manufacturers in 33 countries. This difference does not represent absolute growth in the sector: Twenty-four products and 9 manufacturers were removed from our original database because they no longer appear to be active, while a small number of products in our new database appear to have already been on the market before February 2018.
- One hundred and seventy five of the products in the database are designed only for detection, while 214 systems are designed only for interdiction.
- At least 138 systems are advertised as being capable of both detection and interdiction, while 10 systems can be equipped with an optional interdiction element.
- A majority of the systems, 375 in total, are designed for ground-based use; of these, 260 are fixed systems, 55 are mobile, and 59 are undefined or platform agnostic. One hundred and six systems are handheld and 34 systems are mounted aboard a drone. Twelve products consist of a combination of ground-based elements and either a handheld device or a UAV.
- Of the 323 systems that are capable of detection, 190 appear to employ a single sensor type, while at least

133 employ a combination of one or more sensor types (we count EO and IR sensors as distinct detection elements, though the two are more often than not used in conjunction). Forty two systems employ a combination of four or five different sensor types.

- RF and radar are the most common detection elements, appearing in 159 and 147 systems respectively. EO and IR systems, which are usually used in conjunction, appear in 113 and 111 systems, respectively. Acoustic sensors are used in 34 products. (In a small number of products, some of these detection elements may be optional).
- Of the 362 systems capable of interdiction, 147 rely on a single technique and 215 rely on two or more techniques (we count RF and GNSS jamming systems as distinct, even though the two are more often than not used in conjunction).
- Jamming (both RF and GNSS) is the most common interdiction method—259 systems employ some form of signal jamming as a standard feature. Thirty one systems have a spoofing capability, 18 involve lasers, 27 employ nets, and eight take the form of a sacrificial collision drone. (A small number of systems have certain interdiction elements as added optional extras)



Photo by Wesley Farnsworth.

# **CHALLENGES OF COUNTERING DRONES**

As of this writing, the technical challenge of countering drones has not yet been fully surmounted. In a solicitation published in March 2019, the U.S. Defense Innovation Unit stated that "it has proven difficult to identify and mitigate threats using currently fielded technologies."<sup>6</sup> Dozens of background interviews with military and law enforcement personnel have validated this assertion. The challenges posed by, and to, counter-drone technology also extend beyond a simple matter of effectiveness: they include complex questions around safety, practicality, policy, and legality.

#### **Detection Effectiveness**

Every detection system has drawbacks. For example:

- Radar systems may struggle to pick out small drones and UAS flying very close to the ground.
- Camera systems might confuse a drone with a bird or an airplane, and may also struggle in adverse weather with low visibility, or if the drone is backlit by a strong light source such as the sun.
- Electro-magnetic interference can degrade the detection capabilities of RF sensors. In urban environments, there are many potential sources of such interference, including communications antennae, two-way radios, telemetry systems, and even power lines and LED lights.<sup>7</sup>
- Certain RF sensors, including some systems marketed as "passive" may likewise emit RF signals that could interfere with other communications, making them potentially dangerous to deploy in some environments.<sup>8</sup>
- Radar, certain RF systems, and EO/IR sensors must have a direct line of sight with the intruding drone in order to make a detection. This could be particularly problematic in urban environments, where a drone may only appear within a sensor's line of sight for a couple of seconds before disappearing again.<sup>9</sup>
- Some detection systems may only be capable of providing a rough estimate of an incoming drone's location.<sup>10</sup>
- Certain flight patterns—most notably hovering and moving vertically—can make drones harder to detect

with automated tracking algorithms applied to radar or camera data.<sup>11</sup>

• Acoustic sensors rely on a library of sounds emitted by known drones, while RF detection systems likewise only detect certain frequency bands in a pre-established library. Given the rapid rate at which drones are emerging on the market and proliferating, even libraries that are updated often will never cover 100 percent of the drones that might be operating at any given time.

#### False Negatives and False Positives

In order to be useful, C-UAS detection systems must generate low levels of false negatives and false positives. This is difficult to achieve. C-UAS detection elements must be sensitive enough to detect all drones operating within the area of use, but systems that are too sensitive may create an overwhelming number of false positives, rendering the system unusable. According to the results of FAA counter-drone systems testing, distinguishing true-positives from false positives in cluttered environments requires "a high level of manpower."<sup>12</sup>

### Distinguishing Legitimate and Illegitimate Drone Use

In future operating environments where legitimate drone use is common, it will become increasingly important for C-UAS operators to be capable of differentiating between legitimate and rogue drones. For example, at a large sporting event, the airspace may be crowded with legitimate aerial cinematography drones that do not pose a security risk alongside rogue drones that do. During its deployment to the 2019 Super Bowl, the FBI counter-UAS team was "seconds away," according to one official involved in the operation, from mitigating a drone that turned out to be operating as part of a sanctioned cinematography service. Particularly given the potential hazards of mitigating a drone in civilian environments, C-UAS operators will need to develop means to rapidly and reliably determine the threat level of an incoming UAV based on the limited information provided by existing detection technologies\* (Remote ID technology—discussed in the insert on page 13—may go a long way to addressing this issue once implemented, but it will not be a total fix). In the military domain, this could also be an issue; a C-UAS system that cannot tell the difference between allied and adversary unmanned aircraft could accidentally shoot down friendly drones.

#### **Response Window**

Counter-drone operators may only have a very brief window of time to make a decision as to whether an incoming drone is indeed malicious. For example, consider that a security team is protecting a large public gathering with a counter-drone system that has an effective identification range of 750 meters and an interdiction element that could pose a certain level of hazard to the crowd when activated (see following section). If a drone is travelling toward the crowd at 15 meters per second (a fairly standard speed for many commercial systems available on the market today), the team will have less than 50 seconds to decide upon an appropriate response. Thanks to advances in propulsion technologies, commercially available drones will become much faster in the years ahead, further reducing the viable response window for C-UAS.

#### Interdiction Hazards

Many—if not all—counter-drone interdiction techniques can be dangerous in certain circumstances. Drones that have their flight interrupted by kinetic means may fall to the ground with considerable force. Even certain net-based systems that are equipped with a parachute to bring the ensnared drone down to the ground in a controlled manner may be risky if the parachute fails to deploy correctly or if the interdiction occurs at low altitude. Interdiction elements must be incredibly precise to hit a moving drone, and could be dangerous to bystanders if they miss. Long-range effectors such as lasers and high-powered microwaves could pose a serious threat to aircraft operating above a targeted

#### Non-State Group Use of Drones in Conflict

A range of non-state groups, including ISIS, Hezbollah, Hamas, the Kurdistan Workers' Party, Jabhat al-Nusra, Donetsk People's Republic, and Ansar-Allah (more commonly known as the Houthi Movement) have demonstrated a capability to use drones for a wide range of operations including aerial strikes, surveillance and reconnaissance, and propaganda. This has had a profound effect on the conflicts in which these types of actors fight.

- Using mostly commercial off-the-shelf drones and subcomponents, ISIS has conducted hundreds of armed aerial attacks,<sup>13</sup> many of which have been lethal, and has also used drones to help guide vehicle-borne IEDs more accurately toward their targets.
- In August 2018, two commercial multirotor drones carrying explosives descended on a military parade in Caracas, Venezuela in an apparent assassination attempt by an anti-government group against President Nicolás Maduro, sparking a stampede that left several injured.<sup>14</sup>
- In Ukraine, the Donetsk Peoples' Republic and other belligerents have employed drones built largely with off-the-shelf components to conduct surveillance, manage the battlespace, and drop small explosive devices—all to considerable effect.<sup>15</sup>
- Using a range of aircraft developed with direct support from Iran, Houthi units have mounted successful attacks on a variety of different targets, including critical infrastructure deep within defended Saudi airspace. In January 2019, a Houthi drone packed with 80kg of explosives detonated over the dais at a Yemeni military parade, killing six soldiers and injuring many others.<sup>16</sup> Eight months later, the group used ballistic missiles and an armed drone to strike a military camp in Aden, killing 36 people.<sup>17</sup> The following month, in an attack thought to be conducted by or in connection with the Iranian government, a small swarm of attack drones and cruise missiles caused significant damage to critical Saudi oil processing facilities in Abgaig and Khurais.<sup>18</sup>
- Federal law enforcement authorities have disrupted several schemes by extremist groups and "lone wolf" actors to use remote-control aircraft for various kinds of kinetic attacks in the U.S.<sup>19</sup>

<sup>\*</sup>Some systems may be able to identify the drone's registration number, which could aid in this estimation, but such systems still wouldn't be able to prove beyond reasonable doubt that a drone is being operated with malicious intent at that very moment. Imagine, for instance, that a malicious actor uses a stolen drone to conduct an attack.

drone. Jamming systems, meanwhile, can interfere with legitimate communications links in their vicinity; if used at an airport, for example, they could interrupt air traffic management operations.\* The use of GPS jamming or spoofing systems, in particular, is especially dangerous in areas where other entities rely on reliable GPS navigation (for example, manned aircraft at an airport).

### Interdiction Effectiveness

Like detection systems, no interdiction system is 100 percent effective. Following a five day counter-drone exercise in 2017 in which a variety of established defense firms and startups tested their counter-drone products on drones operating at a distance of roughly 200 meters, the Joint Improvised-Threat Defeat Organization, which organized the event, reported that the drones were, in general, "very resilient against damage" and concluded that most of the C-UAS systems needed further development.<sup>20</sup> More recent C-UAS exercises indicate that this problem remains an enduring one.

Like detection systems, all interdiction systems have specific drawbacks:

- RF jamming systems have no effect against drones that operate without an active RF link.
- Many signal jammers have a limited effective range of a few hundred meters, meaning that the system must be very close to the intruding drone to successfully mitigate it, and are not effective without a direct line-of-sight to the drone. Jammers that are capable of operating at long ranges and beyond line-of-sight must be significantly more powerful, but more powerful jammers also pose a higher risk of interference to legitimate communications.
- All kinetic systems may struggle against drones that are moving quickly or in unpredictable patterns. (And when they do work as intended they may destroy components of the drone that are necessary for forensic investigations).
- Spoofing systems, meanwhile, are technically very difficult to build and implement, and may not be

universally effective against all drones. Unmanned aircraft that have been built with protected communication links, for example, could be resistant to spoofing attacks.

#### **Drone Threats in Civilian Environments**

In civilian environments, the threat of rogue, malicious drone use continues to grow and extends beyond the troubling prospect of a kinetic attack by a terror group.

- The prolonged disruption at Gatwick Airport in December 2018, which grounded flights for more than 36 hours and left hundreds of thousands of passengers stranded, costing airlines an estimated \$60 million in losses,<sup>21</sup> not only demonstrated the technology's capacity to cause havoc but also the impunity that it can afford the operators. As of this writing, the perpetrators of the disruptions have not been apprehended. And this is to say nothing of the fact that, had the drones been armed, they could have been used to attack the aircraft, with potentially devastating consequences.
- Sightings of drones over sensitive facilities such as a submarine base in Washington State<sup>22</sup> and nuclear facilities in France<sup>23</sup> have raised the specter of state- and non-state-sponsored drone espionage, while sightings of drones at large sporting events are also becoming increasingly common, highlighting how these generally well-protected facilities also remain vulnerable from the air.
- Among criminal groups, drones have become a popular tool for smuggling contraband into prisons and across heavily secured borders. Drones have also reportedly been used for counter-surveillance,<sup>24</sup> scoping targets for robberies and, in at least one dramatic case in the U.S, disrupting a major law enforcement operation.<sup>25</sup>
- Meanwhile, near misses between drones and manned aircraft have become a common occurrence in every crowded airspace system in the world. Even though many of these incidents are the result of clueless—or perhaps reckless operators, many worry that they could still cause a collision with a manned aircraft that could result in a catastrophic accident.<sup>26</sup>

<sup>\*</sup>Advanced jamming systems that only block the frequency on which the targeted drone is operating, as well as directed jamming antennas, may reduce interference with legitimate communications, but this technology is only beginning to emerge on the market, and it has not yet been certified as entirely safe.<sup>27</sup>

### Advances in Drone Technology

Drone technology itself is not standing still, and advances in this area will pose new challenges for counter-drone systems. As the unmanned aircraft systems market expands and the range of readily available aircraft types becomes more diverse, counter-drone systems will need to be flexible enough to detect and neutralize drones that come in a wide variety of shapes and sizes. These could span from large unmanned aircraft capable of carrying heavy payloads at very high speeds to low-flying micro surveillance drones that might only weigh a few grams. paper describes as an "essentially unlimited operation range,"<sup>34</sup> making the pilot harder to find. Furthermore, LTE drones would be difficult or dangerous to interdict with jamming systems without interfering with ubiquitous cellular communications.<sup>35</sup>

Not all of these advances are motivated by a desire to make drones harder to counter. Somewhat ironically, many of these advances are driven by efforts to make drones safer. Certain commercially available drones today already come with frequency-hopping systems as standard, a feature intended to create a more resilient link to the operator that could nevertheless make the

"This threat is evolving every three to six months—it is just that adaptive...This is going to be a continuing challenge due to the adaptive nature of the problem of being able to use small drones in so many different ways and you cannot rely on one technique to respond to them."<sup>28</sup> —Vayl S. Oxford, Director, U.S. Defense Threat Reduction Agency, March 2019

There are also individual technological advances emerging that pose unique challenges from a counter-drone perspective. Perhaps most notably in the near-term is the active research to develop drones that can operate in GPS-denied environments,<sup>29</sup> which would be resilient to any kind of jamming (which is currently by far the most common interdiction method on the market). For example, according to Russian state media, the Russian military is planning to deploy GLONASS-free surveillance drones to the Arctic to track vessels across wide areas,<sup>30</sup> while the U.S Defense Advanced Research Projects Agency is developing autonomous, GPS-free multirotor drones that can travel at 20 m/s.<sup>31</sup>

Other research tracks seek to develop systems capable of actively defeating jamming or spoofing attacks. Eventually, drones could be programmed to evade the specific frequencies targeted by a jammer, or to switch frequency bands across a broad spectrum, or initiate a series of evasive maneuvers, as soon as they detect a jamming signal.<sup>32</sup> Modern GPS receivers are also increasingly being designed to minimize interference from the ground, which can make them difficult to jam with terrestrial systems. Others are being developed with features to detect incoming spoofing attacks.<sup>33</sup>

In a similar vein, consumer drones may soon be controllable via mobile LTE networks rather than through an RF link. An LTE drone could be operated at what one aircraft more robust against jamming. Researchers at the University of Zürich are developing a multirotor drone that can autonomously dodge fast-moving objects at close range. The idea is to enable unmanned aircraft to avoid obstacles such as birds or other aircraft,<sup>36</sup> but the same feature could also enable the drone to avoid nets and other projectiles.

The proliferation of C-UAS technology will also accelerate the development of technologies that will render C-UAS systems less effective—countermeasures to the countermeasures—particularly in military environ-



Photo by Staff Sgt. Mylinda DuRousseau

ments. For example, drones might be programmed to operate in patterns that make them difficult to detect with automated target detection algorithms. Rotors might be modified to dampen a drone's engine noise so that it can evade acoustic detection. Military drones could begin carrying devices to detect incoming spoofing attacks. Drones might be designed in such a way as to reduce their radar signature (some have speculated that ISIS drones are often wrapped in tape for precisely this reason). Groups might program an explosives-laden drone's "home" location as its intended target, so that if the drone is jammed and initiates a "return to home" mode (a standard feature on many commercial drones), it will fly straight to the very place that the C-UAS operators are trying to protect.

Finally, the advent of drone swarms (or simple agglomerations of multiple drones) would present a range of particularly vexing technical challenges from a defensive perspective.\* A swarm of drones would outmatch any interdiction system with a smaller number of "shots" than the number of aircraft in the swarm—consider, for example, a swarm of ten drones against a net-cannon that only holds five nets. A swarm would also defeat any counter-drone system with a smaller effective detection or interdiction area than the spread of the swarm itself; directional jammers, for example, only project a narrow beam of radio frequency, and as such they would be ineffective against a group of drones spread across an area that is wider than that beam. Certain detection and tracking products may even be unable to track more than a handful of drones simultaneously.37 A "swarm" doesn't have to be dynamic or truly autonomous to achieve these effects; ten individual drone operators flying ten drones in unison may be just as difficult to defend against as a true autonomous swarm of ten aircraft. While a number of firms are developing counter-drone products capable of mitigating multiple incoming aircraft, this remains a developmental capability.38

\*In 2018, a committee of subject matter experts convened by the National Academies of Sciences, Engineering, and Medicine concluded that the technologies necessary to deploy collaborative swarms of up to hundreds of drones will be widely available by 2025.<sup>39</sup>

### Lack of Operational Data

There is a distinct lack of information regarding the operational track record of deployed systems. Not a single C-UAS manufacturer approached in the preparation of this report would provide details about their product's performance in real-world use. This information vacuum makes it difficult for would-be C-UAS owners to know what actually works and what doesn't, anticipate potential issues, and select a system that is best suited to their needs.

#### Cost

Counter-drone technology is expensive. Though most manufacturers do not disclose their price lists, the relatively sparse pricing information available suggests that the technology falls beyond the reach of many small organizations wishing to protect their airspace. According to a 2019 study by Sandia National Laboratories, out of 123 C-UAS products for which pricing information was available, 77 cost more than \$100,000.40 Just two weeks after the Gatwick drone incident, the airport announced that it had already spent more than \$6 million installing counter-drone systems to prevent future incidents.<sup>41</sup> According to a study by Deutsche Flugsicherung, equipping Germany's 16 busiest airports with drone detection systems would cost upwards of half a billion euros.<sup>42</sup> Personnel training, maintenance, and staff time to operate the counter-drone system all incur significant additional costs.



Photo by Lance Cpl. Dalton Swanbeck / USMC

### Legality

In the U.S. and many other countries, counter-drone systems share a common drawback: they may not always be legal. In many instances, there is significant confusion and ambiguity as to the exact legal dimensions of counter-drone technology use. This is because the technology is often subject to numerous overlapping laws that were drafted to address other technologies, long before counter-drone technology existed. Adding to this ambiguity is the fact that most governments have not yet established comprehensive C-UAS-specific policies, while airspace regulators continue to develop regulations that may, in turn, have a bearing on C-UAS (see insert on page 13).

Signal jamming devices, including the more advanced directed systems, are either illegal or restricted in many countries. In the U.S., jamming systems may also violate the Wiretap Act, which forbids the interception of electronic communications. (Even systems that merely detect and track a drone by downloading information about its location and telemetry might violate this law.)<sup>43</sup> Spoofing systems, meanwhile, may contravene the Computer Fraud and Abuse Act.<sup>44</sup> Both kinetic and non-kinetic systems may also violate the U.S. Aircraft Sabotage Act, which imposes heavy fines and even prison sentences for anybody who willfully "sets fire to, damages, destroys, disables, or wrecks any aircraft" in U.S. airspace.<sup>45</sup>

As of this writing, four federal agencies—the Department of Defense, Department of Energy, Department of Justice, and Department of Homeland Security have been granted authority to mitigate drones in U.S. airspace. These agencies use C-UAS to protect sensitive government facilities such as nuclear sites and military



Photo by Deborah Lee Soltesz

bases, as well as for security during large events such as the Super Bowl. Some local law enforcement agencies and other organizations have urged the government to extend this C-UAS authorization below the federal level so that they can protect their own airspace without relying on the small number of federal C-UAS units.<sup>46</sup> Federal officials have indicated that they may do so, but have not provided a timeline for the policy change. In the meantime, a growing number of local law enforcement agencies are likely to acquire drone mitigation systems anyway, in spite of their legally dubious status, and there is confusion as to whether a police officer shooting down a drone would be granted immunity under provisions that authorize the use of force in emergencies.

Certain common detection systems may also not always be legal.<sup>47</sup> The FAA has stated, as recently as May 2019, that it "cannot confirm the legality of any UAS detection system." For example, certain types of radar could, according to the FAA, "require FCC [Federal Communications Commission] or NTIA [National Telecommunications and Information Administration] authorization and interagency coordination," and the use of any type of detection system at any U.S. airport could implicate various sections of the U.S. Code and a number of FAA Orders.<sup>48</sup>

Such legal restrictions and ambiguities are mirrored around the globe. In the United Kingdom, countering a drone in any way may violate provisions in the Aviation Security Act and the Criminal Damage Act; jamming a drone likely violates the Wireless Telegraphy Act and the Electromagnetic Compatibility Regulations; laser-based systems could run afoul of a 2016 Air Navigation Order.\* In Europe, C-UAS sensors that collect personally identifiable information may implicate the General Data Protection Regulation.<sup>49</sup>

A detailed analysis by Jonathan Rupprecht of the various legal obstacles to C-UAS use in the United States is available <u>here</u>.<sup>50</sup> An analysis by the ALADDIN project of the legal implications of C-UAS in Europe is available <u>here</u>.<sup>51</sup>

<sup>\*</sup>A number of British laws might likewise provide legal cover for C-UAS actions, depending on the context, including the Criminal Law Act, the Police and Criminal Evidence Act, the Criminal Justice and Immigration Act, and the Investigatory Powers Act, though the potentially relevant provisions in these laws have not been tested against cases involving drone interdiction.<sup>52</sup>

#### Lack of Standards

No international standards exist for the proper design and use of C-UAS systems. This means there may be significant variances between the performance and reliability of systems that might, at the spec-sheet level, appear to be very similar. Given that the demand for this technology has only emerged in the past few years, many of the products offered by the companies that we identified have not yet had time to mature. Some firms appear to be working to capitalize on the growing interest in this technology before properly maturing or field-testing their products. U.S. security officials who spoke on background have noted that a large proportion of systems that are actively marketed to U.S. government customers do not perform as advertised. The absence of standards also raises questions about the safety of these systems. Particularly in civilian environments, a malfunctioning C-UAS system might present a public safety threat-consider, for example, a jamming system that interferes with emergency radio communications, or a kinetic system that misses its intended target.

#### Privacy

Because counter-drone detection systems are a form of surveillance technology, they potentially pose a risk to privacy if misused or if the data that they collect is not handled properly. For example, electronic identification systems could be capable of obtaining personally identifiable information-such as the aircraft's registration number-for drones operating across a broad area. Similarly, wide-area camera systems could inadvertently record individuals or vehicles on the ground that are not relevant to the counter-drone operations itself.53 This is in addition to private digital information that could be collected from a drone either at the point of detection and tracking or during forensic analysis. So far, there have been relatively few efforts to evaluate how to mitigate privacy risks that could arise from the use of these systems.\* Under the Preventing Emerging Threats Act of 2018, U.S. agencies with C-UAS authorities are required to ensure that their operations respect First and Fourth Amendment protections, responsibly handle

collected data, and destroy all intercepted drone communication data within 180 days,<sup>54</sup> but many civil or private C-UAS operators around the globe likely do not have similar protections in place.

#### <u>Electronic Identification and Unmanned Traffic</u> <u>Management</u>

Running in parallel to the growing adoption of counter-drone technologies is the range of efforts by airspace authorities to implement Unmanned Aerial System Traffic Management (UTM) systems and Remote Identification (Remote ID or RID) requirements for civilian and civil drones. UTM systems will enable airspace authorities to segregate compliant unmanned aircraft from airports, restricted airspace, and airspace inhabited by manned aircraft. Remote identification, meanwhile, refers to a range of systems for remotely accessing information such as the model type, operator name and location, and registration number of certain nearby drones. Chinese drone maker DJI produces one such system, called AeroScope<sup>55</sup>—which has already been adopted for drone detection by C-UAS teams-and other manufacturers are likely to follow suit. A number of governments are in the process of developing detailed plans for implementing UTM, as well as regulations to require all drones to be equipped with Remote ID capabilities. In the long-term, the combination of Remote ID and UTM is likely to significantly reduce potentially dangerous drone incidents caused by "careless" or "clueless" operators who simply venture into restricted airspace by mistake. This will narrow the C-UAS challenge to those cases where a drone operator has both malicious intent and some technical capacity to bypass these routine airspace control systems. These cases will be far less common than the non-malicious cases that make up the majority of drone incidents today, but they will also be far more dangerous and difficult to defend against.

<sup>\*</sup>One notable exception is a study by the Advanced hoListic Adverse Drone Detection, Identification & Neutralization (ALADDIN) program, an E.U.-funded initiative to develop a sophisticated counter-drone detection and neutralization system.

# **READING LIST**

- "Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems," Global Counterterrorism Forum, September 2019. https:// www.thegctf.org/LinkClick.aspx?fileticket=j5gj4fS-J4fI%3d&portalid=1&timestamp=1569424280400
- "Blue Ribbon Task Force on UAS Mitigation at Airports Final Report," Blue Ribbon Task Force on UAS Mitigation at Airports, October 2019. https://uasmitigationatairports.org/wp-content/uploads/2019/10/ BRTF-Report2019.pdf
- Scott Brooks and Camron Kouhestani, "Counter-Unmanned Aircraft Systems Market Survey," Department of Homeland Security, Prepared by Sandia National Laboratories, February 2019.
- "Counter-Unmanned Aircraft System (C-UAS) Strategy Extract," United States Army, 2016. www.arcic.army. mil/App\_Documents/Army-CUAS-Strategy.pdf
- Scott Crino and Andy Dreby, "Drone Technology Proliferation in Small Wars," Small Wars Journal, September 2019. https://smallwarsjournal.com/jrnl/ art/drone-technology-proliferation-small-wars?mc\_cid=90e54c31e2&mc\_eid=cb69914e13
- Dan Gettinger, "The Drone Databook," Center for the Study of the Drone, 2019. https://dronecenter.bard. edu/projects/drone-proliferation/databook/.
- Dan Gettinger, "Drones Operating in Syria and Iraq," Center for the Study of the Drone, 2016. https:// dronecenter.bard.edu/drones-operating-in-syria-andiraq/
- Dan Gettinger and Arthur Holland Michel, "Drones at Home: Drone Incidents," Center for the Study of the Drone, 2017. http://dronecenter.bard.edu/drones-athome-drone-incidents/
- Brian A. Jackson, David R. Frelinger, Michael J. Lostumbo, and Robert W. Button, "Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles," RAND Corporation, 2008. https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND\_MG626.pdf

- Don Rassler, "The Islamic State and Drones: Supply, Scale, and Future Threats," Combating Terrorism Center at West Point, United States Military Academy, July 2018. https://ctc.usma.edu/app/uploads/2018/07/ Islamic-State-and-Drones-Release-Version.pdf
- Deepan Sarma and Paul Quinn, eds., "D3.1 Data protection, Social, Ethical and Legal Frameworks," Diginext, Advanced hoListic Adverse Drone Detection, Identification Neutralisation program, February 2018. http://aladdin2020.eu/wp-content/ uploads/2018/04/ALADDIN\_D3.1\_DataProtection-SoEL\_Framework\_V1\_0\_PU.pdf
- Col. Matthew T. Tedesco, "Countering the Unmanned Aircraft Systems Threat," Military Review, November-December 2015. usacac.army.mil/CAC2/ MilitaryReview/Archives/English/MilitaryReview\_20151231\_art012.pdf
- U.K. Parliament Defence Committee, Domestic Threat of Drones inquiry - publications. https://www.parliament.uk/business/committees/committees-a-z/ commons-select/defence-committee/inquiries/parliament-2017/domestic-threat-drones-17-19/publications/
- John Wendle, "The Fighting Drones of Ukraine," Air & Space Magazine, February, 2018. https:// www.airspacemag.com/flight-today/ukrainesdrones-180967708/

# NOTES

- 1. Dan Gettinger, "The Drone Databook," Center for the Study of the Drone, 2019. https://dronecenter.bard.edu/ projects/drone-proliferation/databook/
- 2. Ilan Ben Zion, "IDF fails 3 times to bring down drone over Golan," *The Times of Israel*, July 17, 2016. https:// www.timesofisrael.com/idf-we-tried-and-failed-3-timesto-bring-down-drone-over-golan/
- Gabriel C. Birch, John C. Griffin, and Matthew K. Erdman, "UAS Detection, Classification, and Neutralization: Market Survey 2015," Sandia National Laboratories, Sandia Report SAND2015-6365, 2015. prod.sandia.gov/ techlib/access-control.cgi/2015/156365.pdf
- Rachel Bishop and Mathew Di Salvo, "British prison becomes first in world to use anti-drone 'disruptor' shield to stop inmates smuggling in contraband," *Mirror*, May 16, 2017. https://www.mirror.co.uk/news/uk-news/britishprison-becomes-first-world-10433402
- Panel Discussion: "UAS Mitigation from a Public Safety Standpoint," AUVSI Xponential, Chicago: April 30, 2019. https://www.xponential.org/xponential2019/public/ SessionDetails.aspx?FromPage=Sessions.aspx&Session-ID=3158&SessionDateID=41
- "Tech Area of Interest: Installation Counter Unmanned Aerial Systems (CUAS)," NC Deftech, March 11, 2019. https://deftech.nc.gov/opportunities/2019-04-30/tech-area-interest-installation-counter-unmanned-aerial-systems-cuas
- "Unmanned Aircraft System Detection Technical Considerations," U.S. Federal Aviation Administration, 2019. https://www.faa.gov/airports/airport\_safety/media/Attachment-3-UAS-Detection-Technical-Considerations.pdf
- 8. "Unmanned Aircraft System Detection Technical Considerations"
- "Questions to Ask When Researching Counter Unmanned Aerial Systems," U.S. Department of Homeland Security Science and Technology Directorate, 2019.
- Scott Brooks and Camron Kouhestani, "Counter-Unmanned Aircraft Systems Market Survey," Department of Homeland Security, Prepared by Sandia National Laboratories, February 2019.
- "Unmanned Aircraft System Detection Technical Considerations," U.S. Federal Aviation Administration, 2019. https://www.faa.gov/airports/airport\_safety/media/Attachment-3-UAS-Detection-Technical-Considerations.pdf
- Letter from John R. Dermody, P.E., Director, Office of Airport Safety and Standards, U.S. Federal Aviation Administration, July 19, 2018. https://web.archive.org/ web/20190110160243/https://www.faa.gov/airports/air-

port\_safety/media/counter-uas-airport-sponsor-letter-july-2018.pdf

- 13. "Home-made drones now threaten conventional armed forces," The Economist, February 8, 2018. https://www. economist.com/news/science-and-technology/21736498their-small-size-and-large-numbers-can-overwhelm-defences-home-made-drones-now
- Nick Paton Walsh, Natalie Gallón, Evan Perez, Diana Castrillon, Barbara Arvanitidis and Caitlin Hu, "Inside the August plot to kill Maduro with drones," CNN, June 21, 2019. https://edition.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html
- Scott Crino and Andy Dreby, "Drone Technology Proliferation in Small Wars," Small Wars Journal, September 2019. https://smallwarsjournal.com/jrnl/art/drone-technology-proliferation-small-wars?mc\_cid=90e54c31e2&mc\_eid=cb69914e13
- Ahmed Al-Haj, "Bomb-laden rebel drone kills 6 at Yemen military parade," Associated Press, January 10, 2019. https://www.apnews.com/92f491d2794440afaf53967fceb0c1b9
- 17. "Yemen: Dozens killed in Houthi attack on Aden military parade," Al Jazeera, August 1, 2019. https://www.aljazeera.com/news/2019/08/yemen-houthi-rebels-target-military-parade-aden-190801065146809.html
- 18. "Major Saudi Arabia oil facilities hit by Houthi drone strikes," Associated Press, September 14, 2019. https:// www.theguardian.com/world/2019/sep/14/major-saudiarabia-oil-facilities-hit-by-drone-strikes
- Eric Convey, "Feds: Ashland man plotted to blow up Pentagon, Capitol," *Boston Business Journal*, September 28, 2011, https://www.bizjournals.com/boston/ news/2011/09/28/feds-ashland-man-plotted-to-blow-up. html.
- Eric Schmitt, "Pentagon Tests Lasers and Nets to Combat a Vexing Foe: ISIS Drones," *The New York Times*, September 23, 2017. https://www.nytimes.com/2017/09/23/ world/middleeast/isis-drones-pentagon-experiments.html
- Hallie Detrick, "Gatwick's December Drone Closure Cost Airlines \$64.5 million," *Fortune*, January 22, 2019. https://fortune.com/2019/01/22/gatwick-drone-closurecost/
- 22. Hal Bernton,"Who flew drone over Bangor submarine base? Navy wants to know," *The Seattle Times*, February 25, 2016. https://www.seattletimes.com/seattle-news/ crime/whos-flying-drones-over-bangor-submarine-basenavy-wants-to-know/
- 23. "More drones spotted over French nuclear power sta-

tions," *Agence France-Presse*, October 31, 2014. https:// www.theguardian.com/environment/2014/oct/31/moredrones-spotted-over-french-nuclear-power-stations

- "Drug syndicate 'used drones to monitor police'," BBC News, June 30, 2017. https://www.bbc.com/news/ world-australia-40453026
- Patrick Tucker, "A Criminal Gang Used a Drone Swarm To Obstruct an FBI Hostage Raid," *Defense One*, May 3, 2018. https://www.defenseone.com/technology/2018/05/criminal-gang-used-drone-swarm-obstructfbi-raid/147956/
- 26. Dan Gettinger and Arthur Holland Michel, "Drones at Home: Drone Incidents," Center for the Study of the Drone, 2017. http://dronecenter.bard.edu/drones-at-homedrone-incidents/
- Michael J. O'Donnell, A.A.E., Director of Airport Safety and Standards, U.S. Federal Aviation Administration, October 26, 2016. https://www.faa.gov/airports/airport\_safety/media/UAS-Counter-Measure-Testing-letter.pdf
- Interview with Vayl S. Oxford in Kristina Hummel, "A View from the CT Foxhole: Vayl S. Oxford, Director, Defense Threat Reduction Agency," CTC Sentinel, Volume 12, Issue, March 2019, pp10-14. https://ctc.usma.edu/app/ uploads/2019/03/CTC-SENTINEL-032019.pdf
- G. Balamurugan, J. Valarmathi and V. P. S. Naidu, "Survey on UAV navigation in GPS denied environments," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016, pp. 198-204. doi: 10.1109/ SCOPES.2016.7955787
- Paulina Glass, "Russia's New Arctic Drones Are Built to Spot Ships," *Defense One*, December 11, 2018. https:// www.defenseone.com/technology/2018/12/russias-newarctic-drones-are-built-spot-ships/153444/
- "Fast Lightweight Autonomy (FLA)," Defense Advanced Research Projects Agency. https://www.darpa.mil/program/fast-lightweight-autonomy
- 32. S. Walker-Roberts and M. Hammoudeh, Written evidence submitted by Manchester Metropolitan University, U.K. Parliament Defense Committee, Domestic Threat of Drone Inquiry, May 9, 2019. data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/ defence-committee/domestic-threat-of-drones/written/101797.html
- Information provided by Red Six Solutions, a U.S. red teaming firm specializing in drones and counter-drone dynamics.
- Yong Zeng, Jiangbin Lyu, and Rui Zhang, "Cellular-Connected UAV: Potentials, Challenges and Promising Technologies," draft paper published on arXiv, April 6, 2018. https://arxiv.org/pdf/1804.02217.pdf
- 35. Angus Batey, "Regulatory Uncertainty Roils UK Response To Drone Threat," *Aviation Week & Space Technology*, May 10, 2019. https://aviationweek.com/ future-aerospace/regulatory-uncertainty-roils-uk-response-drone-threat
- 36. Davide Falanga, Suseong Kim, and Davide Scaramuzza, "How Fast is Too Fast? The Role of Perception Latency

in High-Speed Sense and Avoid," IEEE Robotics and Automation Letters, Preprint Version, January 2019. rpg. ifi.uzh.ch/docs/RAL19\_Falanga.pdf

- Scott Brooks and Camron Kouhestani, "Counter-Unmanned Aircraft Systems Market Survey," Department of Homeland Security, Prepared by Sandia National Laboratories, February 2019.
- See for example, the U.S. Air Force THOR program, the U.S. Army's Indirect Fires Protection Capability system, And Raytheon's High-Power Microwave and laser systems.
- 39. "Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations," Board on Army Science and Technology Division on Engineering and Physical Sciences, National Academies of Sciences, Engineering, and Medicine, 2018. (Abbreviated Version of a Restricted Report.)
- 40. Scott Brooks, Camron Kouhestani, "Counter-Unmanned Aircraft Systems Market Survey," Department of Homeland Security, Prepared by Sandia National Laboratories, February 2019.
- Josh Spero, "Gatwick spends £5m on airport anti-drone measures," *Financial Times*, January 3, 2019. https:// www.ft.com/content/cdaa19e6-0f97-11e9-a3aa-118c761d2745
- 42. "Integrating drone detection systems into airport surveillance networks in Germany 'will cost EUR500 million,"" *Unmanned Airspace*, October 1, 2019. https://www. unmannedairspace.info/counter-uas-systems-and-policies/ integrating-drone-detection-systems-into-airport-surveillance-networks-in-germany-will-cost-eur500-million/
- "National Defense Authorization Act for Fiscal Year 2018," Sec. 1602, 115th Cong, 2018. https://fas.org/sgp/ news/2017/06/dod-uas.pdf
- 44. "Computer Fraud and Abuse Act (CFAA)," Internet Law Treatise. https://ilt.eff.org/index.php/Computer\_Fraud\_ and\_Abuse\_Act\_(CFAA)
- 45. "S.2623 Aircraft Sabotage Act," 98th Cong., 1984. https://www.congress.gov/bill/98th-congress/senate-bill/2623
- 46. "Blue Ribbon Task Force on UAS Mitigation at Airports Final Report," Blue Ribbon Task Force on UAS Mitigation at Airports, October 2019. https://uasmitigationatairports.org/wp-content/uploads/2019/10/BRTF-Report2019. pdf and Joseph De Avila, "New York Police Seek Authority to Take Down Drones," *The Wall Street Journal*, February 17, 2019. https://www.wsj.com/articles/new-yorkpolice-seek-authority-to-take-down-drones-11550419320
- 47. Letter from John R. Dermody, P.E., Director, Office of Airport Safety and Standards, U.S. Federal Aviation Administration, July 19, 2018. https://web.archive.org/ web/20190110160243/https://www.faa.gov/airports/airport\_safety/media/counter-uas-airport-sponsor-letter-july-2018.pdf
- Letter from John R. Dermody, P.E., Director, Office of Airport Safety and Standards, U.S. Federal Aviation Administration, May 7, 2019. https://www.faa.gov/airports/ airport\_safety/media/Updated-Information-UAS-Detec-

tion-Countermeasures-Technology-Airports-20190507. pdf

- Deepan Sarma and Paul Quinn, eds., "D3.1 Data protection, Social, Ethical and Legal Frameworks," Diginext, Advanced hoListic Adverse Drone Detection, Identification Neutralisation program, February 2018. http://aladdin2020.eu/wp-content/uploads/2018/04/ALADDIN\_D3.1\_DataProtectionSoEL\_Framework\_V1\_0\_PU.pdf
- 50. Jonathan Rupprecht, "7 Big Problems with Counter Drone Technology (Drone Jammers, Anti Drone Guns, etc.)," Rupprecht Law, P.A.. https://jrupprechtlaw.com/ drone-jammer-gun-defender-legal-problems
- 51. "D3.1 Data protection, Social, Ethical and Legal Frameworks"
- 52. "D3.1 Data protection, Social, Ethical and Legal Frameworks"
- 53. "D3.1 Data protection, Social, Ethical and Legal Frameworks"
- 54. "Counter Unmanned Aircraft Systems Legal Authorities," U.S. Department of Homeland Security, 2019. Retireved from https://www.dhs.gov/sites/default/files/publications/19\_0502\_cisa\_dhs-cuas-legal-authorities-factsheet. pdf
- 55. Brian Heater, "DJI's 'electronic license plate' helps authorities identify drones in mid-flight," *TechCrunch*, October 25, 2019. https://techcrunch.com/2017/10/25/ djis-electronic-license-plate-helps-authorities-identifydrones-in-mid-flight.

# **COUNTER-DRONE SYSTEMS DATABASE**

#### <u>About</u>

The database notes the features and capabilities of each system as described by the manufacturer or, in cases where no manufacturer information is available, by reliable media sources. These features have not been independently verified by the Center for the Study of the Drone. Some of the products listed in the database consist of multiple different devices developed by multiple manufacturers that have been combined into a single integrated product (for example, a product that consists of a radar, a camera, and a jammer). In cases where individual elements of those combined products are marketed separately, they are also included in the database as standalone products. The database does not include software products, such as command and control products that are used to manage incoming data from sensors.

### At a Glance

Number of Products	537
Number of Manufacturers	277
Countries of Origin	38
Systems for Detection Only	175
For Interdiction Only	214
For Detection and Interdiction	138

#### **Products**

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
4Intelligence	INT-AU002 Anti UAV	Sweden	Radar, EO (Optional), IR (Optional)	RF Jamming, GNSS Jamming	Ground-based: Fixed
4Intelligence	INT-AU001 Anti UAV Rifle	Sweden		RF Jamming, GNSS Jamming	Handheld
802Secure	AirShield	USA	RF	Spoofing	Ground-based: Fixed
Accipiter	NM1-8A Drone Radar System	Canada	Radar		Ground-based: Fixed
Accipiter	NM1-KHSxV Securi- ty Radar System	Canada	Radar, EO, IR		Ground-based: Fixed
ADE	Maestro	South Korea		RF Jamming, GNSS Jamming	Handheld
Advanced Protection Systems	Ctrl+Sky Stationary	Poland	Radar, Acoustic, EO, IR, RF	Optional: RF Jam- ming, GNSS Jamming	Ground-based: Fixed
Advanced Protection Systems	Ctrl+Sky Portable	Poland	Radar, Acoustic, EO, IR, RF	Optional: RF Jam- ming, GNSS Jamming	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Advanced Protection Systems	Ctrl+Sky Mobile	Poland	Radar, Acoustic, EO, IR, RF	Optional: RF Jam- ming, GNSS Jamming	Ground-based: Mobile
Advanced Protection Systems	Ctrl+Sky Jammer	Poland		RF Jamming, GNSS Jamming	Ground-based: Mobile
Advanced Radar Technologies	Drone Sentinel	Spain	Radar, EO, IR		Ground-based: Fixed
AerialX	DroneBullet	USA		Collision Drone	UAV
AerialX	UAS Locator	USA	RF		Handheld
AeroDefense	AirWarden	USA	RF		Ground-based: Fixed
Aerospace Security & Defense Technologies (ASDT)	SEN&DES	Spain		RF Jamming, GNSS Jamming	Ground-based: Mobile
AimLock	R-M1	USA		Projectile	Ground-based: Mobile
Ainstein	ULGB-D1	USA	Radar		Ground-based: Fixed
Airbus Defence and Space	Counter UAV System	France	Radar, IR,	RF Jamming, GNSS Jamming	Ground-based: Fixed
AirShare	OVERWATCH	Canada	RF	Projectile	Handheld
Airspace Systems	Airspace	USA		Net	UAV
Airspace Systems	Galaxy	USA	RF, EO, IR		Ground-based: Fixed
Airspace Systems	Interceptor	USA		Net	UAV
Alion Science and Technology		USA		Spoofing	Ground-based: Fixed
Allen-Vanguard	ANCILE	Canada		RF Jamming	Ground-based
Almaz Scientific-Pro- duction Enterprise	Attack-DBS	Russia	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
ALS (Pacem Defense)	SKYNET Mi-5	USA		Net	Handheld
ALX Systems	Sentinel	Belgium	EO, IR		UAV
ALX Systems	Spartiath	Belgium	Radar		UAV, Ground-Based: Fixed
AMTEC Less Lethal Systems	Skynet	USA		Net Shotgun Shells	Handheld
Anduril Industries	Anvil	USA		Collision Drone	UAV
Anduril Industries	Lattice	USA	Radar, EO, IR		Ground-based: Fixed
Anti-Drones	Skynet Ultra	Taiwan		RF Jamming, GNSS Jamming	Handheld
Anti-Drones	Skynet DDS	Taiwan	RF		Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
ApolloShield	Omni RF Sensor	Israel	RF		Ground-based: Fixed
ApolloShield	Directional RF Sensor	Israel	RF		Ground-based: Fixed
ApolloShield	RF Sense&Block	Israel	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
ApolloShield	RF Gun	Israel		RF Jamming, GNSS Jamming	Handheld
ApolloShield	RF Jammer	Israel		RF Jamming	Ground-based: Fixed
ApolloShield	RF Locator	Israel	RF		Ground-based: Mobile
Applied Technology Associates	Low-Cost Count- er-Unmanned Aerial System for Targeting (LOCUST)	USA	RF, EO, IR	Laser	Ground-based
Aquila Defense Group	Aquila Defense Group Counter-UAS	Switzerland	RF, Radar, Acoustic, IR	RF Jamming, GNSS Jamming	Ground-based
Aquila International	Beam 250	USA	Radar		Ground-based
ARTsys360	RS500	Israel	RF	RF Jamming, GNSS Jamming	Ground-based: Mobile
Ascent Vision	CM202U	USA	EO, IR		Ground-based: Mobile
Aselsan	IHASAVAR	Turkey		RF Jamming, GNSS Jamming	Handheld
Aselsan	IHTAR	Turkey	Radar, RF	RF Jamming, GNSS Jamming, Projectile (Optional)	Ground-based: Fixed
Aselsan	GERGEDAN	Turkey		RF Jamming, GNSS Jamming	Ground-based
Aselsan	Laser Defense System (LSS)	Turkey		Laser	Ground-based
ATL Europa	INH-606-SW1W2	Spain		RF Jamming, GNSS Jamming	Handheld
ATL Europa	CON-001-SW1W2	Spain		RF Jamming, GNSS Jamming	Handheld
Atos	Bull Drone Shield	France	RF, Radar, Acoustic, IR		Ground-based: Fixed
Aveillant	Gamekeeper 16U	UK	Radar		Ground-based: Fixed
Avtomatika Concern (Rostec)	Shipovnik-Aero	Russia	RF, Unknown	RF Jamming, GNSS Jamming	Ground-based
Avtomatika Concern (Rostec)	Pischal	Russia		RF Jamming, GNSS Jamming	Handheld
Avtomatika Concern (Rostec)	Sapsan-Bekas	Russia	RF, Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Mobile
Babcock	LDEW-CD	USA	Radar, EO, IR	Laser, Projectile	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Bei Dou Open Lab	Antidrone Gun	China		RF Jamming, GNSS Jamming	Handheld
BEL	Drone Guard System	India	RF, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Fixed
Belgian Advanced Technology Systems	AD26B Anti-drone Guard	Belgium	Radar, EO, IR, RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Black Sage	TD-1	USA		RF Jamming, GNSS Jamming	Handheld
Black Sage/IEC Infrared	UASX	USA	Radar, EO, IR	RF Jamming, GNSS Jamming, Dazzling (Optional), Laser (Optional)	Ground-based
Blighter Surveillance Systems	A400 Series	UK	Radar		Ground-based: Fixed
Blighter Surveil- lance Systems/Chess Dynamics/Enterprise Control Systems	Anti-UAV Defence System (AUDS)	UK	Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Fixed
Blind Tiger	Wireless Intrusion Detection and Defeat System	USA	RF	Managed Access	Ground-based
Boeing	Laser Avenger	USA	Radar	Laser	Ground-based
Boeing	Compact Laser Weap- on System	USA		Laser	Ground-based
Boeing/General Dynamics	MEHEL 2.0	USA		Laser	Ground-based: Mobile
Booz Allen Hamilton	Enforce Field	USA	Acoustic, EO, IR, RF, Radar		Ground-based: Fixed
Broadfield Security Services	Drone Blocker	Netherlands		RF Jamming	Ground-based: Fixed
BSVT – New Tech- nologies	TRIO	Belarus	Radar, EO, IR	Projectile	Ground-based: Mobile
BYLBOS/Roboost	SPID	France	EO, IR, RF	RF Jamming, GNSS Jamming	Ground-based
C Speed	LightWave CUAS Surveillance Suite	USA	Radar, RF		Ground-based
CACI	SkyTracker	USA	RF	RF Jamming	Ground-based: Fixed
CACI	BITS Electronic Attack Module	USA	RF	RF Jamming, GNSS Jamming	Ground-based, Hand- held
CACI	CORIAN	USA	RF	RF Jamming	Ground-based: Fixed
CACI	AWAIR	USA	RF	RF Jamming	Ground-based: Mobile
CACI	Small Form Factor	USA	RF	RF Jamming	Handheld

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Capture Systems	Anti-Threat Intelligent Detector	Israel	EO, IR	Optional: RF Jam- ming, GNSS Jamming	Ground-based: Fixed
Centum	JANO	Spain	Radar		Ground-based: Fixed
Centum	HERMES	Spain	RF		Ground-based: Fixed
Centum	ARES	Spain		RF Jamming, GNSS Jamming	Ground-based: Fixed
Centum	ATENEA	Spain		Spoofing	Ground-based: Fixed
Centum	No Fly Zrone	Spain	Radar, RF	RF Jamming, GNSS Jamming, Spoofing	Ground-based: Fixed
CerbAir	CerbAir Fixed	France	RF, EO,IR	RF Jamming, Net	Ground-based: Fixed
CerbAir	CerbAir Mobile	France	RF, EO,IR	RF Jamming, Net	
Chenega Europe	dronesnarer	Ireland		Net	Handheld
Chenega Europe	dronevigil Defender	Ireland		RF Jamming	Handheld
Chenega Europe	dronecollider	Ireland		Collision Drone	UAV
Chenega Europe	dronetaker	Ireland		Spoofing	UAV
Chenega Europe	dronesoaker	Ireland		Water projector	Handheld
Chenega Europe	dronetracker	Ireland	Acoustic, Motion Detection		Ground-based: Fixed
Chenega Europe	dronevigil Array	Ireland	Radar		Ground-based: Fixed
Chenega Europe	dronevigil Field Mobile	Ireland	Radar		Ground-based: Mobile
Chenega Europe	dronevigil Holo- graphic	Ireland	Radar		Ground-based: Fixed
Chenega/Synergia	dronesafeguard	USA	RF, Radar, Acoustic		Ground-based
Chess Dynamics	AirGuard	UK	RF, Radar, EO, IR, Acoustic		Ground-based: Fixed
Chess Dynamics	AirShield	UK	Radar, EO, IR		Ground-based: Fixed
China Aerospace Science and Industry Corporation		China		Net	UAV
Cintel	N/A	USA		Spoofing	UAV
Citadel Defense	DFU3000	USA	RF	Spoofing	Handheld, Ground- based: Fixed
Citadel Defense	Titan	USA	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Cobham Antenna Systems	Directional Flat Panel Antenna	USA	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Cobham Antenna Systems	Directional Helix Antenna	USA	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Cobham Antenna Systems	High Power Ul- tra-Wideband Direc- tional Antenna	USA	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Cobham Antenna Systems	Wideband Omni-Di- rectional	USA	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Colorado Engineering	Skyline	USA	Radar		Ground-based
Communications & Systèmes/HGH/Spec- tracom	Boreades	France	Radar, EO, IR	RF Jamming, GNSS Jamming, Spoofing	Ground-based: Fixed
Controp	SPEED-BIRD	Israel	EO, IR		Ground-based: Fixed
Controp	Tornado	Israel	EO, IR		Ground-based: Fixed
Convexum		Israel	RF	RF Jamming, Spoof- ing	Ground-based: Fixed
Copious Imaging	WISP 2.0	USA	IR		Ground-based: Fixed
CPM Elettronica	CPM-DJI-120-4B	Italy		RF Jamming, GNSS Jamming	Handheld
CPM Elettronica	CPM-WILSON	Italy		RF Jamming, GNSS Jamming	Handheld
CRFS	RFeye	UK	RF		Ground-based: Fixed
CTS	Drone Jammer	China		RF Jamming, GNSS Jamming	Handheld
D-Fend Solutions	EnforceAir	Israel	RF	RF Jamming, Spoof- ing	Ground-based: Fixed
DataExpert	Anti-Drone Gear	Singapore		RF Jamming	Handheld
DeDrone	Drone Defender (handheld)	USA		RF Jamming, GNSS Jamming	Handheld
DeDrone	Drone Defender (land- based unit)	USA		RF Jamming, GNSS Jamming	Ground-based: Fixed
Dedrone	RF-300	USA	RF		Ground-based: Fixed
Delft Dynamics	DroneCatcher	Netherlands		Net	UAV
Department 13 Inter- national/Raytheon	MESMER	USA	RF	Spoofing	Ground-based: Fixed
DeTect	DroneWatcherAPP	USA/UK	Mobile App		Handheld
DeTect	DroneWatcherRF	USA/UK	RF		Ground-based: Fixed
DeTect	HARRIER Drone Surveillance Radar	USA/UK	Radar		Ground-based: Fixed

Handheld netic pulse Ground-based F Jam- Ground-based: Fixed Ground-based Ground-based: Fixed
F Jam- Ground-based: Fixed Ground-based Ground-based: Fixed
Ground-based: Fixed
Ground-based: Fixed
Ground-based: Fixed
F Jam- Ground-based: Fixed
Handheld
g Ground-based: Fixed
g, GNSS Ground-based: Mobile
UAV
Ground-based
Ground-based: Fixed
Ground-based: Fixed
Ground-based
Ground-based: Fixed
g, GNSS Ground-based: Fixed
Ground-based: Fixed
g, GNSS Ground-based: Mobile
g, GNSS Ground-based: Fixed
Handheld
g, GNSS Handheld
Ground-based: Fixed
g Ground-based: Mobile

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
DroneShield	DroneGun Tactical	Australia		RF Jamming, GNSS Jamming	Handheld
DroneShield	RadarZero	Australia	Radar		Ground-based: Fixed
Droptec	Dropster	Switzerland		Net	Handheld
Dynamic Shielding	Drone Hunter	South Korea		RF Jamming, GNSS Jamming	Handheld
Dynamic Shielding	Drone Hunter X	South Korea		RF Jamming, GNSS Jamming	Handheld
Dynamite Global Strategies	AIRDEFENSE 6.0	USA		RF Jamming, GNSS Jamming	Ground-based: Fixed
Dynamite Global Strategies	UDJV-01	USA		RF Jamming, GNSS Jamming	Handheld
Dynamite Global Strategies	UD-9B	USA		RF Jamming, GNSS Jamming	Ground-based: Fixed
Dynamite Global Strategies	UD-10F	USA	Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Fixed
Dynamite Global Strategies	UD-20V	USA	Radar, EO, IR, RF	RF Jamming, GNSS Jamming	Ground-based: Mobile
Dynetics	GroundAware	USA	Radar		Ground-based: Fixed
Dynetics	SoundAware	USA	Acoustic		Ground-based: Fixed
ECA Group	EC-180	France	Acoustic, EO, IR, RF, Radar		Ground-based, UAV
Echodyne	EchoGuard	USA	Radar		Ground-based: Fixed
Elbit Systems	ReDrone	Israel	RF, EO (Optional), IR (Optional), Radar (Optional)	RF Jamming, GNSS Jamming	Ground-based: Fixed
Elbit Systems	SupervisIR	Israel	IR		Ground-based: Fixed
Elbit Systems	ReDrone Vehicular Tactical System	Israel	RF, EO (Optional), IR (Optional), Radar (Optional)	RF Jamming, GNSS Jamming	Ground-based: Mobile
ELT-Roma	ADRIAN	Italy	RF, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Fixed
ELTA North America (IAI)	Drone Guard	Israel	Radar, EO, IR, RF	GNSS Jamming, RF Jamming	Ground-based: Fixed
ELTA North America (IAI)	MARS-K	USA	Radar		Ground-based: Fixed
ELTA North America (IAI)	MADS-K	USA	Radar		Ground-based: Fixed
Epirus	Leonidas	USA	"Visual," Radar	Jamming, Electromag- netic Pulse	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
esc Aerospace	escCUAS	Germany	RF, Radar, Acoustic, EO	RF Jamming, GNSS Jamming, Electromag- netic Pulse	Ground-based: Fixed
EWA Government Systems	EWA Counter UAS System	USA	Radar, IR	RF Jamming, GNSS Jamming	Ground-based: Fixed
Exponent	Drone Hunter	UAE	EO, IR		UAV
Finmeccanica – Selex ES (Leonardo)	Falcon Shield	Italy	EO, IR, Radar	RF Jamming, Spoof- ing	Ground-based: Fixed
Flex Force	DroneBuster Block 3	USA		RF Jamming, GNSS Jamming	Handheld
Flex Force	DroneBuster FS	USA		RF Jamming, GNSS Jamming	Ground-based: Fixed
FLIR Systems	Ranger R8SS-3D	USA	Radar		Ground-based: Fixed
FLIR Systems	Argus	USA	Radar, IR		Ground-based: Fixed
Fortem Technologies	Drone Hunter	USA	Radar	Net	UAV
Fortem Technologies	TrueView R30	USA	Radar		Ground-based: Fixed
Fortem Technologies	TrueView R20	USA	Radar		Ground-based: Fixed
Fortunio	Drone Hunter	Hungary		RF Jamming, GNSS Jamming	Ground-based
Fovea Aero	CCOD	USA		Net	UAV
Fuyuda	Portable Counter Drone Defence System	China		RF Jamming, GNSS Jamming	Ground-based: Mobile
General Atomics	Fencepost	USA	Acoustic		Ground-based: Fixed
General Robotics	PITBULL Ultra Light Remote Weapon Sys- tem (ULRWS)	Israel	Radar, EO, IR	Projectile	Ground-based
GEW Technologies	SkyScan 2	South Africa	RF		Ground-based: Fixed
Gewerbegebiet Aaronia	AARTOS	Germany	RF		Ground-based: Fixed
Gradiant	Counter-UAS by Gradiant	Spain	RF, EO, IR	Spoofing, RF Jam- ming, GNSS Jamming	Ground-based: Fixed
Gradiant	smartHack	Spain	RF	Spoofing	Ground-based: Fixed
Gradiant	smartEar	Spain	RF		Ground-based: Fixed
Gradiant	smartEye	Spain	EO, IR		Ground-based: Fixed
Gradiant	smartJam	Spain		RF Jamming, GNSS Jamming	Ground-based: Fixed
Groupe ADP/DSNA Services	Hologarde	France	Radar, RF, EO, IR		Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Groupe Assman	MTX-8	France		Net	UAV
Groupe Assman/Ma- lou Tech	Drone Interceptor MP200	France		Net	UAV
Gryphon Sensors (SRC)	Skylight	USA	Radar, RF, EO, IR		Ground-based: Fixed
Gryphon Sensors (SRC)	Skylight Mobile	USA	Radar, RF, EO, IR		Ground-based: Mobile
Guangdong Guo-An Intelligent Aviation Company	Anti-Drone Jammer	China		RF Jamming, GNSS Jamming	Handheld
Hanwha Systems	Drone Detection Radar	South Korea	Radar		Ground-based: Fixed
Harp Arge	Drone Savar	Turkey		RF Jamming	Handheld
Hensoldt	SPEXER 2000	Germany	Radar		Ground-based
Hensoldt	SPEXER 500	Germany	Radar		Ground-based
Hensoldt	UK	Germany	Radar, E/O, RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Hensoldt	Xpeller Rapid	Germany	Radar, E/O, RF	RF Jamming, GNSS Jamming	Ground-based: Mobile
Hensoldt	Xpeller Gear	Germany	RF	RF Jamming, GNSS Jamming	Ground-based: Mobile
Hertz Systems	Hawk	Poland	Radar, EO	RF Jamming, GNSS Jamming	Ground-based, Hand- held
HGH Infared Systems	Spynel M	France	IR		Ground-based
HGH Infared Systems	Spynel S	France	IR		Ground-based
HGH Infared Systems	Spynel X	France	IR		Ground-based
Hikvision	Defender Series UAV- D04JAI	China		RF Jamming, GNSS Jamming	Handheld
Hikvision	Defender Series UAV- D04JHI	China		RF Jamming, GNSS Jamming	Handheld
HP Marketing and Consulting	НР 3962 Н	Germany		RF Jamming, GNSS Jamming	Ground-based: Fixed
HP Marketing and Consulting	HP 47	Germany		RF Jamming, GNSS Jamming	Handheld
Hunan NovaSky Elec- tronic Technology	Multi-sensor Anti-UAV Defense System Solution	China	RF, EO	RF Jamming	
IACIT	DRONEBlocker 0100	Brazil	EO, IR, RF, Acoustic, Radar	RF Jamming	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
IACIT	DRONEBlocker 0200	Brazil	EO, IR, RF, Acoustic, Radar	RF Jamming	Ground-based: Fixed
IDS	Black Knight	Italy	Radar, EO (Optional), IR (Optional)	Optional: RF Jam- ming, GNSS Jamming	Ground-based: Fixed
IMI Systems	Red Sky 2 Drone Defender System	Israel	Radar, EO, IR	RF Jamming, GNSS Jamming, Laser (Op- tional)	Ground-based: Fixed
Indra	ARMS	Spain	Radar, RF, EO, IR	RF Jamming, GNSS Jamming, Spoofing	Ground-based: Fixed
Invisible Interdiction	The Ghoul Tool Full Spectrum	USA		RF Jamming, GNSS Jamming	Handheld
Invisible Interdiction	Commercial Hand- held Terminator	USA		RF Jamming, GNSS Jamming	Handheld
Invisible Interdiction	Commercial Termina- tion Module	USA		RF Jamming, GNSS Jamming	Ground-based: Fixed
Invisible Interdiction	Ghoul Tool Short- Range Module	USA		RF Jamming, GNSS Jamming	Ground-based: Fixed
IPB Systems	Drone-Hunter	Spain	Acoustic, RF, EO, IR	RF Jamming, GNSS Jamming, Spoofing	Ground-based: Fixed
Israel Aerospace Industries	POPSTAR	Israel	EO, IR		Ground-based: Fixed
ITHPP	Drone Sniper	France		RF Jamming	Handheld
IXI Technology	Drone Killer	USA		RF Jamming, GNSS Jamming	Handheld
Jammers4u	CT-2065	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	СТ-2065Н	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	СТ-2085Н	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	СТ-1040Н	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	CT-4001P	China		RF Jamming, GNSS Jamming	Handheld
Jammers4u	CT-4002P	China		RF Jamming, GNSS Jamming	Handheld
Jammers4u	CT-3076B-UAV	China		RF Jamming, GNSS Jamming	Handheld
Jammers4u	CT-4035-UAV	China		RF Jamming, GNSS Jamming	Handheld
Jammers4u	CT-3060N-UAV	China		RF Jamming, GNSS Jamming	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Jammers4u	CT-3040-OMN	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	CT-N3076-HGA	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	CT-3076B-HGA	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	CT-5030-UAV	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	CT-5040R-UAV	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	CT-6067-UAV	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	CT-8078AR	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	CT-8078ATW-HGA	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jammers4u	CT-N3060-OMN	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
JCPX	Drone Fighter	France		RF Jamming, GNSS Jamming	Handheld
JCPX Development/ DSNA Services/ Aveillant	UWAS	Monaco	Radar, EO, IR	"Counter measures"	Ground-based: Fixed
Jiangsu Digital Eagle Technology Devel- opment	QR-07S3	China		RF Jamming, GNSS Jamming	Handheld
Jiangsu Digital Eagle Technology Devel- opment	QR-12	China	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Jiangsu Digital Eagle Technology Devel- opment	QR-09	China		RF Jamming	Ground-based: Fixed
Jiangsu Digital Eagle Technology Devel- opment	QR-10	China		RF Jamming, GNSS Jamming	Handheld
Jiangsu Digital Eagle Technology Devel- opment	QR-08	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Jiangsu Digital Eagle Technology Devel- opment	QR-07S SPEC	China		RF Jamming, GNSS Jamming	Handheld
Jiangsu Digital Eagle Technology Devel- opment	QR-07S2 SPEC	China		RF Jamming, GNSS Jamming	Handheld

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Jiun An Technology	Raysun MD1	Taiwan		RF Jamming, GNSS Jamming	Handheld
JSC Concern Radio-Electronic Technologies	Leer-3	Russia		Spoofing, RF Jam- ming, GNSS Jamming	UAV
K9 Electronics	DJ500C	UK		RF Jamming	
K9 Electronics	Terminator 3000	UK		RF Jamming, GNSS Jamming	Handheld
K9 Electronics	DJ500F	UK		RF Jamming, GNSS Jamming	Ground-based: Fixed
Kalashnikov/ZALA Aero Group	REX 1	Russia		RF Jamming, GNSS Jamming	Handheld
Kaspersky	Antidrone	Russia	Laser Scanning	RF Jamming, GNSS Jamming	Ground-based: Fixed
KB Radar Design Bureau	Groza-R2	Belarus		RF Jamming, GNSS Jamming	Handheld
KB Radar Design Bureau	Groza-R	Belarus		RF Jamming, GNSS Jamming	Handheld
KB Radar Design Bureau	Groza-S	Belarus	RF	RF Jamming, GNSS Jamming, Spoofing	Ground-based: Mobile
KB Radar Design Bureau	Groza-Z	Belarus	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Kelvin Hughes	SMS-D	UK	Radar, EO, IR		Ground-based: Fixed
Kineti	GeoDome CDS Go	Netherlands	RF		Ground-based: Fixed
Kineti	GeoDome CDS Advance	Netherlands	RF	RF Jamming	Ground-based: Fixed
Kirintec	Recurve	UK		RF Jamming, GNSS Jamming	Ground-based
Kirintec	Sky Net Longbow	UK		RF Jamming, GNSS Jamming	Ground-based
Kongsberg Geospa- tial/Echodyne/uAvi- onix	Argus CUAS	Canada/USA	Radar, E/O, RF		Ground-based: Fixed
Konsortium Engi- neering Activities & Security (KEAS)	UAS Jammer	France	EO, IR	Jamming	
Kratos Defense & Rocket Support Services	Kratos Tethered UAS	USA	EO, RF		UAV
Kvertus	KVS ANTIDRON-H	Ukraine		RF Jamming, GNSS Jamming	Handheld

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Kvertus	KVS ANTIDRON-M	Ukraine		RF Jamming, GNSS Jamming	Handheld
Kvertus	Veil	Ukraine		RF Jamming, GNSS Jamming	Ground-based: Fixed
Kvertus	Typhoon	Ukraine		RF Jamming, GNSS Jamming	Ground-based: Fixed
Kvertus	KVS ANTIDRON-C	Ukraine		RF Jamming, GNSS Jamming	Ground-based: Fixed
Kvertus	KVS ANTI- DRON-C/M	Ukraine		RF Jamming, GNSS Jamming	Ground-based: Fixed
Kvertus	KVS ANTIDRON-RC	Ukraine		RF Jamming, GNSS Jamming	Ground-based: Fixed
Kvertus	KVS-AD-1	Ukraine	RF		Ground-based: Fixed
Kvertus	FOG X6	Ukraine		RF Jamming, GNSS Jamming	Ground-based: Fixed
Kvertus	MIST	Ukraine		RF Jamming, GNSS Jamming	Ground-based: Fixed
L3Harris Technolo- gies	Drone Guardian	USA	Radar, EO, IR, RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Leidos	Time Integrated Giga- watt Electromagnetic Response (TIGER)	USA		High Power Micro- wave	Ground-based: Fixed
Leonardo DRS	Multi-Mission Hemi- spheric Radar	USA	Radar		Ground-based: Fixed
Leonardo DRS/Moog	Mobile Low, Slow Unmanned Aerial Vehicle Integrated Defense Systems (MLIDS)	USA	Radar	Projectile	Ground-based: Fixed
Leonardo DRS/Moog	SABRE	USA	Radar	Projectile	Ground-based: Mobile
Liteye/Blighter Surveillance Systems/ Chess Dynamics	Counter-UAS Detec- tion and Identification System (ADIS)	USA	Radar, EO, IR		Ground-based: Fixed
Liteye/Blighter Surveillance Systems/ Chess Dynamics/ Enterprise Control Systems	Mobile Anti-UAV Defense System (M-AUDS)	USA/UK	Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Mobile
Liteye/Orbital ATK	T-REX	USA	Radar, EO, IR	RF Jamming, Pro- jectile	Ground-based: Mobile
Lockheed Martin	ADAM	USA	EO, IR	Laser	Ground-based
Lockheed Martin	ATHENA	USA	EO, IR	Laser	Ground-based

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Lockheed Martin	ICARUS	USA	RF, EO, Acoustic	RF Jamming, Spoof- ing	Ground-based
Lockheed Martin	Miniature Hit-to-Kill (MHTK)	USA	Radar	Projectile	Ground-based: Mobile
Lockheed Martin	High Energy Laser and Integrated Opti- cal-dazzler with Sur- veillance (HELIOS)	USA		Laser, Dazzling	Ground-based: Fixed
Lockheed Martin/ Saab/Diehl Defence	Falcon	USA	Radar	Interceptor rockets	Ground-based: Mobile
LocMas	STUPOR	Russia		RF Jamming, GNSS Jamming	Handheld
LX Photon	Drone Jammer	Luxemburg		Jamming	Handheld
LX Photon	Drone Spoofer	Luxemburg		Spoofing	Ground-based: Fixed
LX Photon	Drone Detector	Luxemburg	RF		Ground-based: Fixed
Magna	Detection Solution	Israel	EO, IR, Acoustic	Jamming, Spoofing	Ground-based
Marduk Technologies	Shark	Estonia	EO	Laser	Ground-based
Martek Marine	Marine Anti-Drone System (MADS) Portable	UK	RF, Radar (Optional), EO, IR (Optional)	Optional: RF Jam- ming, GNSS Jam- ming, Spoofing	Ground-based: Mar- itime
Martek Marine	Marine Anti-Drone System (MADS) Fixed	UK	RF, Radar (Optional), EO, IR (Optional)	RF Jamming, Spoof- ing (Optional)	Ground-based: Mar- itime
MBDA Deutschland	High Energy Laser Weapon System	Germany		Laser	Ground-based: Fixed
MC TECH	MC-Horizon	Israel	RF, Radar, EO, IR	RF Jamming	Ground-based: Fixed
MC-CLIC	Anti-UAV Rifle	Monaco		RF Jamming	Handheld
MC2 Technologies	Scrambler 1000	France		RF Jamming	Ground-based: Fixed
MC2 Technologies	Nerod F5	France		RF Jamming	Handheld
MC2 Technologies	Scrambler 300	France		RF Jamming	Handheld
MC2 Technologies	Reconfigurable Jam- ming System	France		RF Jamming	Ground-based: Fixed
Meritis	RTX-300P2/P6	Switzerland		RF Jamming, GNSS Jamming	Handheld
Meritis	RTX-2000M6	Switzerland		RF Jamming, GNSS Jamming	Ground-based: Mobile
Meritis	RTX-3000X	Switzerland		RF Jamming, GNSS Jamming	Ground-based: Fixed
Meritis	SkyCleaner	Switzerland		RF Jamming, GNSS Jamming	Handheld

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Meritis	ADS-2000	Switzerland	Acoustic		Ground-based: Fixed
Meritis	SC-1000T	Switzerland	EO, IR		Ground-based: Fixed
Meritis	SC-1500T	Switzerland	EO, IR		Ground-based: Fixed
Meritis	SR-9000S	Switzerland	Radar		Ground-based: Fixed
METIS Aerospace	SKYPERION	UK	RF, Other		Ground-based: Fixed
Microflown AVISA	SKYSENTRY	Netherlands	Acoustic		Ground-based: Fixed
Mikran	Carnivora	Russia		Net, Ammunition	UAV
Miltronix	Drone Detection Radar	UK	Radar		Ground-based: Mobile
Mitsubishi Electric	Drone Deterrence System	Japan	RF	RF Jamming	Ground-based: Fixed
MyDefence Commu- nication	EAGLE	Denmark	Radar		Ground-based: Fixed
MyDefence Commu- nication	KNOX	Denmark	RF, Radar, EO, IR	Optional: RF Jam- ming, GNSS Jamming	Ground-based: Fixed
MyDefence Commu- nication	WATCHDOG	Denmark	RF		Ground-based
MyDefence Commu- nication	WOLFPACK	Denmark	RF		Ground-based: Fixed
MyDefence Commu- nication	Wingman 100	Denmark	RF		Handheld
MyDefence Commu- nication	Wingman 101	Denmark	RF		Handheld
MyDefence Commu- nication	Wingman 103	Denmark	RF		Handheld
MyDefence Commu- nication	PITBULL	Denmark		RF Jamming, GNSS Jamming	Handheld
MySky Technologies		Australia		Collision Drone	UAV
MySky Technologies		Australia	Machine Learning		Ground-based: Fixed
Nammo		Norway		Programmable ammu- nition	
NEC		Japan	EO, IR		Ground-based: Fixed
Necom Telecommuni- cation Technologies	DJ200	China		RF Jamming, GNSS Jamming	Handheld
Necom Telecommuni- cation Technologies	DJ100	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Necom Telecommuni- cation Technologies	CPJX6105UAV	China		RF Jamming, GNSS Jamming	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Netline Communica- tions	C-GUARD DRONENET	Israel		RF Jamming	Ground-based: Fixed
Netline Communica- tions	WOODPECKER LIGHT	Israel	RF		Ground-based: Fixed
New Telecommunica- tion Technologies	Harpoon-2M	Russia		RF Jamming, GNSS Jamming	Handheld
NNIIRT	1L121-E	Russia	Radar		Ground-based: Mobile
Northrop Grumman	Joint Counter Radio-Controlled Improvised Explosive Device Electronic Warfare (JCREW)	USA		RF Jamming	Handheld
Northrop Grumman	Mobile Application for UAS Identification (MAUI)	USA	Acoustic		Handheld
Northrop Grumman	Drone Restricted Access Using Known EW (DRAKE)	USA		RF Jamming	Ground-based
Northrop Grumman	Mobile Application for UAS Identification	USA	Acoustic		Handheld
Northrop Grumman	Venom	USA	Laser Designator		Ground-based: Mobile
OpenWorks Engi- neering	Skywall 100	UK		Net	Handheld
OpenWorks Engi- neering	Skywall 200	UK		Net	Handheld
OpenWorks Engi- neering	Skywall 300	UK		Net	Ground-based: Fixed
OpenWorks Engi- neering	SkyWall Auto Re- sponse	USA		Net	Ground-based: Mobile
Optix	Anti-Drone	Bulgaria		RF Jamming, GNSS Jamming	Handheld
Orad	DROM	Israel	RF	RF Jamming	Ground-based: Fixed
Orelia	Drone Detector	France	Acoustic	RF Jamming	Ground-based: Fixed
Panasonic	Drone Finder	Japan	Acoustic, EO		Ground-based: Fixed
Patria	MUSCL	Finland	Radar		Ground-based
PDA Electronics	Repulse 24	UK		RF Jamming	Ground-based: Mobile
PDA Electronics	Repulse 2458E	UK		RF Jamming	Ground-based: Mobile
PDA Electronics	Repulse 2458H Handheld	UK		RF Jamming	Handheld
PDA Electronics	Repulse 360	UK		RF Jamming	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
PDA Electronics	Repulse 160	UK		RF Jamming	Ground-based: Mobile
PDA Electronics	Spi-24	UK	RF		Ground-based: Mobile
Phantom Technolo- gies	Eagle108 Tactial Drone Jammer	Israel	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Phantom Technolo- gies	Phantom Dome	Israel	Radar, EO, IR, RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Poly Technologies	Silent Hunter	China	EO, IR	Laser	Ground-based: Mobile
Poly Technologies	LANU-M1	China		RF Jamming, GNSS Jamming	Ground-based: Mobile
Prime Consulting & Technologies	GROK Jammer	Denmark		RF Jamming, GNSS Jamming	Ground-based: Fixed
Prime Consulting & Technologies	GROK Mobile Gun	Denmark		RF Jamming, GNSS Jamming	Handheld
Prime Consulting & Technologies	Mini-range count- er-UAV system	Denmark	EO, IR		Ground-based: Fixed
Prime Consulting & Technologies	Small-range count- er-UAV system	Denmark	Radar, EO, IR		Ground-based: Fixed
Prime Consulting & Technologies	GROK X-band drone detection radar	Denmark	Radar		Ground-based: Fixed
Prime Consulting & Technologies	GROK Ku-band drone detection radar	Denmark	Radar		Ground-based: Fixed
Prime Consulting & Technologies	Medium-range count- er-UAV system	Denmark	Radar, EO, IR		Ground-based: Fixed
Prime Consulting & Technologies	Long-range count- er-UAV system	Denmark	Radar, EO, IR, RF		Ground-based: Fixed
Proximus	Bukovel Mini-FX	Ukraine	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Proximus	Bukovel	Ukraine	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
QiLing UAV	Air Guard-200	China	RF, Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Fixed
QinetiQ	OBSIDIAN	UK	Radar		Ground-based: Fixed
Quantum Aviation	DroneProtect	UK	RF, EO, IR, Radar		Ground-based: Fixed
Quantum Technology Sciences	Vector QA-100 SADAR	USA	Seismic Acoustic De- tection and Ranging		Ground-based: Fixed
RADA Electronic Industries	MHR	Israel	Radar		Ground-based: Mobile
RADA Electronic Industries	RPS-42	Israel	Radar		Ground-based: Fixed
RADA Electronic Industries	ieMHR	Israel	Radar		Ground-based

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
RADA Electronic Industries	xrMHR	Israel	Radar		Ground-based
RADA Electronic Industries	eCHR	Israel	Radar		Ground-based
Rafael Advanced Defense Systems	I-Dome	Israel	Radar	Projectile	Ground-based: Mobile
Rafael Advanced Defense Systems	Drone Dome	Israel	Radar, EO, IR, RF	RF Jamming, GNSS Jamming, Laser	Ground-based: Fixed
Rajant	MANET	USA		Swarming	UAV
Raytheon	MRZR	USA	EO, IR	Laser	Ground-based: Mobile
Raytheon	Phaser	USA	EO, IR	High Power Micro- wave	Ground-based: Fixed
Raytheon	Coyote	USA		Explosive Collision Drone	UAV
Raytheon	High Energy Laser	USA		Laser	Ground-based: Fixed
Raytheon	KuRFS	USA	Radar		Ground-based, Mobile
Raytheon	Howler	USA	Radar, RF	Explosive Collision Drone	Ground-based, UAV
Raytheon	Skyler	USA	Radar		Ground-based: Fixed
Raytheon	Windshear	USA	Radar, RF, Acoustic, EO, IR	Optional: Spoofing, RF Jamming, GNSS Jamming, High Power Microwave	Ground-based: Fixed
Remote Sensing Technologies	UAV Detection Radar	Turkey	Radar		Ground-based
Rheinmetall	"Jammer"	Germany		RF Jamming, GNSS Jamming	Ground-based: Fixed
Rheinmetall	Radshield	Germany	EO, IR, Radar		Ground-based: Fixed
Rheinmetall	HEL Effector Wheel XX	Germany	Radar	Laser	Ground-based
Rinicom	Sky Patriot	UK	EO,IR		Ground-based
Robin Radar Systems	Elvira	Netherlands	Radar		Ground-based: Fixed
Robodub	N/A	USA		UAV	UAV
RoboTiCan	Goshawk	Israel		Collision Drone	UAV
Rohde & Schwarz	ARDRONIS-I	Germany	RF		Ground-based: Fixed
Rohde & Schwarz	ARDRONIS-D	Germany	RF		Ground-based: Fixed
Rohde & Schwarz	ARDRONIS-R	Germany	RF	RF Jamming	Ground-based: Fixed
Rohde & Schwarz	ARDRONIS-P	Germany	RF	RF Jamming	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Rohde & Schwarz	ARDN-WF	Germany	RF	RF Jamming	Ground-based: Fixed
Rohde & Schwarz/ ESG/Diehl	Guardion	Germany	Radar, RF, EO, IR	RF Jamming, GNSS Jamming	Ground-based
Roketsan	Alka	Turkey	Radar, EO, IR	Laser, Electromagnet- ic pulse	Ground-based: Fixed
Ruseletronics		Russia	Radar		Handheld
Saab Group	Giraffe 1x	Sweden	Radar		Ground-based: Mobile
Samjung Solution	Anti-Drone Gun (안 티드론건)	South Korea		RF Jamming, GNSS Jamming	Handheld
SC Scientific and Technical Center of Electronic Warfare	Repellent-1	Russia	RF	RF Jamming	Ground-based: Mobile
SCG/Van Cleve & Associates	DroneRANGER	Switzerland	Radar	RF Jamming	Ground-based: Fixed
SCI Technology	AeroGuard	USA		Net	UAV
SDT Space and De- fense Technologies	Avci	Turkey	Radar, RF, EO, IR, Acoustic	RF Jamming, GNSS Jamming	Ground-based: Fixed
Search Systems	Sparrowhawk	UK		Net	UAV
Sensing Products	Osprey Air	Australia	Radar		Ground-based
Sensofusion	Airfence	Finland	RF		Ground-based: Fixed
SESP Group	Drone Defeater	UK	EO, IR, RF	RF Jamming	Ground-based: Mobile
SESP Group	Drone Defeater	UK	RF, EO, IR	RF Jamming	Ground-based
Shen Zhou Ming Da High Technology	DZ 03	China		RF Jamming, GNSS Jamming	Handheld
Shen Zhou Ming Da High Technology	DZDF-3A4D	China	RF		Ground-based: Fixed
Shen Zhou Ming Da High Technology	LionPAR E500-1011C	China	Radar		Ground-based: Fixed
Shen Zhou Ming Da High Technology	LionPAR E500-1014C	China	Radar		Ground-based: Fixed
Shen Zhou Ming Da High Technology	LionPAR E3000- 2164C	China	Radar		Ground-based: Fixed
Shen Zhou Ming Da High Technology	DZ-OF1	China	EO, IR		Ground-based: Fixed
Shen Zhou Ming Da High Technology	DZ-DN1	China		RF Jamming, GNSS Jamming	Ground-based: Fixed
Shen Zhou Ming Da High Technology	DZ-02 Pro	China		RF Jamming, GNSS Jamming	Handheld

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Shenzhen Jeair Avia- tion Technology	JA-CD01	China		RF Jamming, GNSS Jamming	Handheld
Shenzhen Jeair Avia- tion Technology	JA-CD02	China	RF		Ground-based
Shenzhen Jeair Avia- tion Technology	JA-F01	China	Radar		Ground-based: Fixed
Shenzhen Sharphy Electronic	Portable Shield Shape Jammer	China		RF Jamming, GNSS Jamming	
Sierra Nevada Corpo- ration	SkyCAP	USA		RF Jamming	Handheld, Ground- based
Sierra Nevada Corpo- ration/RADA/Ascent Vision Technologies	eXpeditionary Mobile Air Defense Integrat- ed System (X-MAD- IS) FS	USA/Israel	Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Fixed
Sierra Nevada Corpo- ration/RADA/Ascent Vision Technologies	X-MADIS Mobile	USA/Israel	Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Mobile
Sierra Nevada Corpo- ration/RADA/Ascent Vision Technologies	X-MADIS OTM	USA/Israel	Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Mobile
Signal Systems Cor- poration	Three Dimensional Acoustic Sensing Unit (3DASU)	USA	Acoustic		Ground-based: Fixed
Silent Sentinel	Counter UAV/UAS Platform	UK	Radar, EO, IR, Illumi- nators	RF Jamming, GNSS Jamming	Ground-based: Fixed
SkyCope	SkyCope	Canada	RF	RF Jamming	Ground-based
SkyLock	SkyLock	Israel	Optional: Radar, EO, IR, RF	RF Jamming, GNSS Jamming, Laser (Op- tional)	Ground-based, Mobile
SkyLock	Safe Skies	Israel	Radar		Airborne
SkyLock	360° Drone Detection Radar	Israel	Radar		Ground-based: Fixed
SkyLock	360° RF Drone Detec- tion System	Israel	RF		Ground-based: Fixed
SkyLock	RF Anti-drone jammer	Israel		RF Jamming, GNSS Jamming	Ground-based: Fixed
SkyLock	KNIGHT`S DOME	Israel		RF Jamming, GNSS Jamming	Handheld
SkyLock	Counter Drone Net Catcher	Israel		Net	UAV
SkyLock	Counter Drone Laser Burner	Israel		Laser	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
SkyLock	ULRWS	Israel		Projectile	Ground-based
SkySafe	Skysafe	USA	RF	Spoofing, RF Jam- ming, GNSS Jamming	Handheld
Skysec	Sentinel Catch	Switzerland		Net	UAV
Skysec	Sentinel Catch&Carry	Switzerland		Net	UAV
Smart Shooter	SMASH 2000	Israel		Rifle Fire Control	Handheld
SmartRounds	Smart Anti-Vehicle Aerial Guided En- gagement (SAVAGE)	USA		Projectile	Ground-based: Fixed or UAV
Snake River Shooting	Drone Munition	USA		Projectile	Handheld
Sohgo Security Services		Japan	Acoustic		Ground-based: Fixed
Sozvezdie	Borisoglebsk 2	Russia	RF	RF Jamming, GNSS Jamming	Ground-based, Mobile
Sozvezdie Concern (Rostec)	Solaris-N	Russia	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
SpotterRF	A-150	USA	Radar		Ground-based: Fixed
SpotterRF	A-600	USA	Radar		Ground-based: Fixed
SpotterRF	A-3000	USA	Radar		Ground-based: Fixed
SpotterRF	A-2000	USA	Radar		Ground-based: Fixed
SpotterRF	3D-500	USA	Radar		Ground-based: Fixed
Squarehead	Discovair G2	Norway	Acoustic		Ground-based: Fixed
SRC	Silent Archer	USA	Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Mobile
ST Engineering	SkyArcher	Singapore	RF, EO	Spoofing	Ground-based
ST Kinetics	C-UAS Grenade	Singapore		Projectile	Ground-based
Star Defence Logis- tics & Engineering	Estrella	Spain		RF Jamming, GNSS Jamming	Handheld
SteelRock Technol- ogies	Odin Xpeller	UK	RF	RF Jamming, GNSS Jamming, Spoofing	Ground-based: Fixed
SteelRock Technol- ogies	NightFighter	UK		RF Jamming, GNSS Jamming	Handheld
SteelRock Technol- ogies	NightFighter L	UK		RF Jamming, GNSS Jamming	Handheld
SteelRock Technol- ogies	NightFighter X	UK		RF Jamming, GNSS Jamming	Handheld
System Drone/Em- bention		Spain		Spoofing	UAV

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
SYT technologies	XMR	France	EO, IR		Ground-based
Tarsier	Tarsier	USA	EO, IR		Ground-based
Tayyar Systems	Sa'aq Gun (SG3)	Oman		RF Jamming, GNSS Jamming	Handheld
Tayyar Systems	Sa'aq Gun (SG2)	Oman		RF Jamming, GNSS Jamming	Handheld
TCI	Blackbird	USA	RF		Ground-based
Technology Service	Aquila Seeker	USA	RF	Collision Drone	UAV
Technology Service	Tactical Expeditionary Mobile Protection Radar (TEMPR)	USA	Radar		Ground-based: Mobile
TeleRadio Engineer- ing	SkyDroner 1000	Singapore	EO, Other		Ground-based: Fixed
TeleRadio Engineer- ing	SkyDroner 500	Singapore	EO, Other		Ground-based: Fixed
Terra Hexen	DBS	Poland		RF Jamming, GNSS Jamming	Ground-based
Terra Hexen	SAFESKY	Poland	Radar, EO, Acoustic	RF Jamming, GNSS Jamming	Ground-based
Terra Hexen	Unidirectional Neu- tralizer	Poland		RF Jamming, GNSS Jamming	Handheld
Textron Systems	StrongArm	USA		RF Jamming, GNSS Jamming	Ground-based, Hand- held
Thales	Gecko	France	IR		Ground-based: Fixed
Thales	Margot 8000	France	EO, IR		Ground-based: Fixed
Thales	Squire	France	Radar		Ground-based: Fixed
Thales	Horus Captor	Spain	Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based: Fixed
Thales	Gecko M	France	IR		Ground-based: Mobile
Thales/Raytheon	"AN/MPQ-64F1 Improved Sentinel"	France	Radar		Ground-based: Fixed
Theiss UAV Solutions	Excipio Aerial Netting System	USA		Net	UAV
ThirdEye Systems	Meduza	Israel	Radar, EO, IR		Ground-based: Fixed
Tianjin Rongfei Intel- ligent Technology	Tri-band Anti drone Rifle	China		RF Jamming, GNSS Jamming	Handheld
Torrey Pines Logic	Beam 220	USA	EO, IR (Optional)		Ground-based
Toshiba	Drone Detection System	Japan	RF, EO		Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
TRD Consultancy	Orion-7 ++	Singapore		RF Jamming, GNSS Jamming	Handheld
TRD Consultancy	Orion-H Drone Slayer	Singapore		RF Jamming, GNSS Jamming	Handheld
TRD Consultancy	Orion-D	Singapore	RF		Handheld
TRD Consultancy	Orion-9	Singapore		RF Jamming, GNSS Jamming	Handheld
TRD Consultancy	Orion-V	Singapore	RF		Ground-based: Mobile
TRD Consultancy	Orion-T	Singapore		RF Jamming, GNSS Jamming	Handheld
TRD Consultancy	Orion-B	Singapore		RF Jamming, GNSS Jamming	Ground-based: Mobile
TRD Consultancy	Orion	Singapore	RF, Radar, EO, IR	RF Jamming, GNSS Jamming	Ground-based, Hand- held
TrustComs	DroneBlocker	France	TBA	TBA	Ground-based: Fixed
UAVOS	Interception System	Hong Kong		Net	UAV
Ukroboronprom	Suricatta	Ukraine	RF	RF Jamming, GNSS Jamming	Ground-based
UkrSpecTechnika	Anklav	Ukraine		GNSS Jamming	Ground-based: Fixed
Unknown	Valdai	Russia	RF	RF Jamming, GNSS Jamming	Ground-based: Fixed
Van Cleve & Asso- ciates	cSENTRY	USA	Radar, EO, IR	Dazzling	Ground-based: Fixed
Vector Solutions	Artemis	USA	RF	Spoofing	Ground-based
Version2	Portable Drone Sentry	Canada	RF		Ground-based: Mobile
Version2	V2 Sentry	Canada	RF		Ground-based: Fixed
Verus Technology Group	SkyView-DI	USA	RF		Ground-based: Fixed
Verus Technology Group	SkyView-MP	USA	RF		Ground-based: Mobile
Vigilant Drone Defense	DDU-1	USA	RF		Ground-based
Vigilant Drone Defense	DD-SP1	USA		RF Jamming	Ground-based: Mobile
Vigilant Drone Defense	HH-SP1	USA		RF Jamming	Handheld
Vigilant Drone Defense	DD-SP160	USA		RF Jamming	Ground-based: Fixed

Company Name	Product Name	Country of Origin	Detection	Interdiction	Platform
Vigilant Drone Defense	DD-SP360	USA		RF Jamming	Ground-based: Fixed
Vigilant Drone Defense	LRP-1	USA		RF Jamming	Handheld
Vigilant Drone Defense	LRP-2	USA		RF Jamming	Ground-based: Fixed
Vigilant Drone Defense	LRY-2	USA		RF Jamming	Ground-based: Fixed
Vorpal	VigilAir Drone	Israel	RF		UAV
Vorpal	VigilAir	Israel	RF		Ground-based: Fixed
Vorpal	VigilAir Extract & Control	Israel	RF	Spoofing	Ground-based: Fixed
WhiteFox Defense	Dronefox Fortify	USA	RF	Spoofing	Ground-based: Fixed
WhiteFox Defense	Dronefox Tactical	USA	RF	Spoofing	Ground-based: Mobile
WhiteFox Defense	Scorpion	USA	RF	Jamming	Handheld
ZALA Aero Group	Zont	Russia		GNSS Jamming	Handheld

