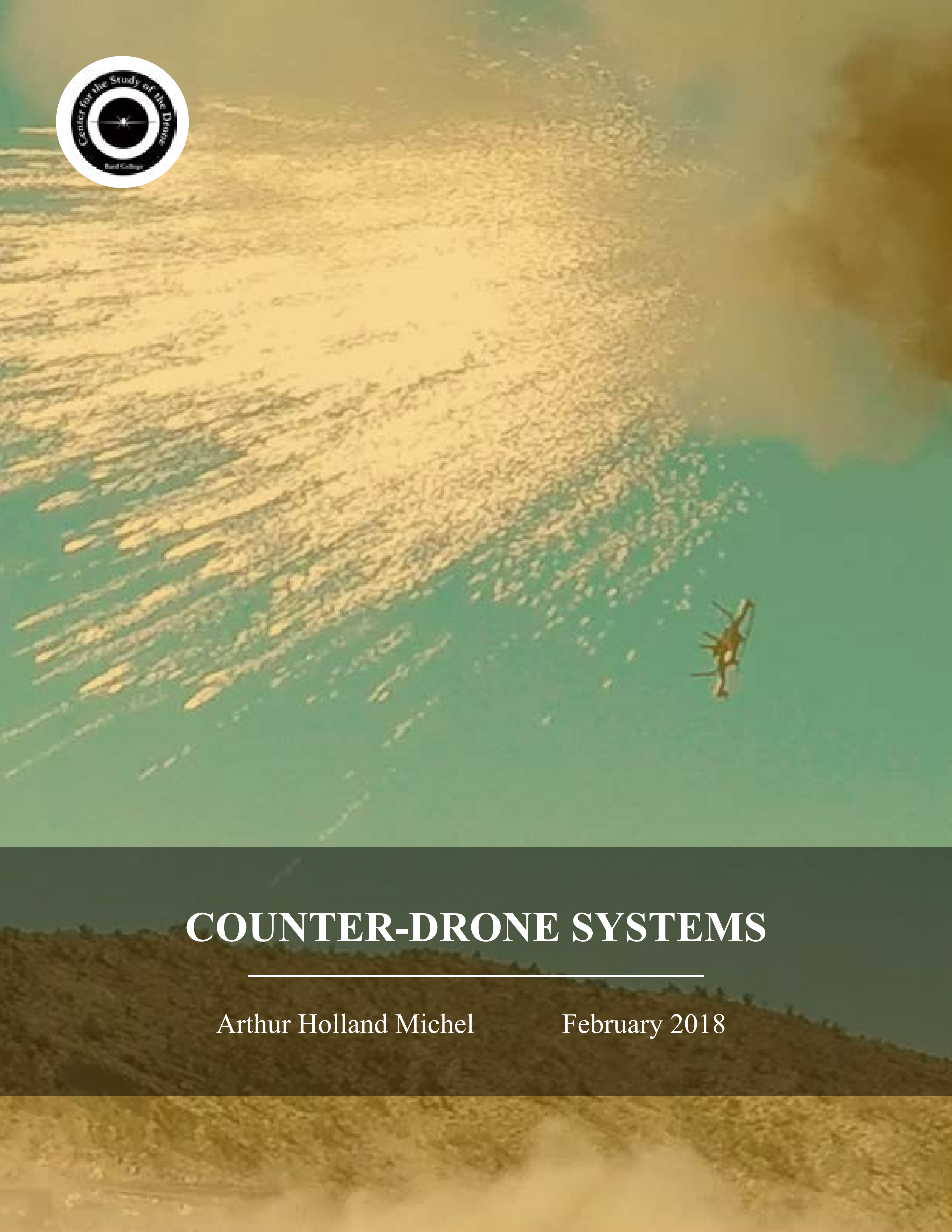
Center for the Study of the Drone
Bard College



COUNTER-DRONE SYSTEMS

Arthur Holland Michel

February 2018

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.

Edited by Dan Gettinger. Editorial support provided by Karin Roslund. Research support provided by Aasiyah Ali, Lynn Barnett, Dylan Sparks, Josh Kim, and John McKeon. Presentation by Dan Gettinger.

Michael Blades, Senior Industry Analyst, Frost & Sullivan, provided assistance in the development of this database. Frost & Sullivan's market reports on C-UAS technology are available for purchase here (defense) and here (commercial).

Holland Michel, Arthur. "Counter-Drone Systems." Center for the Study of the Drone at Bard College, Feburary 20, 2018, http://dronecenter.bard.edu/counter-drone-systems/.

INTRODUCTION

Counter-drone technology, also known as counter-UAS, C-UAS, or counter-UAV technology, refers to systems that are used to detect and/or intercept unmanned aircraft. As concerns grow around the potential security threats drones may pose to both civilian and military entities, a new market for counter-drone technology is rapidly emerging. To date, we have found at least 235 counter-drone products either on the market or under active development. This report provides background on the growing demand for C-UAS technology, describes how the technology works, presents our database of known C-UAS systems from around the globe, and explains some of the challenges surrounding counter-drone technology use.

KEY TAKEAWAYS

- The C-UAS industry has grown exponentially in recent years. We have identified over 230 C-UAS products produced by 155 manufacturers in 33 countries;
- The most popular drone detection techniques are radar, RF detection, EO, and IR. The most popular interdiction technique is jamming;
- C-UAS technology poses a wide range of practical, legal, and policy challenges in all operating environments;
- A lack of common standards in the C-UAS industry means that there is a wide variance in the effectiveness and reliability of systems.

BACKGROUND

Military groups have pondered the issue of how to counter unmanned aircraft for several years. For example, in 2003, NATO launched a ten-year study on how to defend against low, slow, and small aerial targets using ground-based defense systems (the resulting report has not been publicly released). In 2008, RAND Corporation published a seminal report on the threat posed by unmanned aircraft to the U.S., which helped define the contours of the topic.[1] In the ensuing years, a wide range of organizations, labs, and private firms have weighed in on the threat of unmanned aircraft and what to do about it.

The growth of C-UAS technology is directly tied to mounting concerns about the threat that drones pose both 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. In the conflict in Syria and Iraq, at least half a dozen groups operate a wide variety of drones, which give even the most poorly funded actors an aerial command of the battlespace that can prove decisive in engagements.[2] For example, ISIS has used drones to help guide vehicle-borne IEDs more accurately toward their targets. Some of these same groups have successfully armed drones with explosive ordnance, effectively converting cheap hobby kits into rudimentary yet potentially lethal guided missiles. Last year, ISIS claimed to have carried out more than 200 such attacks in just 12 months.[3] In January, an unknown group launched over a dozen such drones in a coordinated attack against two Russian military installations in Syria.[4] Though the offensive was ultimately unsuccessful, it demonstrated the growing sophistication of the unmanned aircraft that are increasingly finding their way into war zones across the globe. Even when these attacks are unsuccessful, they still create serious challenges for belligerents on the ground and in the air; there are so many drones operating in the conflict in Syria and Iraq that one Army official even said that the U.S. has no control of the airspace below 3,500 feet in the area.[5] The conflict in Ukraine is another important case study on the impact of small unmanned aircraft in modern warfare.[6]

A still from an ISIS promotional video shows an armed Skywalker X-8 fixed-wing drone.

Many worry that similar drones could be used in terrorist attacks domestically.[7] In 2013, Germany's Pirate Party flew a small multirotor drone in close proximity to Angela Merkel at an open-air rally, leading many to speculate about the ease with which a drone could attack an otherwise highly secured area.[8] Sightings of drones over sensitive facilities such as a submarine base in Washington State[9] and nuclear facilities in France[10] have raised the specter state- and non-state-sponsored espionage. Other concerns are no longer hypothetical. Around the globe, drones have become a popular tool for smuggling contraband into prisons. Meanwhile, near misses between drones and manned aircraft have become a common occurrence in every crowded airspace system in the world, and many worry that a collision between a manned aircraft and an unmanned aircraft could result in a catastrophic accident.[11]

The air defense systems that have traditionally been used to protect airspace from manned aircraft are generally ineffective against drones. Military anti-aircraft radars are mostly designed to detect large, fast moving objects. As a result, they cannot always pick up small, slow, low-flying drones. Furthermore, since unmanned aircraft are cheap, it is impractical to use traditional anti-aircraft weapons, which can cost hundreds of thousands of dollars per unit, to shoot them down. 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 missile attack from an Israeli fighter jet. In civilian airspace, drones aren't 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.

C-UAS PRODUCTS AT-A-GLANCE

Number of C-UAS products	235
Number of manufacturers	155
Systems capable of detection only	88
Systems capable of interdiction only	80
Of both detection and interdiction	67

(Above) An Immersion Vortex 250 drone is downed by a water cannon at the 2016 AFRL Commander's Challenge, a counter-UAS exercise. Photo by Wesley Farnsworth.

MARKET GROWTH

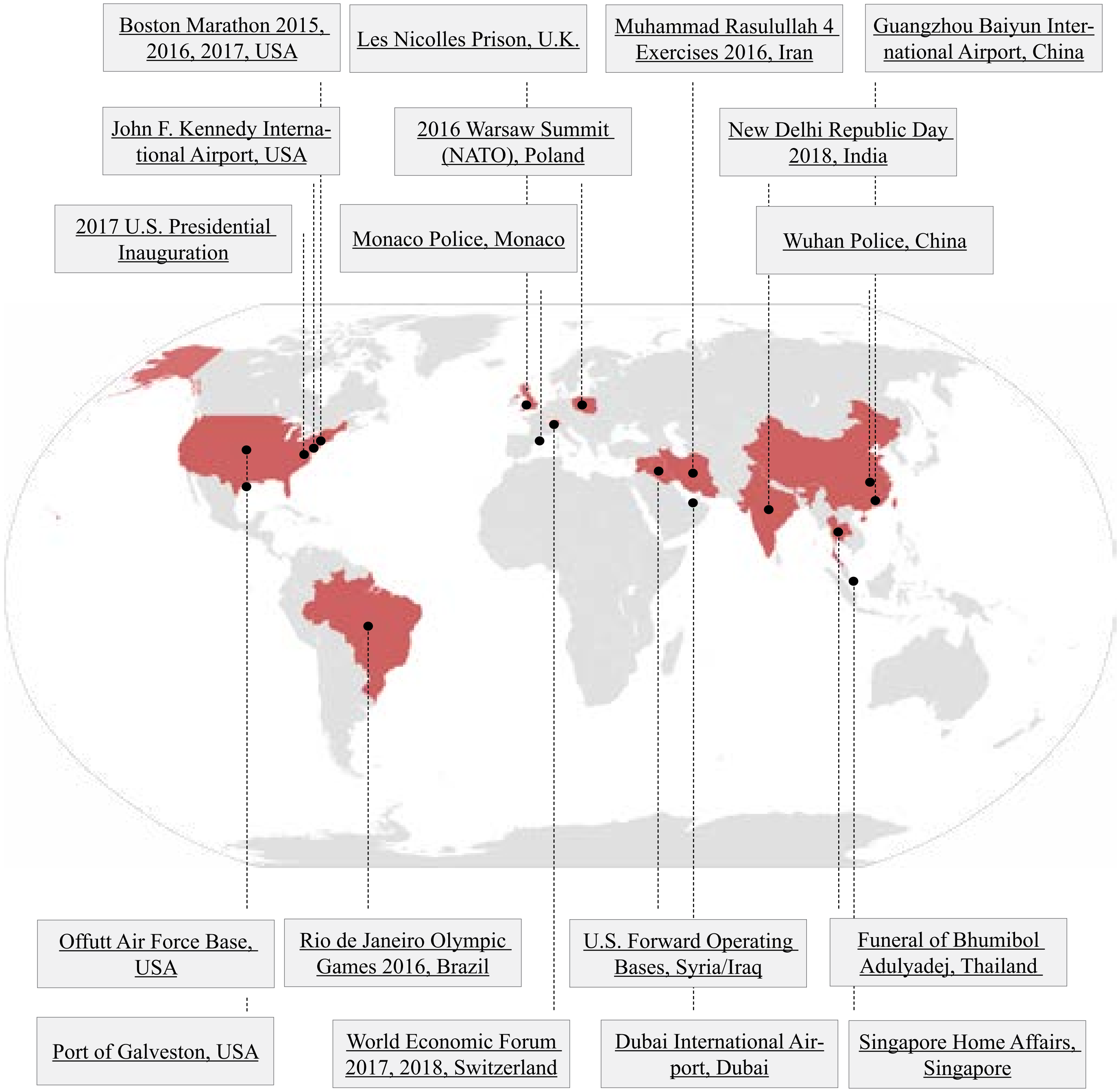
The growth in the counter-drone technology sector is directly correlated to these concerns. The U.S. Department of Defense significantly increased investment in C-UAS technology only after ISIS and other groups operating in the conflict in Syria and Iraq demonstrated the ability to operate a wide range of drones, including armed systems. In 2015, after a man accidentally crashed a DJI quadcopter on the grounds of the White House, revealing that the nation's most protected site could be vulnerable to attacks from unmanned aircraft, the Secret Service began testing C-UAS systems and techniques in D.C.[13] Following hundreds of reports of close encounters between drones and manned aircraft in the U.S. airspace system, the FAA launched a program to test C-UAS at a number of airports, where such incidents are both most common and most dangerous.[14] After law enforcement groups raised the possibility that drones could be an effective weapon for terrorist attacks on large crowds, counter-drone systems began to appear around sporting and political events with increasing regularity.

The expansion of the sector in the roughly five years since counter-drone systems first appeared on the market has been stratospheric. In a market survey conducted in 2015, researchers at the Sandia National Laboratories identified just 10 dedicated counter-drone systems available for acquisition.[15] Today, less than three years later, we have tallied over 200 systems on the market. Venture capital firms have also taken an interest in the sector, and counter-drone technology acquisition and development is now the fastest-growing drone-related spending category in this year's Department of Defense budget.[16] One study estimates that the C-UAS market could be worth as much as $1.5 billion in five years.[17]

HOW C-UAS IS USED

Counter-drone technology has already seen extensive use in certain applications. On the battlefield, C-UAS systems have so far most commonly been used for base protection, complementing existing weapons such as counter-mortar systems and surveillance platforms. There is also growing interest in portable and mobile systems that could be used to protect ground units and convoys. In civilian environments, counter-drone technology has so far primarily been used for airspace protection at airports, security during large events such as party conventions and sports games, VIP protection, and counter-smuggling operations at prisons.[18] Future common applications could include airspace defense around sensitive facilities, port security, maritime security, and personal use over private property.

EXAMPLE USE CASES


Boston Marathon 2015, 2016, 2017, USA
Les Nicolles Prison, U.K.
Muhammad Rasulullah 4 Exercises 2016, Iran
Guangzhou Baiyun International Airport, China
John F. Kennedy International Airport, USA
2016 Warsaw Summit (NATO), Poland
New Delhi Republic Day 2018, India
2017 U.S. Presidential Inauguration
Monaco Police, Monaco
Wuhan Police, China
Offutt Air Force Base, USA
Rio de Janeiro Olympic Games 2016, Brazil
U.S. Forward Operating Bases, Syria/Iraq
Funeral of Bhumibol Adulyadej, Thailand
Port of Galveston, USA
World Economic Forum 2017, 2018, Switzerland
Dubai International Airport, Dubai
Singapore Home Affairs, Singapore

C-UAS 101

Different C-UAS systems rely on a variety of techniques for detecting and/or intercepting drones. This page describes the main detection and interdiction methods employed by products currently available on the market.

Detection amd Tracking Systems

Radar	Detects the presence of small unmanned aircraft by their radar signature, which is generated when the aircraft encounters RF pulses emitted by the detection element.[19] These systems often employ algorithms to distinguish between drones and other small, low-flying objects, such as birds.
Radio-frequency (RF)	Identifies the presence of drones by scanning for the frequencies on which most drones are known to operate. Algorithms pick out and geo-locate RF-emitting devices in the area that are likely to be drones.
Electro-Optical (EO)	Detects drones based on their visual signature.
Infrared (IR)	Detects 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 capability. For example, a system might include an acoustic sensor that cues an optical camera when it detects a potential drone in the vicinity. The use of multiple detection elements may also be intended to increase the probability of a successful detection, given that no individual detection method is entirely failproof.

Interdiction

RF Jamming	Disrupts the radio frequency link between the drone and its operator by generating large volumes of RF output. Once the RF link, which can include WiFi links, is severed, a drone will 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 navigation. Drones that lose their satellite link will hover in place, land, or return to home.
Spoofing	Allows one to take control of the targeted drone by hijacking the drone’s communications link. (Also known as protocol manipulation.)
Laser	Destroys vital segments of the drone’s airframe using directed energy, causing it to crash to the ground.
Nets	Designed to entangle the targeted drone and/or its rotors.
Projectile	Employs regular or custom-designed ammunition to destroy incoming unmanned aircraft.
Combined Interdiction Elements	A number of C-UAS systems also employ a combination of interdiction elements—most commonly, RF and GNSS jamming systems that work in tandem.

Platform Types

Ground-based	Systems designed to be used from either stationary or mobile positions on the ground. This category includes systems installed on fixed sites, mobile systems, and systems mounted on ground vehicles.
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, which can come into proximity with the targeted unmanned aircraft in order to employ interdiction elements at close range.

DATABASE OF PRODUCTS

We have assembled a comprehensive database of publicly known counter-drone systems. The database consists of 235 products sold by 155 firms and partnerships from 33 different countries. This list includes both systems that are on the market and systems that are in active development, as well as existing products designed for other purposes (such as Doppler radars) that have been retooled for C-UAS. Products that could be used for counter-drone operations but are not strictly designed and/or marketed as such (for example, the Iron Dome missile defense system) are not included in the list (see insert on page 8). The database reflects features of each system as described by the manufacturer or, in cases where no manufacturer information is available, by reliable media sources. Some of the systems listed in the database consist of products developed by multiple manufacturers that have been combined into a single integrated product. In cases where individual elements of those combined products are marketed separately, they are also included in the database as standalone products. *The full database can be found on page 11.*

KEY ANALYSIS POINTS

- Eighty eight of the products in the database are designed only for detection, while 80 systems are designed only for interdiction.
- At least sixty seven systems are advertised as being capable of both detection and interdiction.
- A majority of the systems, 177 in total, are designed for ground-based use. Thirty five systems are designed to be handheld, and 18 systems are mounted aboard a drone. Two systems consist of a combination of ground-based and handheld elements, while one system consists of a combination of ground-based and drone-based elements. Two products consist of projectiles designed specifically for C-UAS, and are therefore platform agnostic.
- Of the 155 systems that are capable of detection, 95 appear to employ a single sensor type, while at least 60 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). Sixteen systems employ a combination of four or five different sensor types.
- Roughly an equal number of systems (approximately 60) employ radar, RF detection, and EO sensors. Fifty three employ IR, while 21 systems employ an acoustic sensor.

The AUDS Counter-UAS system. Photo by Blighter.

- About half of the 147 systems capable of interdiction rely on a single technique and half 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 among systems: 88 systems depend on some form of signal jamming alone, while an additional eight systems employ jamming along with another technique. Approximately 30 systems rely solely on kinetic means to intercept and destroy targeted unmanned aircraft, while five systems feature both jamming and kinetic elements. Twelve systems have a spoofing capability.

C-UAS INTERDICTION METHODS

Jamming (RF, GNSS, or Both)	96
Net	18
Spoofing	12
Laser	12
Machine Gun	3
Electromagnetic Pulse	2
Water Projector	1
Sacrificial Collision Drone	1
Other	6

Note: many products employ more than one interdiction technique.

CHALLENGES

Counter-drone systems are not without their challenges at the level of performance, practicality, legality, and policy. These issues are important to consider for both groups hoping to use the technology as well as those seeking to establish the role that the technology could play in the broader integration of drones into the airspace system.

Detection Effectiveness

Every detection system has drawbacks. Since consumer drones are small and tend to fly at low altitudes, they can be hard to detect by radar. Electro-optical systems can only operate during daytime, and might confuse a drone with a bird or an airplane (combining these sensors with other elements may help mitigate this problem). EO and IR systems, as well as certain RF systems, must have a direct line of sight with the intruding drone.

Acoustic sensors rely on a library of sounds emitted by known drones, and might therefore be deaf to drones not covered by the library. RF detection systems likewise only detect certain frequency bands in a library that needs to be regularly updated, and may also be less effective if a drone is not operating within direct line of sight of the sensor. 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. Systems that aren't sensitive enough might generate false negatives, which is even less desirable from the operator's standpoint.

Distinguishing Legitimate and Illegitimate Drone Use

In future operating environments where legitimate drone use is common, C-UAS system may need to be capable of differentiating between legitimate and potentially threatening 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; an effective C-UAS system must be able to tell the difference between those drones and a single rogue drone that is operating with malicious intent. At present, there are no commercially available C-UAS systems that are capable of differentiating between peaceful and malicious drone use. 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.

Interdiction Hazards

The most obvious drawback of kinetic counter-drone systems is that they are dangerous. Drones that have their flight interrupted by physical means will fall to the ground at considerable speed. Even certain net-based systems that are equipped with a parachute that is intended to bring the ensnared drone down to the ground in a controlled manner are risky. As such, kinetic interdic-

The U.S. Defense Advanced Research Projects Agency's Aerial Dragnet program seeks to develop networks of tethered drones that can detect and track every small unmanned aircraft operating within a large coverage area, such as a whole city. Initially, such a system would be used in active battlefield environments, but the agency has suggested that the same technology could also be used for unmanned aircraft traffic management domestically.

tion systems are likely to be inappropriate for use over crowds, and are likely to be limited to operations in military environments or remote areas.

Non-kinetic elements are problematic for different reasons. RF jamming systems work by disrupting the drone's communications link with the operator, but many drones can be programmed to operate autonomously without an active RF link. There is also active research to develop drones that can operate in GPS-denied environments, which would be resilient to GNSS jamming systems.[20] Spoofing systems, 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. Generally speaking, all electronic warfare tactics are subject to countermeasures which may render them ineffective. Furthermore, jamming systems can also interfere with legitimate communications links in the vicinity of a C-UAS system; the FAA has advised airports against the use of jammers since they can interrupt air traffic management operations.[22] 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.

ELECTRONIC IDENTIFICATION

An alternate form of "counter-drone" technology is known as electronic identification, which allows one to remotely access information such as the exact location, model type, operator name, and registration number of drones operating in the vicinity. This information could be used to establish whether a drone presents an immediate threat, something that traditional C-UAS systems cannot do. For example, if a drone is operated by a major broadcasting network, it probably isn't a threat. Electronic ID systems could also provide users with the exact location of a drone's pilot, unlike many existing C-UAS products, which only locate the drone. Chinese drone maker DJI has unveiled one such Electronic ID system, called AeroScope, and other manufacturers are likely to follow suit. A downside of these systems is that they will only work on drones made by manufacturers that have willingly provided their communications protocol to the system manufacturer. The Federal Aviation Administration has taken an interest in this technology as a potential enabler for wider drone integration in the U.S. airspace system. In 2017, it directed an advisory group of industry and policy stakeholders to provide guidance on electronic ID technology, but the group has so far been unable to reach consensus on its recommendations. Industry groups such as the Small UAV coalition continue to urge the FAA to adopt the technology, which they say is a prerequisite to enabling drone operations, such as flights over people and beyond visual line of sight.[21]

Interdiction Effectiveness

No interdiction system, it appears, 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.[23] In real operations, too, counter-drone systems have failed to perform; even though at least eight C-UAS systems were reportedly used during the 2016 Rio Olympics, several drones were spotted near and over events, including the opening ceremony.[24]

Compounding the effectiveness issue is the fact that drone technology itself is not standing still. The C-UAS market will therefore have to constantly respond to new advances in unmanned aircraft technology. As the unmanned aircraft systems market expands, counter-drone systems will need to be flexible enough to detect and neutralize a growing variety of targets, ranging from large unmanned aircraft capable of carrying heavy payloads through to low-flying micro surveillance drones that might only weigh a few grams. Indeed, the proliferation of C-UAS technology might even accelerate the development of technologies that will render C-UAS systems ineffective, particularly in military environments. Drones might be programmed to operate in patterns that make them difficult to detect, or rotors might be modified to dampen a drone's engine noise so that it can evade acoustic detection. 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). Counter-laser systems could protect drones from directed energy attacks.[25] Finally, forces might seek to deploy drone swarms, which present a range of vexing technical challenges from a C-UAS perspective.

Legality of Interdiction

In the U.S. and many other countries, interdiction systems share a common drawback: they may be illegal. In most developed countries, signal jamming devices, including the more advanced directed systems, are either illegal or restricted. In the U.S., jamming systems may also violate the Wiretap Act, which forbids the interception of electronic communications. (Though the Wiretap Act was enacted well before domestic drone use became common, its provisions nevertheless cover the communication between a drone and its operator). Even systems that merely detect and track a drone by downloading information about its location and telemetry might violate this law.[26] Spoofing systems, meanwhile, may contravene the Computer Fraud and Abuse Act.[27]

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. Even a hypothetical C-UAS system that legally disables a drone—which the FAA defines as an "aircraft"—by electronic means would still potentially be illegal. Government employees, including law enforcement officials, are not necessarily exempt from these provisions, apart from 133 military installations around the country that do have authority to shoot down drones.[28] *A detailed analysis of the various legal obstacles to C-UAS use compiled by Jonathan Rupprecht is available here.*[29]

The C-RAM air defense system. Photo by Staff Sgt. Sean Martin.

NON-CUAS-SPECIFIC WEAPONS

While recent years have seen the emergence of a wide range of systems designed specifically with countering drones in mind, a number of existing weapons have been found to work against unmanned aircraft, and are currently being used in that capacity. For example, Israel has used U.S.-made Patriot missile defense systems, which are designed to intercept incoming missiles and rockets, to shoot down drones on at least two occasions.[30] More recently, in January 2017, the Russian military used undisclosed electronic warfare measures to disable a number of drones in a coordinated attack against two of its military installations in Syri,[31] while the Israel Defense Forces used a gunship to destroy what appeared to be an Iranian surveillance drone operated out of Syria.[32] The Army's C-UAS training manual, which was issued in 2017, instructs ground units that discover a drone overhead to engage the aircraft with small arms if necessary.[33]

Responding to the growing interest in counter-drone weapons for use on the battlefield, a number of large defense firms are marketing existing products for counter-drone use. For example, Raytheon claims that its C-RAM air defense system (pictured on this page), which is traditionally used to defend against mortars and other projectiles, is equally effective against slow-moving unmanned aircraft.[34] Northrop Grumman's G/ATOR air defense radar, which has been in active development for over a decade, will be used to detect drones among other airborne threats.[35] In 2016, the U.S. Army awarded Lockheed Martin $27.8 million to tweak its existing AN/TPQ-53 radar to detect drones.[36] In a demonstration in the Persian Gulf last year, the Navy's Laser Weapon System, which was designed to defend ships against a whole range of adversary vehicles, including boats, was used to shoot down a target drone.[37]

Some of the detection and interdiction elements used in new counter-drone systems are, likewise, based on existing products. For example, Babcock's LDEW-CD system incorporates Raytheon's Phalanx unit. A number of radar and jamming units are likewise derived from existing products, and are merely repackaged for the counter-drone mission.

An attack drone armed with a net. Photo by Wesley Farnsworth.

Lack of Standards

No international standards exist for the proper design and use of C-UAS systems. This is an important issue, as it 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. 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 (for example, a jamming system that interferes with emergency radio communications, or a kinetic system that misses its intended target).

Not all C-UAS systems are as effective as advertised. Given that the demand for this technology has only emerged in the past three 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 with the author have noted that a large proportion of systems that are actively marketed to U.S. government customers do not perform at a satisfactory level. In a report released in September 2017, the Department of Homeland Security System Assessment and Validation for Emergency Responders Program only recommends 13 counter-drone products for use by emergency response agencies—and even those recommendations are not necessarily watertight, since the study did not conduct any live testing of C-UAS products.[38] Developing robust universal standards for the technology might help mitigate these issues.

FURTHER READINGS

Birch, Gabriel C., John C. Griffin, and Matthew K. Erdman, “UAS Detection, Classification, and Neutralization: Market Survey 2015,” Sandia National Laboratories, 2015. prod.sandia.gov/techlib/access-control.cgi/2015/156365.pdf

Gettinger, Dan and Arthur Holland Michel, “Drones at Home: Drone Incidents,” Center for the Study of the Drone, 2017. http://dronecenter.bard.edu/drones-at-home-drone-incidents/

Gettinger, Dan, “Drones Operating in Syria and Iraq,” Center for the Study of the Drone, 2016. dronecenter.bard.edu/drones-operating-in-syria-and-iraq/

“Counter—Unmanned Aircraft System (C-UAS) Strategy Extract,” United States Army, 2016. www.arcic.army.mil/App_Documents/Army-CUAS-Strategy.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

Douglas Starr, “This Brilliant Plan Could Stop Drone Terrorism. Too Bad it’s Illegal,” *Wired*, 2017. https://www.wired.com/2017/02/sky-net-illegal-drone-plan/

Guddemi, Charles J. and Catherine L. Feinman, “Unmanned Aircraft Systems: Benefits & Consequences – Part 1 Proceedings of Roundtable,” *Domestic Preparedness Journal*, 2017. www.domesticpreparedness.com/site/assets/files/9770/domprep_uasroundtablereport_part1_final.pdf

“Counter-Unmanned Aerial Systems Market Survey Report,” Department of Homeland Security, September 2017. https://www.dhs.gov/sites/default/files/SAVER_Counter-Unmanned-Aerial-Systems-MSR_0917-508.pdf

“Global Commercial Counter-UAS Technologies Market, Forecast to 2022,” *Frost & Sullivan,* October 30, 2017. www.frost.com/sublib/display-report.do?id=9AB0-00-50-00-00

Jackson, Brian A. and 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

In an entirely different approach to C-UAS, Dutch firm Guard From Above trains large birds of prey to intercept rogue drones in mid-flight. According to Guard from Above, the eagles—which wear protective shin-guards in order to shield their legs from the drone's rotors—have a 95 percent intercept rate, which is likely higher than many mechanical kinetic alternatives. The company sometimes advises clients to operate a secondary C-UAS system in tandem with its eagles for maximum effectiveness. Photos by Guard From Above/Maarten van der Voorde.