Atlantic Council

ISSUE BRIEF

Drone Attacks Against Critical Infrastructure: A Real and Present Threat

MAY 2020 DR. SCOTT CRINO AND CONRAD "ANDY" DREBY

INTRODUCTION

Think about a violent drone attack on a major international airport, an airport like Riyadh, Cairo, or Frankfurt. What could such an attack look like? Maybe it would be a battery-powered, remote-control airplane with a plunger mechanism in its nose, designed to blow up several pounds of explosives when it crashed into a target on the ground like a taxiing commercial airplane. Or it could be a multirotor drone, made of hardened plastic, built for the consumer market but modified, so it can carry a bomb to drop onto a crowd of people waiting for a shuttle bus. Either of these unmanned aerial systems (UAS) would be hard to observe visually or detect with radar, let alone defeat before they hit their targets. What would the aftermath of such attacks be like? Imagine the consequences in terms of damage, injuries, and fatalities. Consider the impact on the transportation network. Reason through the political repercussions and the effects on the government following the attack, and after the inevitable dissection of the intelligence, security, and operations failures that left the targeted airport vulnerable. The final accounting could be inestimably bad for those concerned.

While the likelihood of the above scenarios is hard to estimate, the feasibility is not. Over the past two years, in the ongoing conflicts in the Middle East and North Africa, personnel and critical infrastructure have been attacked by small drones over and over again. From Yemen, *Ansar Allah* (the official name of the Houthi movement) has repeatedly launched attacks using *Qasef* and *Samad* drones against targets deep inside Saudi Arabia—including Saudi Aramco oil-pumping

A Real and Present Threat:

Since July 2018, when Ansar Allah attacked the Abu Dhabi International Airport with a large drone aircraft, there have been more than one hundred attacks by unmanned aerial systems against commercial airports and military air bases in the Middle East and North Africa.

stations in the vicinity of al-Dawadmi and Afif and commercial airports in Abha and Jizan.[1] In Syria, militant groups fighting the Damascus regime have attacked the Russian-occupied Khmeimim airbase dozens of times. Last September, Russia reported the airbase's defenses had defeated fifty-eight drones that targeted Khmeimim, and there have been many more attacks reported since then.[2]

In the United Arab Emirates, *Ansar Allah* attacked the Abu Dhabi International Airport with a large UAS, which exploded in a bright flash over ground-support vehicles parked just outside the airport's main entrance.[3] The aircraft used in these attacks all relied, to varying degrees, on components that are readily available to buyers anywhere in the world through direct-to-consumer Internet purchasing sites. As such, the drone attacks experienced in the Middle East and North Africa could happen anywhere.

The precision and scale witnessed in recent Middle East drone strikes, exemplified in the September 2019 attack on the Saudi Aramco oil-processing plant at Abqaiq and oil fields at Khurais, is forcing a reassessment of UAS-defense plans. According to Saudi Aramco officials, Iranian drones damaged nine oil processing units, known as stabilizers, between the two locations. Additionally, at Abqaiq, eleven of the spherical structures that take gases out of the crude oil were also hit, as were another two tanks that hold water removed from the crude oil.[4] From their launch points, the aircraft were able to successfully navigate to their targets—the separator tanks—and consistently strike them at predetermined impact points in a very short amount of time. Precisely flown, massed drone attacks against critical infrastructure are exceedingly difficult to defend against, because the attacker has the potential to overwhelm the defender. Airports have always been hard to protect against drones because the amount of area they occupy can stretch defenses thin. With precision and mass, attackers can now more readily take aim and hit point targets (e.g., critical components of infrastructure, groups of people, and even specific people) based on their political and military strategies.

1 "Saudi Intercepts Missiles in Attacks Claimed by Yemen's Houthis," *Reuters*, March 28, 2020, https://www.reuters.com/article/us-saudi-riyadh-rockets/saudi-intercepts-missiles-in-attacks-claimed-by-yemens-houthis-idUSKBN21F0XJ; Ben Hubbard, Palko Karasz, and Stanley Reed, "Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran," *New York Times,* September 14, 2019, https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html; "Saudi-led Coalition Intercepts Houthi Drones Targeting Abha and Jizan Airports," *Reuters*, July 16, 2019, https://www.reuters.com/article/us-yemen-security-saudi-airbase/saudi-led-coalition-intercepts-houthi-drones-targeting-abha-and-jizan-airports-idUSKCN1UB2CV.

2 Yuras Karmanau, "Russian Military in Syria Says It Downed Dozens of Drones," Associated Press, September 27, 2020, https://apnews.com/7bb8ba55ed504c2eb2c756135e22c54b.

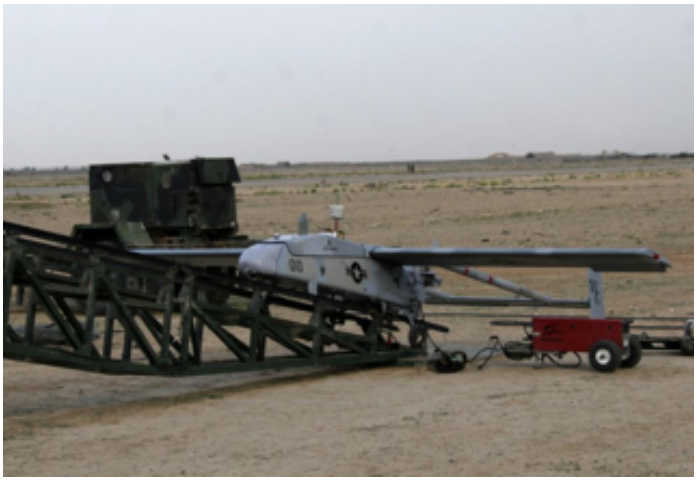
3 Jeremy Binnie, "Video Confirms Yemeni Attack on Abu Dhabi's Airport in 2018," *Jane's Defence Weekly*, May 24, 2019, https://www.janes.com/article/88759/video-confirms-yemeni-attack-on-abu-dhabi-s-airport-in-2018.

4 Summer Said, Benoit Faucon, and Rory Jones, "Aramco's Repairs Could Take Months Longer Than Company Anticipates, Contractors Say," *Wall Street Journal*, September 22, 2019, https://www.wsj.com/articles/aramcos-repairs-could-take-months-longer-than-company-anticipates-contractors-say-11569180194.

DRONES: A HISTORY IN BRIEF

The invention of the drone dates back more than one hundred and twenty years to Nikola Tesla, the Serbian-American inventor, engineer, and futurist. While best known for his work with alternating electrical currents, Tesla also worked to develop remotely piloted vehicles. In 1898, Tesla was granted a US patent for the "method of and apparatus for controlling mechanism of moving vessels or vehicles"—in other words, the first drone. In the same year, Tesla demonstrated the use of wireless alternating electrical currents to command a small boat at the Electrical Exhibition at New York City's Madison Square Garden. Military thinkers immediately saw the potential wartime applications of his invention. When questioned about its potential as an explosives-delivery system, Tesla countered, "You do not see there a wireless torpedo; you see there the first of a race of robots, mechanical men which will do the laborious work of the human race." To militarists, Tesla counterintuitively argued, "The greatest value of my invention will result from its effect upon warfare and armaments, for by reason of its certain and unlimited destructiveness it will tend to bring about and maintain permanent peace among nations."[5]

Following Tesla's invention, many incremental technology gains, particularly in aviation, contributed to the development of drones, but their use was constrained because of their perceived unreliability compared to manned aircraft. That view changed when the Israeli Defense Forces operationalized drones using their Scout UAS for reconnaissance and surveillance missions in the 1982 Lebanon War.[6] After Israel's success, the world's major military powers began investing in drone technology, but progress was slow. During the 1991 US war in Iraq, only a single drone model, the RQ-2B Pioneer UAV, made it to the battlefield.[7] Its mission was day/night reconnaissance, surveillance, and target acquisition. The Pioneer was fourteen feet long, seventeen feet across the wings, and powered by a twenty-six-horsepower snowmobile engine. With a range of only one hundred miles and a price of more than one million dollars, by today's standards the Pioneer was oversized, underpowered,



RQ-2B Pioneer UAV in Iraq (February 2006).
Source: DoD – LCpl Brandon Roach, USMC

Nikolai Tesla, inventor of the first unmanned system, a robotic boat, believed, because of their potential for unlimited destructiveness, the greatest value of robotics would be to "tend to bring about and maintain permanent peace among nations."

5 Kelsey D. Atherton, "Read Nikola Tesla's Drone Patent...From 1898." *Popular Science*, August 19, 2016, https://www.popsci.com/nikola-tesla-patented-drone-controls-in-1898/.

6 "Spies That Fly: Scout (Israel)," PBS, https://www.pbs.org/wgbh/nova/spiesfly/uavs_13.html.

7 Ted Shelsby and Robert Ruby, "Md.-Made Drone Makes Mark as Aerial Spy in Gulf War," *Baltimore Sun*, January 30, 1991, www.baltimoresun.com/news/bs-xpm-1991-01-30-1991030045-story.html.

Leap-Ahead Technologies, such as microcomputer flight controllers, autopilots, GPS, and software-defined radios, have made it possible for almost anyone to acquire capabilities consistent with, and sometimes surpassing, those of the best-funded government programs.

and very expensive. Nonetheless, it was still a safer and cost-effective alternative to using a manned aircraft for the same mission. Seeing the value of drones through the success of the Pioneer and other programs, in the year 2000, Congress mandated that one-third of all attack aircraft operate unmanned within ten years.[8]

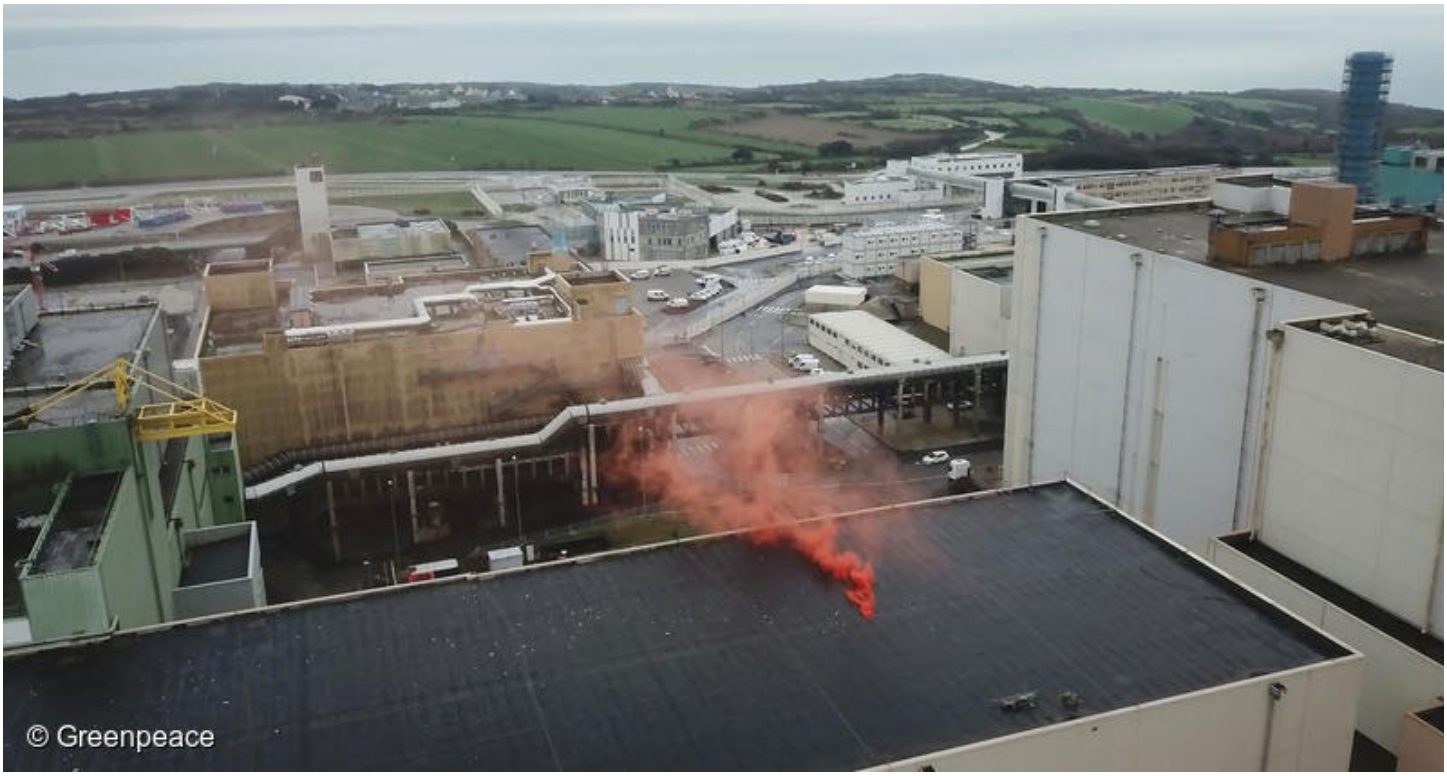
In parallel to the military evolution of drones, there have been other, potentially more significant, technological advances in the commercial sector. While the defense industry put most of its effort toward high-flying, unmanned spy planes and tactical attack drones that could be flown from half a world away, the commercial drone industry focused its sights on smaller, cheaper, easy-to-fly platforms that would appeal to the masses. Innovations in wireless technology and satellite navigation, the move away from hardware- to software-enabled components, improved battery life, and the integration of high-resolution onboard cameras all expanded appeal, reduced cost, and improved the user experience, resulting in broadened popularity of drones for personal and commercial use.

LEAP-AHEAD TECHNOLOGIES

Developing a capable means to counter malicious UAS targeting airports is proving a challenge. By nature, a counter-system for anything is necessarily reactionary; the counter-system developer is almost always one step behind the innovator. This is especially true for counter-UAS systems. Driven by commercial and consumer demand, innovation in the drone world is incessant. And, any new UAS hardware improvement or software design change adopted by the world's threat actors can knock the counter-UAS system developers off their strides. Compounding the challenge of just keeping up with technological change, counter-UAS planners must consider and balance various factors of governance, such as privacy laws, commercial regulations, collateral damage, and legal jurisdictions, any of which might unintentionally impede their security plans.

Many of the technologies used in modern drones are very new. Not long ago, drones were limited to either the world's most technologically advanced, well-funded militaries or a relatively small community of remotely controlled (RC) aircraft enthusiasts. But, in the past fifteen years, "leap-ahead" technology changes in flight controllers, autopilots, global navigation satellite systems (GNSS), and software-defined radios have made it possible for almost anyone to acquire capabilities consistent with, and sometimes surpassing, those

8 Jeremiah Gertler, "U.S. Unmanned Aerial Systems," Congressional Research Service, January 3, 2012, 2, https://crsreports.congress.gov/product/pdf/R/R42136.



A Greenpeace multirotor UAS dropping a smoke bomb on the rooftop of a nuclear-material storage building for Orano SA in La Hague, France (January 2019). Source: © Greenpeace

of the best-funded government programs. The integration of these leap-ahead technologies and others (e.g., onboard cameras and obstacle-avoidance sensors) onto commercially marketed quadcopters revolutionized the RC aircraft industry, and its popularity soared. In turn, strong customer demand brought new businesses into the industry, which accelerated the rate of discovery. In recent years, drone sales in consumer and commercial markets have increased 40 percent year over year.[9] Unfortunately, the same capabilities and ease of use that made commercial drones so popular have transferable military applications, and are readily adapted by irregular militaries and terrorist organizations.

In the Middle East and North Africa, consumer flight controllers and autopilots are being used side by side with military-grade systems. In larger drones, *Ansar Allah* appears to use military-grade flight controllers, as does Iran's military. In smaller drones, however—such as *Ansar Allah*'s Rased reconnaissance drone or those seen used by HTS against Russian assets in Syria—commercially available autopilots are widely used. A person building a UAS from scratch can choose from any variety of vendors online selling autopilot systems using Arduino-based open-source hardware and software, which enables the autopilot to readily accept input from other microcomputers (e.g., altimeters and GPS) and transmit commands to the aircraft.

UAS THREAT TO CRITICAL INFRASTRUCTURE

The West can learn a lot by studying the counter-drone experiences of the Saudis, Emiratis, and Russians in the Middle East. Additionally, based on current knowledge of the state of UAS technology and considering the practical considerations a terrorist group has in planning a drone attack, one can make some inferences about what such an attack might look like. First, for several reasons, the aircraft would probably be smaller than those being flown against airports on the Arabian Peninsula. The *Qasef*s and *Samad*s flown by *Ansar Allah* are large; they weigh close to seventy kilograms and have wingspans almost three meters across. For its operations, Ansar Allah needs expansive safe havens, logistical support, and state sponsorship. While these critical

9 "33 Eye-Opening Drone Stats - Key Trends for 2019," *Philly By Air*, March 15, 2019, https://www.phillybyair.com/blog/drone-stats/.

requirements could be met outside the Middle East, it is more likely that a terror group planning to attack locations such as airports, military bases, or port facilities with a drone in the Western Hemisphere, Europe, or Asia would choose something smaller, more discreet, and with less chance of attribution.

Something smaller, like a medium-sized multirotor or small fixed-wing UAV, would be a more likely airframe to use for an attack against targets outside the Middle East. An octocopter with six to eight motors and propellers could be custom-built to carry large explosives of about six kilograms or more. To help visualize what this type of aircraft might look like, the picture (previous page) shows a similarly sized multirotor used by Greenpeace to drop a large smoke bomb on the French nuclear-processing facility at La Hague in late January 2019. The same drop device Greenpeace used for its smoke bomb could instead carry a lethal munition, resulting in a very different outcome.

As an alternative, a terrorist group might choose to use a fixed-wing UAS instead of a multirotor. In that case, there are a wide variety of commercially available hobbyist kits made of EPO foam, which could be made into flying bombs. In fact, this was the approach the Islamic State of Iraq and al-Sham (ISIS) used, and is what *Ansar Allah* still uses. The *Ansar Allah* Rased UAV is basically a direct copy of the extremely popular Skywalker X8 remote-control airplane design used worldwide by drone enthusiasts. The drone has a strap with a dual function: besides securing the payload, it is also part of a crude drop mechanism used to release it over the aircraft's target. This package could just as easily be a bomb. Alternatively, a bomb could be placed inside the body of the aircraft, set to explode by a GPS coordinate, or on impact when the drone strikes its target.

Another, especially dangerous, aircraft would be a remote-control, turbine-powered jet. Jets are typically assembled from kits and commercially available flight components. The design of turbine-powered aircraft makes them a potent incendiary weapon without the need for additional payloads. Unlike an electrically powered or gas-driven UAS, which requires an explosive payload to cause significant damage, a turbine is a flying bomb. When a turbine crashes into a surface, the heat from the engine ignites the fuel and causes a fiery explosion. A recent video posted to the social media platform Telegram is of an RC jet designed by Ahmad Bawadir Abeidi, called the AMD. It is described as the first of ten models he plans to produce and sell to interested countries in the Middle East.

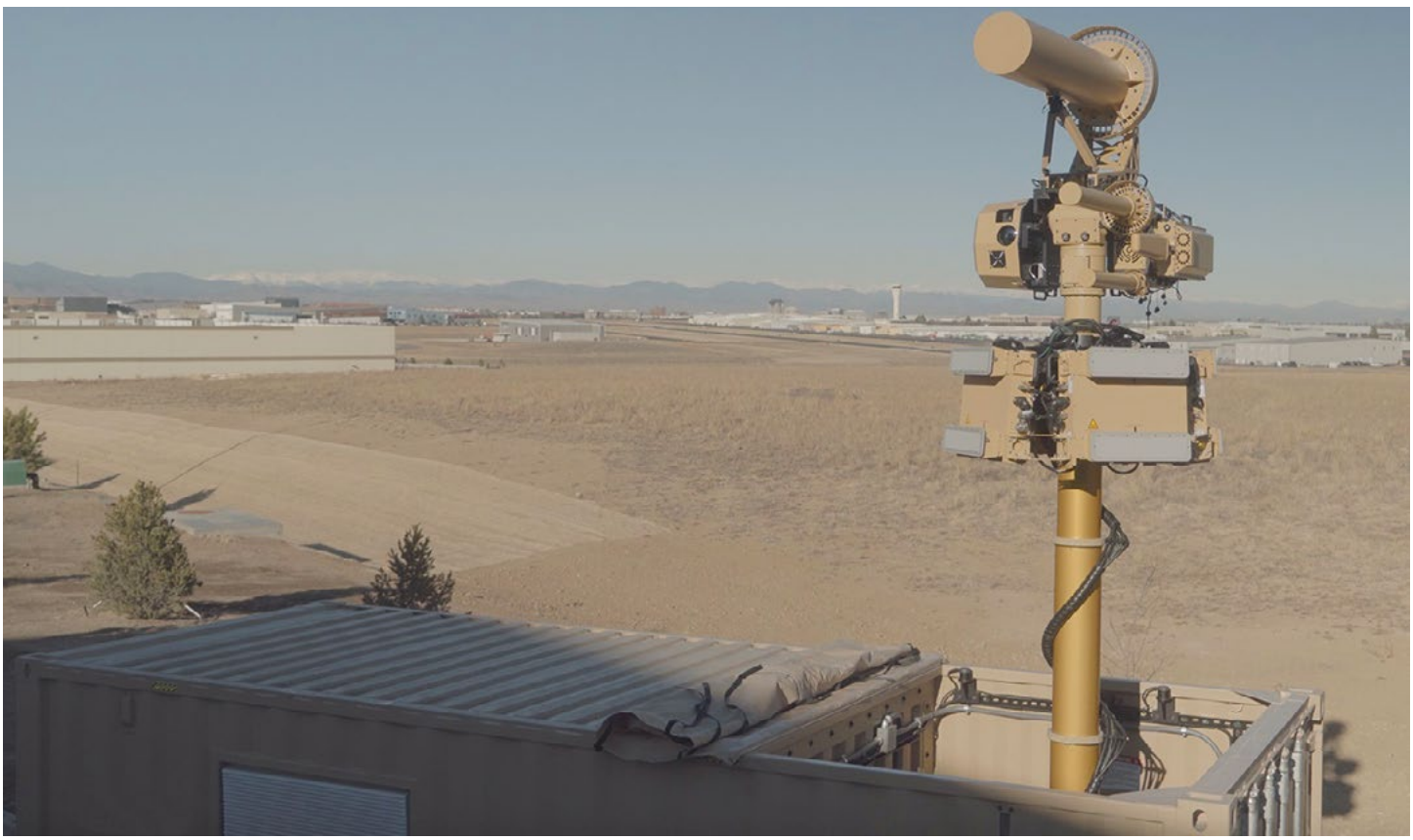
Although using turbine-powered jet technology for weapons is largely aspirational, it should still be considered a viable threat. Radio-controlled jets can fly upward of two hundred miles per hour (mph), covering a lot of ground quickly and reducing response times for counter-UAS systems. Older-model turbines required an external, auxiliary, propane start system and a team of people to prepare for launch, but newer engines are self-contained, and spin up at the flip of a switch. There are, however, significant drawbacks. First, turbines require a very clean environment to operate, which is not always available in the region. Second, although they can be flown autonomously to a target, a much higher level of piloting skill is required to build and operate RC jets. Third, flight times are very short, normally in the 8-10 minute range, so long-range attacks are not possible, although RC jets with larger fuel tanks are beginning to enter the market.

SEEING THE THREAT: DETECTION, TRACKING, AND IDENTIFICATION

Counter-UAS systems consist of three essential components: the sensor systems that detect, track, and positively identify the aircraft; the countermeasure systems to mitigate or defeat the aircraft; and the communications and information systems that enable the sensors and countermeasures to interoperate. Sensors are normally organized by the phenomena they recognize: radio-frequency (RF) sensors, radar, electro-optical/infrared (EO/IR) cameras, and acoustic sensors.

RF sensors detect the signal transmission between the UAS and its remote control. RF detectors scan a defined space in the RF spectrum looking for these signals, which they compare to their databases. A positive correlation means the sensor has found something. While the detection range of an individual RF sensor is typically in the 3-5-kilometer (km) range, multiple sensors can be arranged in a network to increase the system's coverage area. Since most commercial UAVs work in a limited range of frequencies, within the unlicensed industrial, scientific, and medical (ISM) bands, most RF detectors look only within those bands. This enables RF detectors to narrow their search, thereby extending their range, but it also means they will miss aircraft that are using uncommon frequencies.

A challenge for RF sensors is the recent advances being made with regard to frequency-hopping spread spectrum (FHSS) technology. FHSS improves the reliability of the signal connection between the aircraft and its controller, but newer FHSS can hop between channels within ISM bands faster than RF sensors can sweep through the channels to detect their signals, causing problems detecting even the most popular drone models.



A counter-UAS system from Liteye Systems, Inc surveilles a sector near a Middle Eastern airport (May 2019). Source: Liteye Systems, Inc.

Radars are another critical component of counter-UAS systems. The range of radar systems helps them get beyond the range limitations of RF detectors and can bridge gaps in RF coverage. Even more, the extended range offered by radars provides increased response time, which can significantly improve chances for success against incoming-threat UAS.

Like RF detectors, however, radar also has its limitations. The small size and composition of most commercially available UAS already makes detection difficult, and simple modifications to UAS—such as modifying the aircraft's exterior with different coatings and types of materials to alternatively increase or decrease its radar cross-section—can make detection even harder. Even without tradecraft, small UAS can be hard to find with radar. Weather and environmental conditions, terrain features, and flight profiles can all reduce radar effectiveness. The popular Doppler radars work by sending a series of microwave pulses and analyzing how the pulse is altered by an object in motion, which provides the location of the object and inferences about what the object might be. Hovering, low-altitude flight, slow airspeeds, and frequent stops and turns—which are flight profiles often employed by pilots flying multirotor systems during intelligence, surveillance, and reconnaissance (ISR) missions—greatly reduce the effectiveness of Doppler radar.

Some may ask why strategic air defense systems, which may already be in place at many locations, are not sufficient against drones. Beyond the extreme cost, radars are tuned for the size, speed, and altitude of likely threats in the region. Though drones are becoming larger and faster, they are still very small and slow when compared to ballistic missiles and manned aircraft. They also fly much lower, making strategic air-defense systems unviable.

EO/IR cameras are an important sensor component within a counter-UAS system. While the field of view of an EO/IR camera may be narrower than an RF detector, their range may be longer. More importantly, EO/IR cameras are critical to making classification determinations (e.g., is it a drone, or a biologic like a bird?) and for making positive identifications. Often, EO/IR cameras are the only way to confirm an actual UAS detection.

Defense in Depth:
Large-area, protected assets like commercial airports require an integrated approach for counter-UAS with layered, overlapping sensors and countermeasures guarding the most likely approaches against drone attacks.

COMMUNICATIONS AND MANAGEMENT

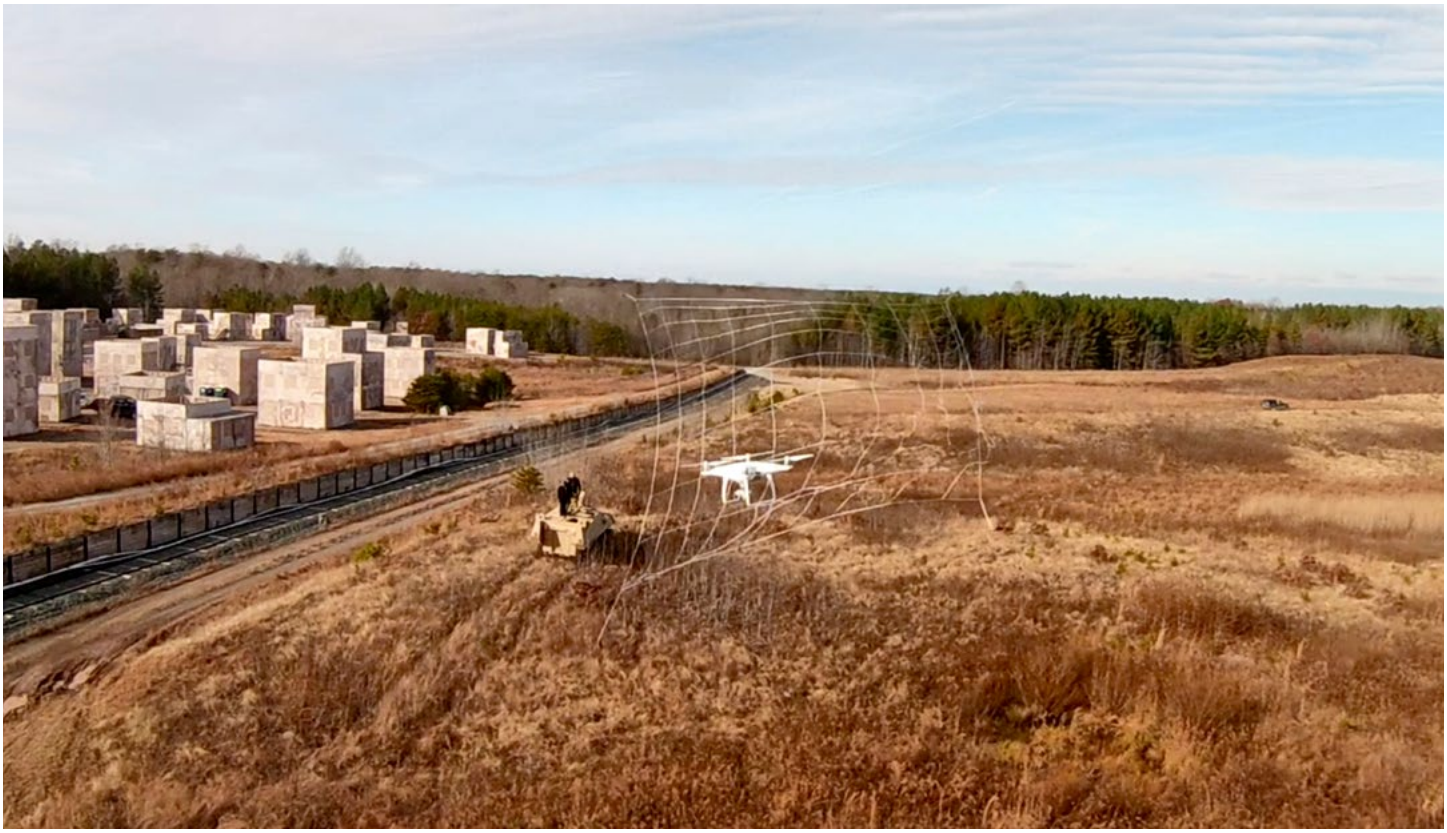
Defeating small UAS is, at best, a difficult task, and there are no silver bullets in drone defense. Every counter-drone system has vulnerabilities, sometimes intuitively obvious ones, which can be exploited. To defend protected assets requires an integrated approach, with counter-UAS systems arrayed in a layered defense. Each location will be different, and will require a unique defensive design attuned to the operating environment. The laydown of the various overlapping sensors should focus on the most likely approach vectors, while remaining able to respond to threats across all potential avenues of approach. It is particularly crucial that all information provided by the sensors be routed to a single common operating picture (COP), using a common data format. In an active situation, where a protected facility is being attacked, the person sitting at the COP should be empowered to make all decisions necessary to defeat the aircraft. It would be smart to duplicate the information to other incident-command locations, but only one person should be in charge.

While entrusting a person with permission to engage a drone at their sole discretion may seem extreme, holding the permission elsewhere risks consequential delays that could cause a tragedy. To put this in perspective, a relatively slow multirotor UAS like the one used by Greenpeace in its protest can easily travel sixty-five kilometers per hour (kph), or forty mph, meaning it will cover a kilometer's distance every minute of flight. Given the challenges described above that current CUAS sensors face, it is not uncommon for detection to occur at or inside a one-kilometer range, depending on the terrain. This situation would leave just seconds of reaction time to initiate a countermeasure.

Besides making the critical decisions for when to engage or not engage a threatening UAS, the person in charge will also be responsible for interfacing with law enforcement. Not all unwanted UAS are intentionally malicious; some end up at sensitive sites through accident or bad piloting. With RF-detection systems, there is a good chance that both the aircraft and pilot's location will be discovered. It will be the person in charge's responsibility to guide security to the pilot, so they can remedy the situation.

COUNTERING UAS THREATS

In the next few years, the technology for directed-energy weapons, such as microwave and laser, may mature into safe and reliable drone-defeat technologies. Because of their speed, accuracy, range, and lower collateral-damage risk, directed-energy weapons may be the best approach for



A net launched from a net-capture system just before catching its target, Quantico, Virginia (December 2018). Source: Red Six Solutions

countering malicious UAS. High-energy lasers have already been tested against small UAS with promising results, but there are drawbacks. These include an extremely high energy requirement (3-5 kilowatts (Kw) or more) and UAS reflective surfaces that can bounce the laser beam off the target, negating its effectiveness and possibly putting ground personnel or other airborne platforms at risk. For this reason, high-power microwaves (HPM) may be a better option. HPM weapons use electromagnetic radiation to destroy the internal electronics of the drone within seconds. Current challenges that need to be worked through before HPM weapons are effective include extending their range, learning how the composition of the aircraft affects absorption of radiation, and assessing the potential risk to humans.[10]

Although the promise of HPM and laser countermeasures is in the future, there exist today UAS countermeasures, which can jam drone signals, inject code to interfere with their communications, capture them with nets, or shoot them out of the sky. While each approach has its drawbacks, several have shown great potential and, in certain circumstances, may be good tools to have on hand when protecting high-risk sites.

RF and GNSS are the two primary types of jammers. RF jammers electronically disrupt the RF communications link between the air vehicle and the ground controller. These jammers are effective when an RF link between the UAS and pilot exists, though this is not the case with autonomous UAS. Because of the way UAS software works, the most likely outcome of jamming is that the drone returns to its launch location, lands, or enters a loiter—in which case, the drone lives to fly another day. GNSS jammers used in conjunction with RF jammers can cause UAS to land immediately—and sometimes crash—or force an uncontrolled flyaway. A GNSS jammer disrupts the global navigation signal to the UAS. However, this might not have much effect, because onboard

10 "High Power Microwave Weapons Types | Directed Energy Weapons," *RF Wireless World*, https://www.rfwireless-world.com/Articles/High-Power-Microwave-Weapon-System-basics-and-types.html.

magnetometers and compasses can keep the aircraft on its programmed route. Using GNSS jammers can, at times, be problematic because of the collateral damage they can cause to myriad other technologies that rely upon the GNSS for precision, navigation, and timing functions.

RF hijacking is a more sophisticated approach to stopping drones. Hijackers electronically take control of the UAS and route it someplace safe. RF-hijack systems are quite promising; however, hijack systems require extensive knowledge of the data-link protocols used by the drone, and a strong 256-bit encryption makes getting that knowledge quite difficult. Autonomous drones are an even bigger problem because, to get to them, the hijacking system has to find a backdoor into the navigation system. An autonomous UAS, flying a one-way, kamikaze-style attack, like the September 2019 attacks on Abqaiq and Khurais, would be next to unstoppable, even with a hijack system.

Physical capture systems, such as those that fire a net at the drone, and hard-kill systems that drop the drone from the sky, are the two other approaches. Both have limited ranges (less than a few hundred meters). Nets work, provided the aircraft is close and maintaining a steady flight path, hopefully hovering in place. Small-arms weapons, especially when aided with smart-aiming technology, can minimize the risk of collateral damage by reducing the number of bullets needed to kill the drone. Even though the ranges of these systems are short, they should still be considered in the defensive plan. In the event a drone eludes the effects of the jammers and defends itself from hacking, nets and small arms may be the only options available to stop a weaponized UAS.

Solving the UAS Defense Challenge

When looking at the threat posed to critical infrastructure by drones, people may be tempted to throw their hands in the air. Admittedly, the UAS threat is complicated and hard to measure, and the solutions may seem difficult to defend in terms of their cost-to-benefit ratio. While this is the type of difficult problem that is the friend of status quo bias or waiting to let the problem solve itself, there are any number of practical steps available to improve the defensive posture of high-risk critical infrastructure today.

Take Immediate Action

Right away, thought should be given to what to do in the case of an emergency. Regardless of the degree of counter-UAS protection implemented at any location, even in the absence of technical solutions (e.g., electronic sensors and countermeasures), there must be centralized control of the monitoring and response to UAS incidents. Upon the alert of a detected threat through the entire engagement sequence, personnel at a centralized control center must be empowered to make decisions. Devolving independent authority for action for any activity can represent an archetypal change for many organizations. But, in situations like counter-UAS engagements, every second will count.

Use a Common Operating Picture to Focus Decision-Making

Supporting the decisions that may have to be made requires an investment in communications and information technology. Over the past several years, virtually every senior public official with a role in developing counter-UAS technologies has stressed the need, in the event of a malicious UAS event, to have a COP. Having a COP requires an information architecture that can move and merge the input from various sensors in arrangements that facilitate decision-making. This will mean building to defined, standardized communications protocols and ensuring sensor output translates into geospatial visualization tools.

Conduct Independent Vulnerability Assessments

The protection needs of every location will be different, as will the physical and human geography of that environment. The science of developing a layered counter-UAS defense architecture will require engineers and technologists; however, a vote in the defensive planning must also go to the enemy. An independent “red team” of pilots, threat analysts, and law enforcement should complete vulnerability assessments at each location and view it as a potential target. A red team helps the design process in multiple ways: it can help identify shortcomings in logic, and it can help to reasonably define the threat (e.g., some worst-case scenarios deserve being ignored).

Employ a Defense-in-Depth Strategy

Counter-UAS networks for expansive locales may, like airports or border areas, need more mobility than smaller infrastructure sites. In setting the defense, the counter-UAS network should include fixed and mobile platforms, with fixed systems providing a primary capability and repositionable mobile systems going where they are needed most. There are many mobile counter-UAS systems that are fast to set up and easy to operate. A terrorist group aiming to conduct an attack will look for ways to avoid sensors and use flying techniques that exploit seams

in defenses. By having a mobile capability, security forces can keep adversaries guessing, and, when necessary, concentrate resources where they are needed most.

Adopt Technologies that Distinguish Good Actors from Bad

In the United States, some form of UAS remote ID will become a requirement in the next few years. The remote ID is the ability of an in-flight UAS to provide identification information to an electronic interrogation platform. The US Federal Aviation Administration is currently seeking input on its proposed rule changes for UAS remote ID. While remote ID is not a counter-UAS solution per se, it should help improve the situation awareness of what is in the air. The same approach could have applicability internationally, and could help distinguish between the good guys and the bad guys.

Establish Clear Lines of Authority

UAS remote ID is just one of myriad drone-policy and regulatory requirements that will shape the air environment in the immediate future. The guiding principle for these initiatives is to safely open the airspace to greater volumes of commercial and recreational drone use. As such, every change recommendation for improved security will be weighed against the demand for more drones. Some of the thornier issues needing to be addressed include: who will be allowed to shoot down or jam drones, and under what conditions; will law enforcement be allowed to electronically take over suspicious drones; what are the limits of counter-UAS systems to surveille the public space; and what are the privacy expectations of drone operators.

Acquire the Means to Positively ID Threats

EO/IR cameras provide an increased level of confidence in the reliability of anomalies detected by RF sensors or radar. Positive identification by EO/IR cameras allows for faster decision-making when determining if a response is required. Furthermore, since EO/IR cameras sometimes see farther than RF-detection systems, software-enabled EO/IR cameras can hand over targets detected by radar to RF-detection and mitigation systems, thereby improving control of the incident through the entirety of the engagement sequence.

In the Middle East and North Africa, the trend in successful, high-profile UAS attacks against personnel and infrastructure is toward fast-moving, autonomously flown, fixed-wing UAS with explosive payloads. The airspeed and lack of radio frequency signature greatly limit the effectiveness of RF-detection systems and increase the need for long-range radar systems and high-resolution cameras. That said, RF detection is essential for detection of close-in threats, such as small multirotor UAS, which can be launched from anywhere.

Use Technology to Support Forensics

In addition to EO/IR, overhead or ground-based imagery can be effective tools to forensically reconstruct UAS events after they occur. Investigations of recent airport closures like the well-known London Gatwick Airport event in December 2018 were hampered because video imagery of the events came from scattered security cameras, usually intended for a purpose different from aerial observation. An approach to consider is wide-area motion imagery (WAMI), which could be set up to interrogate everything that flies over the site for post-event forensic analysis. Orienting WAMI cameras skyward could also help address privacy concerns people may have about UAS sensor operations.

Don't Wait for the Perfect Solution

Counter-UAS technology will continue to improve, but the pace of technological change is impossible to predict. Eventually, improvements in sensors, communications systems, and countermeasures will catch up with today's UAS threat. But, who knows what the UAS threat will be by then? Waiting for the perfect solution is a bad alternative to assessing current strengths and weaknesses, strengthening response plans, and incrementally investing in existing, working technologies.

Dr. Scott Crino is founder and CEO and **Conrad "Andy" Dreby** is director of red-teaming at Red Six Solutions, LLC. Red Six is applying red-teaming research methods to develop counter-UAS operational response and technology requirements.

This issue brief is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this issue brief's conclusions. This report is made possible by general support to the Atlantic Council's Middle East Programs.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org