GlobalResearch
Center for Research on Globalization

The Dark Side of Our Drone Future

By James Rogers
Global Research, November 06, 2019
Bulletin of the Atomic Scientists 4 October 2019

Region: Middle East & North Africa
Theme: Militarization and WMD, US NATO War Agenda

Let me paint a picture of the near future. Drones, some weighing a few pounds and others a few tons, will flow endlessly back and forth from rural distribution centers to inner-city delivery hubs. Day in and day out, they will drop off our weekly shopping, last-minute presents, and important medicines. Drones might even pick us up from work (or the bar) and take us home in automated airborne Ubers. They will transform our lives. Hundreds, if not thousands, of drones will fly high above towns and cities, bypassing the congested highways and streets currently plagued by traffic.

Put simply, the drone revolution will change the way in which we conceive and comprehend logistics and transportation. Yet not all the changes we see from the global spread of drones will be positive. Drones bring with them a novel set of risks and challenges—and these need to be confronted.

Some of the issues are self-evident and have already begun to cause problems as drone technologies expose unforeseen vulnerabilities within vital national infrastructure. Drones made headlines last month when they were flown at low level alongside cruise missiles to evade Saudi Arabia's air defenses and knock nearly 6 percent of the world's oil supply offline. It's still not clear who committed these attacks, with some suspecting Yemen's Houthi rebels and others pointing the finger at Iran, but this is the point. Uncertainty is a core part of the drone's allure. The combination of ever-longer range and remote control allows for a distancing and a deniability when it comes to aggressive drone use. A drone can be above us, next to us, or, horrifyingly, outside our airplane window as we land at an international airport. It is unclear who is controlling any given drone, and there are currently few measures that can effectively trace, track, and disable the eclectic mix of drone systems that populate our skies.

"Drone" has, of course, become a somewhat amorphous term, used to describe a vast array of systems. Yet in all forms, from fixed-wing systems to quadcopters, drones present novel risks to security. These are unlikely to be resolved quickly, if at all.

The warning signs. Even if Yemen's Houthi rebels did not conduct the September 14 attack, as they claimed, they have been successfully using fixed-wing drones for a while. They began with state support, allegedly from Iran, but soon turned to commercial drone supplies to bolster their arsenal. High-definition cameras, industrial motors, and long-range transmitters all added to the Houthis' capabilities. Their attacks on oil pipelines in Saudi Arabia in May 2019, assassination of high profile military leaders in Yemen in January 2019, and alleged strikes on national airports in Abu Dhabi in July 2018 and Dubai the following month highlighted the protentional for hostile actors, bolstered by commercially available technology, to cause death and destruction by remote control. Even the most innocuous

commercial system can be misused.

The chaos at Gatwick airport, where the alleged sighting in December 2018 of two quadcopter drones—or perhaps just one, several, or no drones at all (depending who you ask)—highlighted both this threat and its deniability. The United Kingdom's second largest airport was brought to a standstill, but no one was brought to justice. Not only this, but the 125 near-misses and dangerous encounters that occurred between planes and slow, low-flying, off-the-shelf drones in that country last year occupied the time, capacity, and resources of police forces, airport officials, and parliamentary committees as the drone threat loomed.

The press has capitalized on the climate of fear, gleefully warning of quadcopter drones fitted with "machine guns," "flamethrowers," and payloads of radioactive waste—novel inventions that highlight the disturbing versatility of simple-to-acquire, and easy-to-adapt, remote systems. In fact, we need only look at the Japanese "atomic drones," ISIS "Trojan Horse drones," and Venezuelan "assassination drones" for pertinent reminders of how these toys can be transformed into weapons capable of violating secure governmental and military sites.

Still, this is just the start. Think of today's nefarious drones as the Model T of dangerous drones. As drone technologies grow ever more sophisticated, proliferating in an unchecked and under-regulated manner, "hostile drone" incidents will increase in impact and number.

Evolving technology. Let's focus on the future of the quadcopter drone threat. These drones, including systems consumers can already buy from mainstream manufacturers like DJI or Parrot, are now able to go faster, transmit images further, and fly for much longer than they could just a few years ago. Some are now "fast and furious," rather than "low and slow." The latest DJI Mavik 2, a relatively basic drone from a Chinese technology company, has a maximum speed of 72 kilometers per hour, an 8-kilometer video transmission distance, and can fly for up to 31 minutes. The recent use of drones to fly over the many thousands of protesters and security forces in Hong Kong highlights the pace, agility, versatility, and access of the current drone generation.

DJI, to be fair, has introduced a number of measures to encourage responsible use, particularly around airports. But as drones increase in numbers and capabilities, they are becoming more difficult to confine and counter. Readily available "add-ons"—such as the latest motors, transmitters, apps, and cameras—exacerbate the dangers.

Swarms of drones, sometimes more than a thousand strong, have kept us enthralled and entertained—be it at the Olympics or on New Year's Eve—as Intel, one of the world's largest computer technology companies, has shown off its multi-drone control software. Nevertheless, there is a troubling side to this captivating capability. For the princely sum of zero dollars, drone operators can download software and online tutorials that make it possible to fly multiple drones, simultaneously, toward a chosen target. When this capability is combined with ever-more-sophisticated smartphone apps that allow drone pilots to pre-set their drones' final destination, it is easy to see how free, open-access, autonomous drone swarms are born. Of course, there is no need for these apps, tutorials, or software if a maliciously minded group has multiple operators, with multiple drones, flying all at once at a target. But the software and apps make it easier for an individual to achieve this once remarkable feat.

A window into the future. A terrorist attack by swarming drones may seem farfetched, and it is important not to engage in hyperbole. However, scenarios similar to this are playing out around the world, often in a hostile manner. Once again, the recent attacks on Saudi Arabia should give pause for concern. At least 18 drones and seven cruise missiles were reportedly used to break through national defenses and strike the designated targets in Abqaiq and Khurais. The use of these systems in swarms makes tactical sense, as it increases the likelihood of a successful strike, by overwhelming and saturating defenses. Drones may also be used to help identify targets, allowing secondary systems to strike with precision. In a different, but not unfamiliar manner, swarms have been used for saturation, spotting, and strike purposes by both criminal gangs and terrorists.

Last year, the FBI was operationally blinded when a criminal gang, embroiled in a hostage situation, made "high-speed low passes" at FBI agents with a rudimentary quadcopter drone swarm. Joe Mazel, who heads the FBI's Operational Technology Law Unit, told *Defense One* that the gang buzzed the hostage rescue team and even "had people fly their own drones up and put the footage to YouTube."

The incident was headline-grabbing, yet not a wholly new use of drones by criminal gangs. Previously, drones have been used to intimidate officers, stalk witnesses, smuggle drugs and contraband into prisons, spy on homes and industrial sites to see when occupants leave, and search for vulnerable and valuable assets. In Mexico, a drug cartel used quadcopter drones to spy on, identify, and attack a high-ranking official. The drones were fitted with grenades and sent to the residence of Gerardo Sosa Olachea, the public safety secretary for the Mexican state of Baja California. Fortunately, the grenades did not detonate. However, events like this provide a glimpse into the future.

What will the next drone attack look like? We can gain insight from the case of Basil Hassan in Denmark. Born in 1987 in a small town 20 kilometers from Copenhagen, Hassan would become known as one of the most dangerous individuals on the US list of foreign terrorists. He had a passion (and a talent) for engineering and flight. These were skills he chose to apply helping ISIS establish a caliphate in Iraq and Syria. Specifically, he saw how drone systems could be easily acquired in Denmark or ordered online, sent to Turkey, and then smuggled across the border to help ISIS units that had emerged from captured resources at the University of Mosul in Iraq. By 2014, the units were experimenting with chemical agents and explosives in attempts to create deadly weapons. They were also testing and developing both fixed-wing and quadcopter drone systems. In time, Hassan played a major role in harnessing simple commercial technologies and using them to create effective weapons of war for ISIS's new drone squadrons across Syria and Iraq.

The Danish authorities had known about Hassan since a friend was convicted of terror-related offenses in 2007. Hassan still managed to flee the country in the spring of 2014, turning up in Turkey, where he was arrested and jailed. By the fall of 2014, however, he was suddenly released from Turkish prison in a prisoner exchange between ISIS and Turkey. Hassan then used his engineering knowledge, training, and contacts from his previous life in Denmark to smuggle advanced drone technologies into ISIS-held territory. He was able to obtain the technology he needed from a hobbyist shop in Copenhagen—using his connections in the region to order five drone computers worth a total of around $6,000, and 20 thermal imaging cameras at $4,000 each. The Danish authorities noticed, tracked, and infiltrated his activities—but over a five-year period he had managed to bolster the ISIS drone arsenal.

It's hard to attribute specific drone attacks to Hassan, but what is clear is that the ISIS drone program grew in impact and lethality after his arrival in the terror group, and the arrival of the high-tech drone parts. What has often been overlooked is the extent to which, since 2014, ISIS has used such drone systems en masse and in coordinated, highly tactical attacks. The group has used 10 or 20 drones at a time, alongside thermal imaging systems, long-range transmitters, high-definition cameras, onboard computers, and high-speed motors to attack coalition forces in Iraq and Syria.

According to my own interviews with coalition special-operations forces and journalists, in one series of attacks that occurred within a 24-hour period, there were no less than 82 drones of all shapes and sizes lobbing bombs at Iraqi, Kurdish, US, and French forces. During these attacks, ISIS was adept at coordinating its drone attacks with suicide bombers, improvised explosive devices, and sniper fire, to cause maximum damage and chaos for coalition forces.

ISIS was able to upgrade its drone systems by fitting them with better motors and thermal imaging cameras, making it possible to conduct high-speed night attacks. As one member of the Kurdish forces recalled, the drones were so effective that some soldiers began to "fear the noise and flee from the front line."

The upshot is that drone technologies, supplied from the European continent, made their way to war zones with devastating impact. As drone technologies become more sophisticated and available in Europe, a pertinent question for security authorities should be: What could happen in Europe if these systems got into the wrong hands?

Systems already available in Europe include agricultural drones and their chemical spraying systems, high-speed motors that can propel drones faster and farther than ever before (while carrying heavier payloads), long-distance transmitters and batteries that allow an operator to be far from the drone in use (improving deniability), thermal-imaging cameras that allow an operator to effectively see in the dark, commercially developed (or even improvised) object-release devices that allow for the deployment of mortars and grenades, data theft/transmission software to capture sensitive metadata or send misinformation messages, and the aforementioned swarming and autonomous drones. When these technologies are combined, it is easy to see how a drone could be manipulated in creative ways.

In the future, population centers will become increasingly reliant on drones to provide the vital goods and services that keep a nation functioning commercially and socially. Amazon deliveries and Uber autonomous taxis are just the beginning. Emergency medical services, police forces, and fire and rescue responders will increasingly use drones. So will postal services, communications conglomerates, and social media giants. Each will seek to harness the speed and cost-effectiveness of drones, leaving society increasingly vulnerable.

A future vulnerability. In this future, drones are not only a threat to vital national infrastructure, but also a vital national infrastructure themselves. This is troubling for a variety of reasons, not least because one rogue drone incident could mean the grounding of a whole regional or national drone fleet, bringing critical and lifesaving services to a grinding halt. If hacked, drones could be put to insidious uses by criminal gangs, or even other nations, that wish to gather data or spread misinformation.

In August 2019, for example, hackers attending the annual Defcon conference in Las Vegas

managed to demonstrate how a simple off-the-shelf quadcopter drone, fitted with a radio transmitter, could hover above a home and take control of its smart TV. The drone transmitted a signal "more powerful than the one broadcast by legitimate TV networks, overriding the legitimate signal." This may seem harmless, but such a technical capability could allow a hacker to "display phishing messages that ask for the viewer's passwords, inject keyloggers that capture the user's remote button presses, and run cryptomining software." The drone could even broadcast its own material.

In Ukraine, Russian-backed forces have already used fixed-wing drones, alongside ground-based systems, "to conduct electromagnetic reconnaissance and jamming against satellite, cellular and radio communication systems along with GPS spoofing and electronic warfare attacks." One of the tactics in Ukraine was to send menacing messages to Ukrainian troops on the ground, urging retreat.

Drones are useful for information capture, as well as disinformation. As the *New York Times* reported two years ago, US Immigration and Customs Enforcement officials have raised concerns that Chinese drones manufactured by DJI "may be sending sensitive information about American infrastructure back to China." Broader worries soon surfaced, leading the US Army to ban the use of all drones made by DJI. As *Foreign Policy* reported in August, the Army "may soon ban all Chinese-built drones and Chinese-manufactured components from military use."

As the drone future approaches, policy makers, industry leaders, security forces, and technology innovators must prioritize key questions: How will national governments secure emerging drone infrastructures as they grow exponentially over the next few years? How will data be kept secure? Can the hacking of drones and spread of disinformation be prevented? And, in the face of the most advanced drones, how will counter-drone systems react?

As one counter-drone expert recently warned, "'very few airports have any countermeasures or even processes in place to detect and defeat drones," and many existing technologies are underperforming or too risky to use. It will take a lot of work, and focused investment from authorities and industry, to create a safe and vibrant drone future—one that can harness the benefits of drones while keeping out the darker sides of the technology.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

James Rogers is DIAS Assistant Professor in War Studies within the Center for War Studies at the University of Southern Denmark, and Visiting Research Fellow within the Department of International Security Studies at Yale University.

Featured image is from Bulletin of the Atomic Scientists

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: James Rogers