AIR SECURITY

HACKING DRONES

Fleets of unmanned aircraft may soon scan terrain for forest fires and deliver FedEx packages. Yet drones' security flaws allow them to be readily hijacked with simple technologies

By Kyle Wesson and Todd Humphreys

Kyle Wesson is a Ph.D. candidate in electrical and computer engineering and a member of the wireless networking and communications group and the Radionavigation Laboratory, which develops new GPS-related technologies, at the University of Texas at Austin.

Todd Humphreys is a professor of aerospace engineering at the University of Texas at Austin, where he specializes in satellite navigation and directs the Radionavigation Laboratory.

AUGUST 2, 2010, A U.S. NAVY HELICOPTER WANDERED LAZILY INTO THE SKIES of the highly restricted airspace that extends like an invisible dome over the American capital. The event might have merited nothing more than a routine log entry for air-traffic controllers at Ronald Reagan Washington National Airport, except for one disturbing detail. The helicopter had no human pilot. The aircraft had no cutout space for windows, and its cockpit was filled with nothing more than electronic instrumentation. It was a drone.

The MQ-8B Fire Scout, a 1,429-kilogram, 9.7-meter-long drone, had experienced what investigators later called a "software issue," whereby its communications link had been severed with human operators, who sat helplessly in a ground-control room at Naval Air Station Patuxent River in Maryland. To make matters worse, the drone failed to execute software instructions that would have forced it to return to its base. The Fire Scout, used for reconnaissance off warships, had wandered into the same airspace that Air Force One uses when it takes off from and lands at Andrews Air Force Base.

After 30 minutes of jangled nerves, the operators reestablished the communications link and took back control. Afterward, a navy official tried to put a good face on the incident by praising the drone's performance during its unexpected detour—the autopilot system kept the aircraft flying straight and level, for instance.

The Fire Scout's errant journey provides a lesson about the immense security challenges that unmanned drones pose. These iconic reconnaissance and weapon systems have now begun to take on a range of peacetime tasks. The Federal Aviation Administration estimates that more than 10,000 unmanned aircraft will fly the U.S. skyways by 2020. Drones may soon be involved in search and rescue, crop dusting, power-line monitoring, scientific research, and myriad other uses.

The logic for deploying drones is compelling. By eliminating the need for a pilot and for outfitting a cockpit and cabin to accommodate a human crew and passengers, commercial air ventures that deploy drones stand to reap enormous savings. For instance, for the price of renting a human-piloted airplane for a power-line inspection campaign, a utility company could buy an entire unmanned aerial vehicle system to do the same job for years to come. The allure of drones has captured the attention of the largest U.S. corporations. FedEx founder and CEO Frederick W. Smith has talked about using drones to replace the company's fleet of package-delivery aircraft.

Even the U.S. Congress has begun to recognize the inevitability of the coming era of the commercial drone. When Congress passed the FAA Modernization and Reform Act of 2012 in February of that year, it directed the agency to draw up "a comprehen-

IN BRIEF

More than 10,000 unmanned aircraft are expected to be roving the skies by 2020 for search and rescue, power-line monitoring, scientific research and other uses that will become less costly than if the same tasks were carried out by humans.

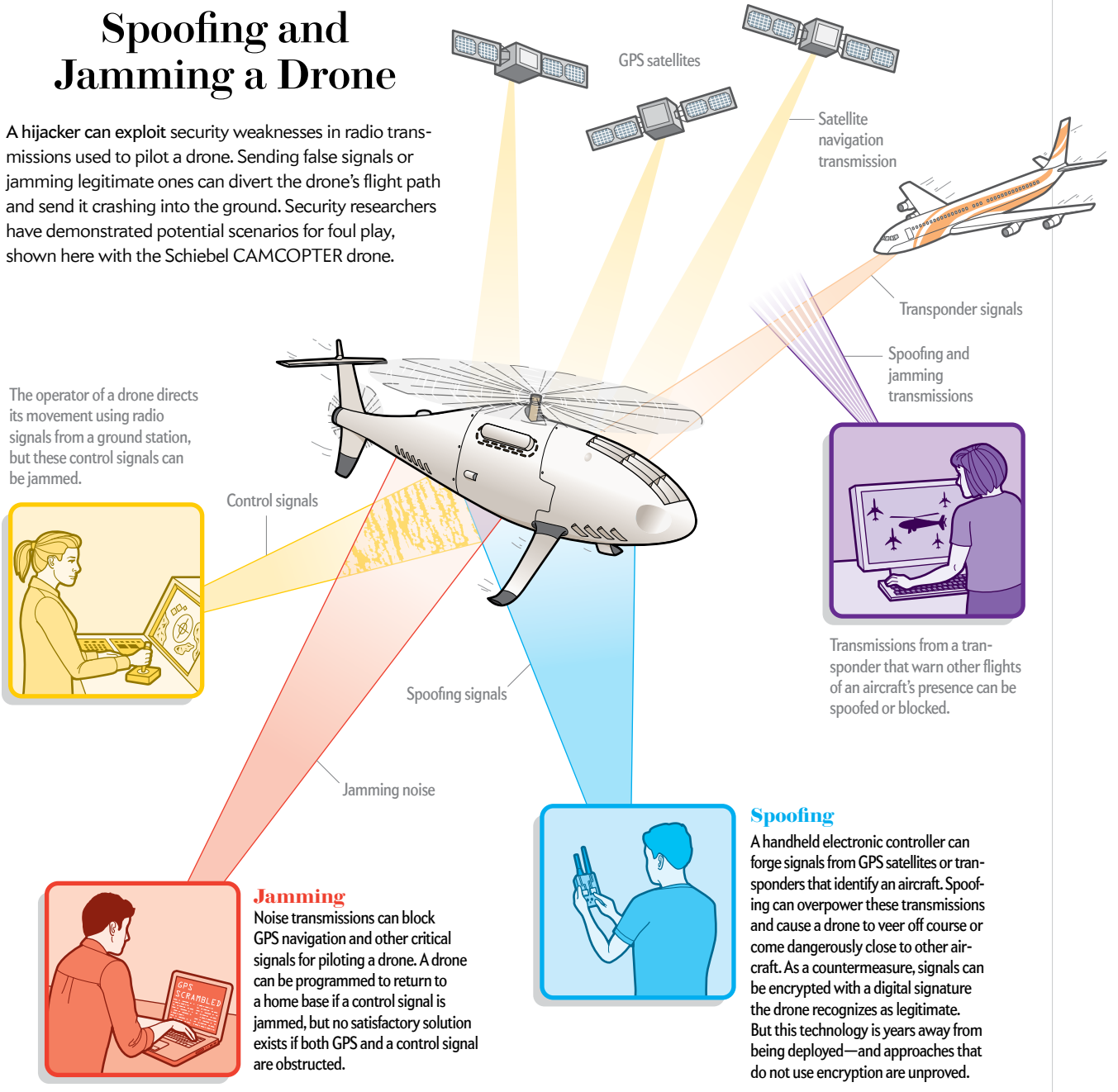
Swarms of drones traversing U.S. airspace pose elaborate security challenges that regulatory agencies are ill prepared to face. The Federal Aviation Administration's traditional role of keeping aircraft from colliding must be extended so that drones cannot be hacked.

Technical steps need to be implemented to ensure that radio signals to guide and control the aircraft are made secure from being hacked or jammed by wrongdoers who wish to take over piloting of the aircraft, perhaps to use it as a weapon of terror.

PRECEDING PAGES: DAN WINTERS

Spoofing and Jamming a Drone

A hijacker can exploit security weaknesses in radio transmissions used to pilot a drone. Sending false signals or jamming legitimate ones can divert the drone's flight path and send it crashing into the ground. Security researchers have demonstrated potential scenarios for foul play, shown here with the Schiebel CAMCOPTER drone.



Jamming
Noise transmissions can block GPS navigation and other critical signals for piloting a drone. A drone can be programmed to return to a home base if a control signal is jammed, but no satisfactory solution exists if both GPS and a control signal are obstructed.

Spoofing
A handheld electronic controller can forge signals from GPS satellites or transponders that identify an aircraft. Spoofing can overpower these transmissions and cause a drone to veer off course or come dangerously close to other aircraft. As a countermeasure, signals can be encrypted with a digital signature the drone recognizes as legitimate. But this technology is years away from being deployed—and approaches that do not use encryption are unproved.

sive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system" by 2015.

Unfortunately, the regulatory apparatus to manage what are essentially remote-controlled robots is unlikely to be ready in time. Drones expand the FAA's responsibilities beyond the agency's traditional role of ensuring that two Boeing 737s can keep their distance and can cope with the vicissitudes of inclement weather. Although the FAA's mission broadened considerably following the attacks of 9/11 to encompass aircraft security issues (it was the FAA that oversaw installation of reinforced cockpit doors, for instance), the prospect of swarms of drones in the skies poses more elaborate security challenges that the agency is currently ill equipped to face.

VITAL LINKS

THE MOST DAUNTING of these challenges is securing the drones' wireless links. To maneuver a drone up, down, sideways or forward requires three main communications links: the incoming navigation signal from GPS satellites, one or more signals to notify other aircraft of the drone's whereabouts, and a two-way link between ground and drone to pilot the aircraft. Disruption of any of these three can spell disaster. In some cases, more-

Illustration by Brown Bird Design

over, no clear technical solution exists to secure these links.

GPS is the linchpin of a drone's navigation system, complementing inertial guidance sensors, magnetometers, altimeters and even cameras. The GPS receiver takes pride of place in this navigation suite because, unlike the other devices, it works in all weather conditions while retaining pinpoint accuracy.

Unlike military GPS, the civil version is freely accessible and unencrypted. Continuously beamed to smartphones and sports watches alike, civil GPS is enormously popular but lacks any form of authentication, giving rise to a dangerous weakness. A fake signal can easily be substituted for the real one—a process known as spoofing.

In June 2012 at White Sands Missile Range in New Mexico, our laboratory demonstrated that vulnerability to GPS spoofing has serious consequences for unmanned aircraft. From about half a kilometer away, our spoofing device took command of an $80,000 drone. Our hand-built spoofer generated a nearly perfect forgery of the satellite signals that relay coordinates to the drone. Unable to distinguish between genuine and forgery, the drone picked our stronger signals for guidance.

Once fooled, the drone took positioning commands from our spoofing device. When signals beamed to the craft indicated falsely that it was rising vertically upward, the drone dutifully descended to maintain the desired altitude programmed into its autopilot system. By trying to adjust its location aloft based on erroneous data, the drone actually started to head directly toward the desert floor. It was only saved from crashing by an operator who was poised to override the spoofed commands and take manual control of the craft.

The danger of spoofing has been known for at least a decade. The Department of Transportation had previously documented the spoofing threat in a 2001 report, but policy makers and GPS manufacturers largely ignored that report's warnings until very recently, perhaps reasoning that an attack was too unlikely to warrant attention. Technical fixes, though, are not close at hand. Techniques that could protect GPS signals with cryptographic watermarking—a secure digital signature that identifies the origin of a signal and assures the content of its message—are years away from being implemented, and noncryptographic techniques that could be put in place sooner have yet to prove themselves

Spoofing is not the only threat that a GPS-reliant drone faces. It is also surprisingly easy to simply block reception of its navigation signals. Near the earth's surface, the signals are extraordinarily weak, having no more flux density—a measure of the signal's power—than light received from a 50-watt bulb at a distance of 22,000 kilometers. A jamming device can do its dirty work by generating noise in the same region of the radio spectrum occupied by the GPS signal. Almost any modern electronic system, even a laptop, can jam GPS signals inadvertently by sending noise into a GPS receiver at close range.

An intentional jamming device can be designed to be much more effective in confusing the drone's navigation system. In May 2012 operators in South Korea lost control of a 150-kilogram Schiebel CAMCOPTER S-100 reconnaissance drone that crashed into its ground-control station, killing an engineer and wounding two drone operators. North Korean GPS jamming directed into South Korea most likely had precipitated a sequence of events that led to the crash, including some mistakes made by the South Korean drone operators. As this incident and our spoofing demonstration make clear, secure navigation—resistant to spoofing and jamming—will be essential before aircraft without onboard pilots can fly safely in our skies.

A recent government report warns that technology has yet to be developed that gives a remotely piloted drone the ability to sense and avoid other aircraft in U.S. airspace.

COLLISION AVOIDANCE

THE POSSIBILITY of a midair crash between a drone and another aircraft will further complicate acceptance of drones. Traditional pilots use visual observation and radar to detect the presence of other aircraft and avoid collisions. But drones have a long way to go before they can provide that routine level of vigilance. "No suitable technology has been deployed that would provide [unmanned aircraft] with the capability to sense and avoid other aircraft and airborne objects" while complying with FAA regulations, the federal Government Accountability Office noted in a 2012 report.

Staying out of the way of other aircraft is especially challenging for small drones because they cannot accommodate existing airborne radar systems, which are prohibitively bulky and power-hungry. Visible-light and infrared cameras offer an inexpensive and reasonably effective alternative, but they cannot see through clouds.

One solution may ultimately come from Automatic Dependent Surveillance–Broadcast, or ADS-B. An ADS-B transponder broadcasts an aircraft's position and velocity every second and receives similar reports from nearby aircraft. By 2020 the FAA will require all licensed aircraft, big or small, to operate ADS-B transponders as part of a major overhaul of the air-traffic system. So long as all nearby aircraft—whether manned or unmanned—broadcast their positions and velocities through ADS-B transponders, a collision can be avoided by using these devices to find a safe flight path.

As with civil GPS, ADS-B has a serious Achilles' heel: its transmissions are not authenticated and thus can be faked. When ADS-B was first under development in the 1990s, security was a minor concern: the idea of broadcasting fake ADS-B signals was virtually unimaginable. Yet the cost and expertise to mount an ADS-B attack have become alarmingly low. In 2012 researchers at the Air Force Institute of Technology in Ohio showed that a variety of attacks using false signals could be readily coded and transmitted from either the ground or air

with a cheap antenna. Such a "false injection" attack could cause an aircraft to believe a collision was imminent.

The same technology is capable of issuing hundreds of false transmissions or preventing reception of legitimate messages. False ADS-B messages would tax small drones more than an airplane with a human pilot in the cockpit. Using onboard radar, a pilot may quickly verify whether or not a false aircraft is on a collision course, but a drone lacks a comparable backup.

The FAA wants to deal with the threat of false ADS-B messages through multilateration, a technique for locating the source of a transmission by measuring its relative arrival time at multiple ground receivers and then relaying that information aloft to an airplane. Reliable multilateration, however, depends on a precise alternative to GPS, an affordable version of which remains elusive.

Drones are controlled by a wireless tether, the so-called command-and-control radio link between the operator and the craft, which seems, at first glance, to present a lesser security challenge than do GPS or ADS-B. Secure communications protocols exist for these signals, which should suffice to ward off spoofers and other malefactors.

The signals can still be blocked, though. Loss of contact with a drone—what experts refer to as a lost link—from intentional jamming or a malfunction persists as a threat, and no satisfactory solution has emerged. Operators typically configure their drones with a lost link protocol (which prompts the aircraft, for example, to return to its base if the radio link is lost for more than 30 seconds), but such a protocol assumes that the drone's navigation system, itself subject to hacking, is operating properly and that its control system has not succumbed to a software glitch, as happened in 2010, when the Fire Scout helicopter headed toward Washington, D.C.

Another problem for regulators is finding areas of the radio spectrum that can be dedicated specifically for transmission of the command-and-control signals. Because of the scarcity of spectrum, many drones would have to resort to transmitting in unprotected radio bands used for other types of radio transmissions, which would render them susceptible to unintentional interference from the many electronic systems that already legally occupy these bands.

CHALLENGES AND MORE CHALLENGES

THE TECHNICAL COMPLEXITY of securing U.S. airways for drones bumps against a slow-moving, risk-averse bureaucracy—and a growing legislative backlash. Regulators must come to grips with a fundamental change in the way an aircraft is piloted. The ground-based drone operator, no longer a true pilot with hands on the yoke and eyes glued to the cockpit windshield, has to input a flight route into a computer, control the drone with a joysticklike device and monitor a series of communications links that wirelessly tether the aircraft to its base. At times during the course of a flight, the operator maneuvers the drone as if it were a remote-controlled hobby plane weighing, possibly, thousands of kilograms. At other moments, the drone may be flying completely autonomously.

The FAA, under the new congressional mandate, bears responsibility for making sure that the air-traffic system develops the technical wherewithal to ensure that a drone can safely share airspace with an Airbus 380 jumbo jet or a single-engine Piper Mirage. That means the FAA must come up with regulations to make certain that drones do not pose a danger if control or navigation signals are lost.

The FAA's unparalleled safety record is rooted, in part, in its intrinsic caution in adopting new technologies that could potentially disrupt the smooth functioning of the air-traffic system. Agency officials must now cope with the difficult challenge of regulating drones while they are already enmeshed in a broad-based modernization effort—the Next Generation Air Transportation System, or NextGen, that will replace radar with satellite navigation. On paper, the Department of Homeland Security would be expected to provide assistance, but officials there have stated repeatedly that they do not consider the drone issue to be part of their mission.

In crafting regulations, the FAA will have to engage in a difficult balancing of public safety considerations against the economic benefits of drone technology. A requirement that licensed, unmanned aircraft always be maintained within an operator's line of sight would make hijacking unlikely but would render drones utterly useless for many purposes. Drone technology also raises privacy issues that have never been within the FAA's purview. Privacy advocates and members of Congress are now demanding that the agency come up with regulations to deal with an aircraft that can hover above a suburban backyard while deploying high-definition cameras.

Many lawmakers, meanwhile, see no good reason to welcome the arrival of drones, having gained familiarity with them through footage on nightly newscasts that highlight their role in surveillance and missile strikes in conflict zones outside the U.S. In response, at least 42 states so far have proposed legislation imposing limits on drone use. Texas House Bill No. 912 makes it a misdemeanor for a drone operator to capture images of private property from an unmanned aircraft without the property owner's "express consent." At the federal level, the proposed Preserving American Privacy Act of 2013 would prohibit law enforcement from conducting drone-based surveillance without a warrant and would outlaw the use of armed drones by law enforcement or private citizens over the U.S.

The list of technical and regulatory demands—and the worries voiced by legislators at congressional hearings—will likely slow but fail to stop the adoption of drone technology. Some perspective is needed when considering the security of unmanned aircraft. Their vulnerabilities have longtime parallels in the world of aviation that retains captains and first officers in the cockpit. An airplane can still be hijacked, pilots coerced, communications links interrupted. Yet we continue to fly, not because we are unaware of the risks but because convenience trumps them. Drones will seek from us the same concession. SA

MORE TO EXPLORE

Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System. U.S. Government Accountability Office, September 18, 2012. www.gao.gov/products/GAO-12-981

Unmanned at Any Speed: Bringing Drones into Our National Airspace. Wells C. Bennett. Issues in Governance Studies series, No. 55. Brookings Institution, December 14, 2012. www.brookings.edu/research/papers/2012/12/14-drones-bennett

SCIENTIFIC AMERICAN ONLINE

Watch a video demonstration of a drone being hacked in New Mexico at ScientificAmerican.com/nov2013/hacked