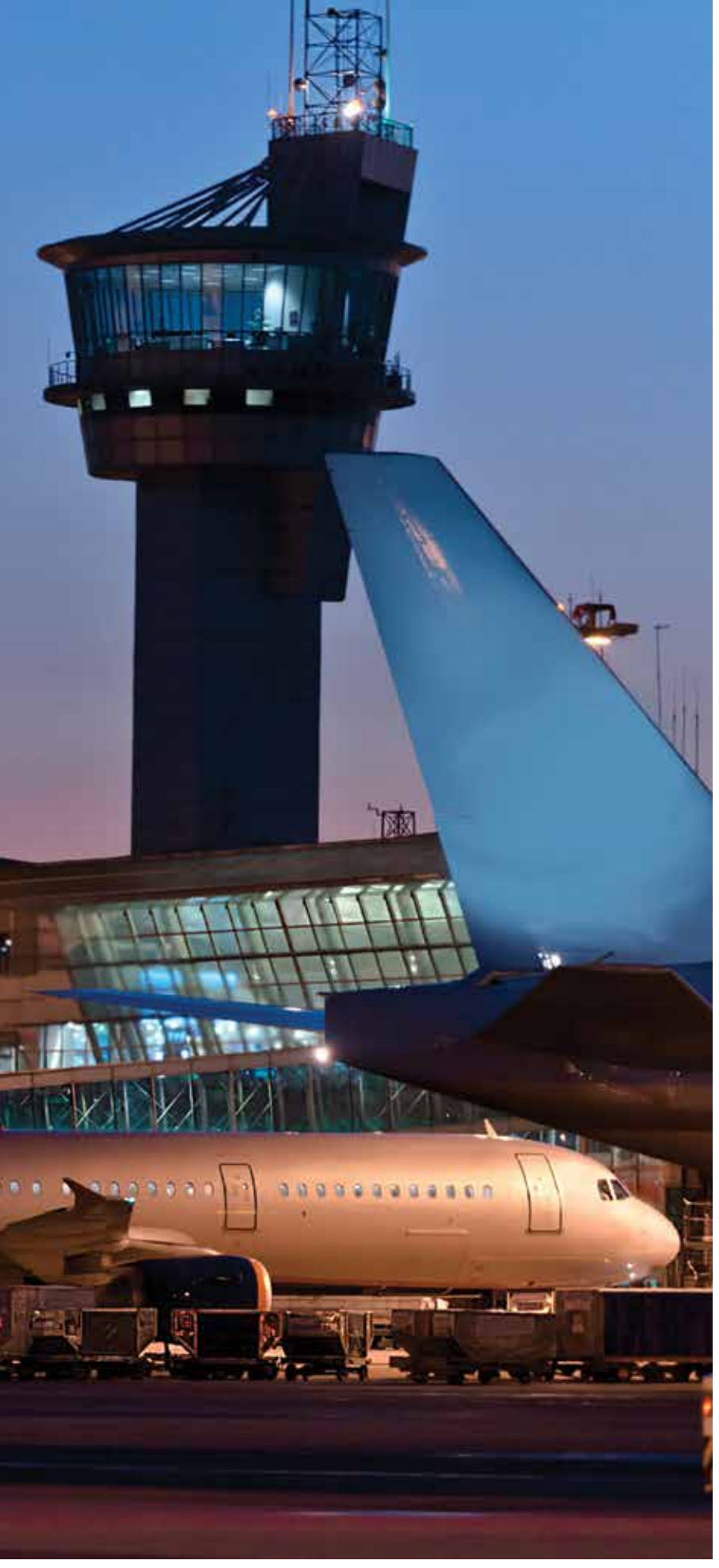
AIR NAVIGATION JITTERS

Those who have the job of protecting air travelers and assuring the security of military planes have deep concerns as the U.S. races toward the FAA's deadline for aircraft to broadcast their GPS locations and identities. U.S. agencies are looking for backups and technologies to improve the navigation security of the FAA's NextGen air traffic initiative. Jan Tegler spoke to government and industry officials about the problem.

BY JAN TEGLER | wingsorb@aol.com



Imagine you're on a commercial airliner bound for Chicago's O'Hare International Airport. The flight is progressing well, with air traffic controllers tracking the plane not by radar but by a new technique in which the plane transmits its GPS coordinates and other data once a second from an Automatic Dependent Surveillance-Broadcast Out radio.

Unbeknownst to anyone, a bad actor armed with a computer and maybe a commercially purchased ADS-B Out unit has injected false information into the ADS-B broadcast as the plane approaches O'Hare.

"It's called spoofing," says cybersecurity expert Bob Gourley, "and the threat is very real."

By design and international agreement, ADS-B signals are unencrypted and are available to anyone with the right kind of receiver. Trusting all of the world's air navigation services to manage encryption keys was viewed as too daunting a task. In fact, with thousands of planes now equipped for ADS-B Out, online services such as FlightAware.com are starting to provide free real-time in-flight tracking of commercial and private aircraft. FlightAware even sells software so that individuals can build their own ADS-B ground stations.

Back to our hypothetical scenario. Having been easily spoofed, air traffic controllers tell the pilot in command to fly in a direction and altitude that could potentially put the aircraft on a collision course with other airplanes.

This scenario, which I constructed with the aid of Gourley, is among the nightmares that are hot on the minds of security experts as the aviation industry races toward the FAA's Jan. 1, 2020, mandate for installation of ADS-B Out. Spoofing is just one concern. Jamming is another. Even when ADS-B works fine, the Pentagon has balked at its aircraft routinely broadcasting ADS-B Out, because of the tactical knowledge a potential adversary could gain, even during peacetime.

The FAA likes ADS-B Out because, along with other digital improvements, it would empower controllers to safely pack the 5,000 aircraft in U.S. skies (at peak times) closer together on straighter routes. The air transportation industry could meet rising demands for air travel and minimize carbon emissions as the demand soars. The technology is at the heart of the FAA's Next Generation Air Transportation System, called NextGen. Gourley, co-founder and chief technology officer of OODA LLC in Virginia, a cybersecurity and artificial intelligence consultancy, counts himself among those who worry about the security of all this.

"I have seen proposals on ways to mitigate [vulnerability to spoofing] but I have not seen a government action plan that makes me confident that we're going to eliminate the threat."

Radars vs. ADS-B

Specifically, the FAA mandate calls for owners and operators of civilian, commercial and military aircraft flying in controlled airspace — the airspace near sizeable airports and cities — to install ADS-B equipment.

Total reliance on ADS-B would be a dramatic shift. For decades, American air traffic controllers have relied mainly on two kinds of radars. Primary radar antennas at FAA ground stations across the nation send out electromagnetic waves that reflect from the surfaces of aircraft at distances of up to 100 kilometers to determine their distance and azimuth, the term for direction of travel.

A second radar antenna attached to the top of the primary radar triggers the transponders on airliners to report their altitudes, identification codes and any emergency conditions.

Primary radars are vital to national airspace security because they provide position information for "noncooperative" aircraft, meaning those without transponders or with their transponders turned off. These could include hostile aircraft violating U.S. airspace.

The radar system works well, but it is not as precise as GPS, and so controllers must keep a greater separation from aircraft than will be necessary once an ADS-B Out network is fully in place with each plane broadcasting every second.

Early on, there was supposed to be an even clearer cost benefit. Retiring a large number of ground radar stations would save money in addition to the air traffic management benefits of ADS-B. This thinking changed after the Sept. 11 terrorist attacks in New York and Washington, D.C. "The post-9/11 requirement to maintain primary active radar surveillance has decreased the primary benefit-to-cost ratio that was used to initially justify moving to ADS-B in the first place," says George Dononhue, the fomer FAA associate administrator who was responsible for initiating the ADS-B system, by email. The rollout of ADS-B has nevertheless continued. A total of 68,743 aircraft in the U.S. were equipped with ADS-B as of Feb. 1, according to FAA data. This represents somewhere near 50 percent of the American aviation fleet that must be equipped by the 2020 deadline, based on my conversations with the Aircraft Owners and Pilots Association, the National Business Aviation Association, the General Aviation Manufacturers Association and Southwest Airlines.

Once an aircraft is equipped for ADS-B Out, it is required to be used on every flight, says Rune Duke, the senior director of government affairs at the Aircraft Owners and Pilots Association.

Pentagon remains wary

Military strategists in the U.S. don't like the idea of routinely broadcasting position, heading, ground speed and identity. They continue to talk with the FAA regarding when and how military aircraft must broadcast.

The Defense Department "has significant operational security concerns associated with the broadcast nature of ADS-B and other advanced transponder technologies," says Rowayne Schatz, the executive director of the Defense Department's Policy Board on Federal Aviation. Potential adversaries could learn about U.S. tactics by monitoring nonwartime military flights, he says.

Schatz is the Pentagon's liaison with the Transportation Department and the FAA on federal aviation issues, including aviation cybersecurity. He

ADS-B air traffic is indicated by white diamonds on the left hand side of this cockpit screen. A receiver picks up the signals and relays them to the G600 TXi display, which can be installed on single- and twin-engine general aviation aircraft.

Garmin

▲ **U.S. military air** traffic controllers work in the control tower at Holloman Air Force Base, N.M. Pentagon strategists are balking at routinely transmitting the GPS cooridnates of U.S. military aircraft as part of the FAA's Next Generation Air Transportation System.

U.S. Air Force

notes that the Defense Department is also concerned about broader risks to the national airspace system due to the "fragility of the GPS signal" and the risk associated with "using GPS-only for an aircraft's position, altitude, heading and ground speed."

Schatz is among those who think navigation radars will be needed for the foreseeable future as a backup to ADS-B. The question is how to keep the secondary radars, in particular, technically and financially viable for years to come. Schatz says a research effort called Spectrum Efficient National Surveillance Radar, or SENSR, may provide the answer. The goal is "to be able to recapitalize our radar system and keep some ground-based secondary radar as a backup for satellite-based NextGen," he says. Here's how it would work. The FAA, Defense Department, Department of Homeland Security and NOAA are researching the possibility of consolidating aircraft tracking and weather monitoring frequencies into a new part of the radio spectrum. This would free up bandwidth that could be auctioned to the private sector to pay for the SENSR radars that would operate in the consolidated spectrum. In as little as three to five years, Schatz says, SENSR could be in use alongside ADS-B.

Having SENSR as backup would provide reassurance to security experts, given all the warnings issued by reputable groups about the vulnerabilities of ADS-B and GPS. The list includes a January 2018 report by the congressional Government Accountability Office; a March 2018 report by the Radio Technical Commission for Aeronautics (a standards organization that works with the FAA); and a 2017 report from the Air Traffic Controllers Association.

Consider man-in-the-middle attacks in which the unencrypted packets of ADS-B information are

forged by hackers as the information travels to and from ADS-B ground stations. That's the scenario depicted in our hypothetical flight to Chicago. Another threat would be distributed denial-of-service attacks in which multiple forged packets overwhelm ADS-B ground stations, potentially causing them to go off the air. Gourley says jamming and denial-of-service attacks are more sophisticated than spoofing and therefore harder to carry out, "but they are doable."

Last July, the FAA and the Pentagon signed an agreement committing each side to broader discussions of security and structural risks related to NextGen.

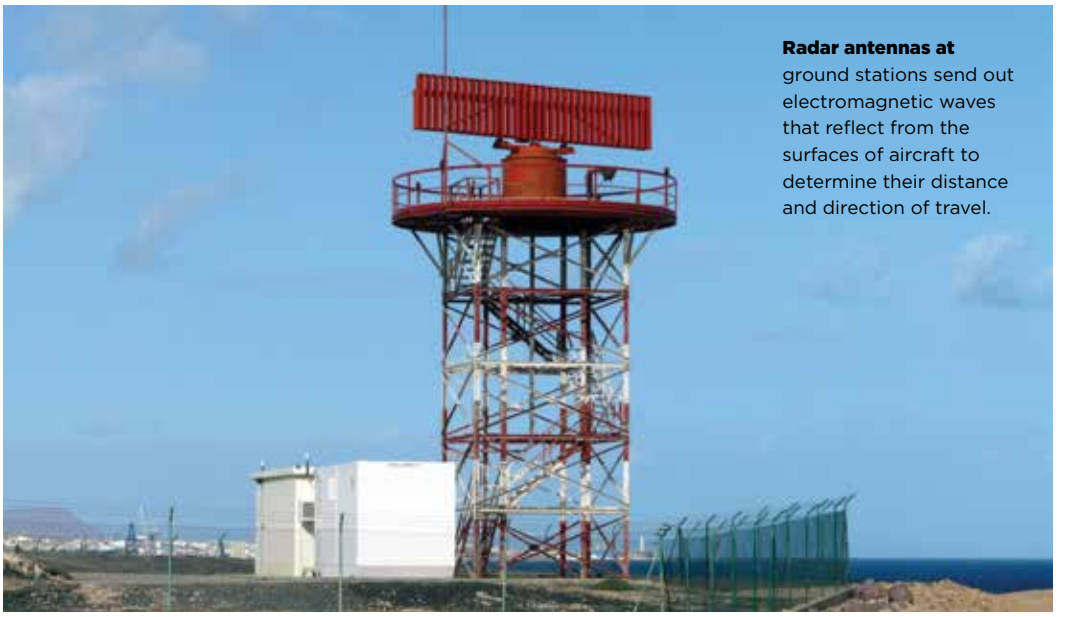
The FAA and Pentagon declined to provide a copy of the document, but Joe Kirschbaum, director, defense capabilities and management for the Government Accountability Office, says the congressional watchdog has reviewed earlier agreements between the FAA and the Defense Department pertaining to NextGen. According to Kirschbaum, "none ever talked about security."

Wake-up call for FAA

I reached out to the FAA's NextGen Office to discuss the potential security risks posed by ADS-B and other NextGen technologies but the agency said, "We are not conducting any interviews nor will we be able to address your questions at this time."

Nevertheless, Schatz told me that the FAA is "starting to reassess some of the initial thoughts" about going to an air traffic surveillance system

▲ **A formation of F-35As** flies over the Utah Test and Training Range during training. The U.S. Defense Department wants to exempt some military aircraft from the FAA requirement to routinely broadcast position and other details in Automatic Dependent Surveillance-Broadcast transmissions.
U.S. Air Force



Radar antennas at ground stations send out electromagnetic waves that reflect from the surfaces of aircraft to determine their distance and direction of travel.

reliant solely on GPS and ADS-B Out, based on the fragility of satellite-based navigation. Donohue, the former FAA official, noted that when ADS-B was conceived, "it was before 9/11 and before our current concerns and understanding of the cyber threat. I now now share the DoD concerns." Since the ADS-B rule was finalized in 2010, the FAA has touted the economic benefits of switching away from radar surveillance. Cost savings from dismantling the network of ground radar stations that still provide aircraft position information was chief among the advantages cited by the agency. Money saved would help pay for the NextGen transition — an effort that had consumed approximately $7.4 billion by the end of 2016, according to GAO estimates. An FAA business case estimate for NextGen in 2016 pegged its total estimated cost at nearly $21 billion.

However, the Defense Department expects ground radars to remain an important component of the national airspace system "for the foreseeable future," according to Schatz.

He says the Pentagon and the FAA are "working very closely to identify a minimum operating network of radars, both primary and secondary, to ensure the surveillance infrastructure meets the mission requirements of all federal departments."

Schatz says maintaining part of the FAA's current radar surveillance network makes sense as a backup to ADS-B. "Utilizing and maintaining cooperative and noncooperative surveillance technologies provides a robust and resilient infrastructure that is not overly dependent on any single component."

Finding security solutions

The Defense Department, Department of Homeland Security and FAA established an Aviation Cyber Initiative to address the security issues raised by NextGen and ADS-B. As Schatz puts it, the goal is to "reduce cybersecurity risks and improve cyber resilience" in the aviation sector. The agencies are examining potential vulnerabilities from "out-ticketing and reservations centers to aircraft with ADS-B signals and the ability to make sure an aircraft is not able to be tampered with from the ground through an ADS-B signal," he adds.

Tampering is far from the Pentagon's only concern. Schatz gave me an example of why the military strategists don't want to broadcast positions even in peacetime. "If you have F-35 fighters flying out to a local training range, we don't want someone to be able to pull up their website and get an ADS-B feed from those aircraft and be able to watch the tactics, techniques and procedures that they're employing on that training range," he says.

Schatz says the Pentagon is working through procedures with the FAA to allow those aircraft to take off from their home station, fly out to the range and then be able to turn off that equipment for that part of the mission. "There are others we will not equip [with ADS-B] because of the nature of their mission — we really don't want to broadcast where they are."

He explains that the two agencies have agreed to accommodate U.S. military national security missions by exempting military aircraft from the requirement to broadcast ADS-B depending on the nature of their mission.

"We are committed, where it makes operational sense, to make sure that our aircraft are broadcasting (ADS-B Out)," Schatz says. "A lot of our cargo-type aircraft, our air refueling tankers — they tend to operate more in the parts of the national airspace that are more congested with other traffic. We're committed and planning still to equip those aircraft ." ★