ILLUSTRATION BY *SECURITY MANAGEMENT*; ISTOCK

FLIGHT RISKS

UNMANNED AERIAL SYSTEMS ARE BEING INCREASINGLY ADOPTED BY PUBLIC AND PRIVATE SECTOR ORGANIZATIONS. BUT THEY COME WITH CYBERSECURITY RISKS. **BY MEGAN GATES**

IT STARTS OUT AS AN IDEA with the best intentions. Britain's bee population is collapsing, so a private company strikes a deal with the government to provide minuscule robotic drones to pollinate plants and save the nation's agriculture—and humanity itself.

But this good idea in "Hated in the Nation"—a buzzy episode in the science fiction anthology TV series *Black Mirror*—soon devolves into unintended consequences. The drone bees' source code can be compromised, and instead of simply spreading pollen from plant to plant, they begin to target and kill humans who engage in public shaming on social media using the hashtag #DeathTo.

While fantastical, the episode points out the dangers of using tools without understanding their vulnerabilities. Drones, or unmanned aerial systems (UAS), have become increasingly used operational tools over the past several years. Goldman Sachs predicted that by 2020, there would be a $100 billion market opportunity for drones, with high demand from the commercial and civil government sectors.

"Drones are already generating climate data, monitoring the borders, and more—and they're just scratching the surface of their commercial potential," Goldman Sachs said in an industry insights report.

The U.S. Department of Interior (DOI) is one of these users, with a fleet of UAS to meet statutory obligations such as emergency management, fighting wildland fires, conducting search and rescue, surveying federal land, collecting research data, and assisting law enforcement. It also uses drones to assess, collect, and maintain information on critical infrastructure, including energy, transportation, and defense-related systems.

In January 2020, U.S. Secretary of the Interior David Bernhardt signed an order grounding all of the department's nonemergency unmanned aircraft systems fleet operations.

"Drones are important to critical Department of the Interior missions, such as combating wildfires and conducting life-saving search and rescue operations; however, we must ensure that the technology used for these operations is such that it will not compromise our national security interests," said DOI spokesperson Carol Danko. Drone operations could continue, however, for fighting wildfires, search and rescue, and dealing with natural disasters that threaten life or property.

Bernhardt issued the order during an internal review of the department's drone fleet's cybersecurity, technology, and domestic production concerns. In a follow-up with *Security Management*, DOI spokesperson Conner Swanson says that Bernhardt received classified briefings on security concerns related to the department's drone fleet in late 2019.

"Currently, we are working hand-in-hand with experts in the executive branch to coordinate a thorough assessment of certain DOI drones and scanning for any potential national security threats," Swanson explains. "This thorough review will ensure that a robust, secure, and reliable source of unmanned aerial systems is available to meet DOI's multiple needs."

Swanson did not say what specific threats the DOI was examining or confirm when the department would complete its review. He also did not elaborate on whether the department had guidance for the public and private sectors, which could be using drone systems similar to the department's to carry out operational surveillance and inspections.

The decision, however, was seen by some as a political maneuver by the Trump Administration to target Chinese drone manufacturers, like DJI Technology, which supplies approximately 20 percent of DOI's grounded drone fleet.

In a statement released shortly after the DOI order, DJI said it was "troubled" by the secretary's order that essentially prohibits employees from operating drones made by foreign-owned companies or those made with foreign-manufactured components based on "undefined cybersecurity concerns."

Prior to the order, DJI worked with the department, cybersecurity professionals, and NASA officials to create a drone solution that met DOI's security requirements.

"The result of this collaboration was our Government Edition (GE) solution, which provides additional safeguards, so drone data is not intentionally or accidentally stored with unauthorized parties," DJI said. "Just a few months later, at the request of the Department of Homeland Security, our GE drones were independently evaluated a second time by the Department of Energy's Idaho National Lab, which also found no areas of concern related to drone leakage."

DJI has worked to increase the security features on its drones, even those not used by the U.S. federal government, says Michael Oldenberg, DJI's senior communications manager for North America.

One feature is local data mode, which allows drone users to eliminate the connection and data transfer between the drone operator's mobile device (connected to the drone) and DJI's servers.

"We developed that for customers doing critical infrastructure inspection as an added assurance that no data is leaving that mobile device while they're using the DJI app," Oldenberg explains.

DJI also offers to host flight data on server infrastructure hosted by Amazon's AWS and the Alibaba Cloud in the United States for its customers outside of mainland China. Customers can use this option to upload the GPS paths of drone flights, along with thumbnails of images taken while the drone is in flight.

Oldenberg says some customers are interested in having this option for auditing and compliance reasons. For instance, a utility operator could use the saved data to show an auditor that an inspector conducted a specific flight path.

And any data that is stored on DJI-controlled servers is not synchronized or sent to other third-party companies. Users who want to delete any data DJI has stored for them can contact DJI to set that in motion, according to a recent white paper on the company's security policies.

Oldenberg says DJI takes users' data security concerns seriously and that the DOI ban is the result of the ongoing geopolitical trade war between the United States and China.

We find that nearly all DHS components and offices could become victims of a drone-led botnet or data exfiltration attack.

"It has nothing to do with the security or performance of DJI's drones—or any drone manufactured in China," he adds.

However, cybersecurity concerns related to the use of commercially available drones remain. A recent analysis by the RAND Corporation of the U.S. Department of Homeland Security's (DHS) use of drones found that the department is vulnerable to drone-enabled cyberattacks.

"We find that nearly all DHS components and offices could become victims of a drone-led botnet or data exfiltration

UAS-RELATED CYBER THREATS

In a recent analysis, *How to Analyze the Cyber Threat from Drones,* the RAND Corporation categorized unmanned aerial system-related cyber threats into four categories:

U.S. Department of Homeland Security and its allies' unmanned aerial systems (UAS), with compromised systems as cyber weapons:

1. Used to disable adversary networks through interference
2. Used to harvest credentialing information
3. Used for probing and data collection

U.S. Department of Homeland Security and its allies' UAS, with UAS as cyberattack targets:

1. Could spoof legitimate law enforcement systems to misrepresent location information or collected data
2. Used to take over, lockdown, or take out law enforcement UAS
3. Used to steal probe data, UAS identity, or network access

Adversarial and other UAS, with UAS as cyber weapons:

1. Used in a botnet attack
2. Used to create a cascading infection of Internet of Things through UAS

Adversarial and other UAS, with UAS as cyberattack targets:

1. Used to distort or destroy probe data
2. Used to take over, lockout, or take down adversarial UAS

attack," according to the report, *How to Analyze the Cyber Threat from Drones*. "These offices and components all have physical locations where sensitive data and wireless networks are prevalent, making them targets for these types of attacks. UAS that have loitering capabilities—for example, those that can land and takeoff again after some period of time—allow this type of covert attack, increasing risk to unhardened systems."

Future attack methods could also target DHS employees' personal devices or home networks to gain entry to DHS systems "either wirelessly or by an employee connecting an infected device to a DHS laptop," the report's authors cautioned.

To mitigate against threats, the authors said DHS needs to develop a coherent UAS cyber strategy—in partnership with senior policymakers, cybersecurity experts, and other government and law enforcement agencies.

"DHS should invest in operating a UAS test range (or ranges) in collaboration with the private sector, national labs, and other government stakeholders such as the Federal Aviation Administration," the report explained. "This step would help ensure industry compliance with safety and security protocols, and would promote interagency coordination."

My advice to people is to really understand your goal: What are you trying to accomplish using an unmanned system?

The report also recommended DHS prioritize the most critical vulnerabilities and find ways to mitigate them, including monitoring developments in counter-UAS systems.

"A coordinated and updateable system of monitoring and intervention is likely to be required as the innovation cycle of cyberattack and countermeasure ensures that even hardened systems cannot be guaranteed immune to attack," the authors wrote.

Additionally, DHS will need to monitor UAS adoption and anticipate how this will affect its security posture.

"As UAS are used in a wider range of activities, the number of legitimate-use UAS that are airborne at any given time will increase," according to the report. "From the perspective of threat mitigation, one of the most important tasks in this new UAS-dense environment will be distinguishing licit from illicit activity."

As of *Security Management*'s press time, the DOI had not issued findings from its review. Regardless, nongovernment users should be thinking about the security of their drone systems and their level of exposure, says James Acevedo, CPP, founder of StarRiver Inc., who specializes in drone security and regularly builds his own.

Acevedo first raised concerns about drones that were manufactured in China and the need for greater cybersecurity protections at the 2014 ASIS Seminar and Exhibits (now GSX) in Atlanta. His biggest concern at the time was that these drones were designed to be connected to smartphones. Because of their connection to the Internet, Acevedo says users could unknowingly be uploading more flight data and sensitive information than they intended to—creating a security risk.

"My advice to people is to really understand your goal: What are you trying to accomplish using an unmanned system? What's the goal?" he says. Once users have their purpose for the system determined, they can consider where the drone is manufactured, what kind of data it aggregates, and their ability to access that data and delete it.

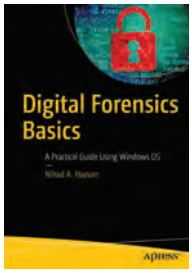
"People are going to these drones like the ones made by DJI because they're user friendly and intuitive," Acevedo says. "But there are risks attached to it. You should conduct a risk assessment, and if you're willing to accept that risk—fine. But realize that your system could be compromised at some point in time." ◼

@ To read the reports mentioned in this article, visit SM Online.

DIGITAL FORENSICS BASICS

BY NIHAD A. HASSAN. Apress; apress.com/us; 360 pages; $39.99.

FOR ANY NETWORK OF SIGNIFICANT SIZE, the question is not if there will be a breach, but when the breach will happen. And when that breach occurs, there are generally two goals at hand—get the intruders out and determine who they were.



In *Digital Forensics Basics: A Practical Guide Using Windows OS,* author Nihad Hassan has written a practical, hands-on guide that can help the novice user get up to speed on Windows forensics.

The book starts with an introduction to the core concepts of digital forensics and technical concepts around file systems. It then progresses to the steps needed to investigate an incident, including gathering and analyzing data. The author explores several software tools that can be used in the investigation process.

Written for those with little to no background in digital forensics, the book walks the reader through the various actions involved. The book covers only the Microsoft Windows operating system; therefore, if the affected systems are Macintosh or Linux, this book does not address them.

While far from a definitive reference, this book is a reliable guide. For those looking for a practical introduction to digital forensics, this is an excellent book to start with.

REVIEWER: *Ben Rothke, CISSP (Certified Information Systems Security Professional), is a senior information security specialist with Tapad, Inc.*