SUBMITTED STATEMENT FOR THE RECORD OF

KATHRYN WALDRON
RESEARCH ASSOCIATE, NATIONAL SECURITY AND CYBERSECURITY POLICY
R STREET INSTITUTE

BEFORE THE

SUBCOMMITTEE ON SECURITY
COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION
UNITED STATES SENATE

HEARING ON

DRONE SECURITY: ENHANCING INNOVATION AND MITIGATING SUPPLY CHAIN RISKS

JUNE 18, 2019

DRONE SECURITY: ENHANCING INNOVATION AND MITIGATING SUPPLY CHAIN RISKS

Chairman Sullivan, Ranking Member Markey and members of the Committee:

Thank you for holding this hearing on drone security, and particularly for focusing on innovation enhancement and supply chain risk mitigation. In general, a strong national security strategy must simultaneously enhance innovation and mitigate supply chain risks. The United States must achieve both of these objectives even though they may appear, at times, to be in tension with each other. To encourage innovation we may need to relieve tech startups and more established companies from regulations that unnecessarily discourage entrepreneurship, creativity and investment. At the same time, Congress must protect the government from the use of unprotected, easily hacked technologies. Navigating this tension can be difficult for both companies and policymakers. This hearing is, therefore, both timely and important.

My name is Kathryn Waldron, and I am a research associate with the national security and cybersecurity team at the R Street Institute. The R Street Institute is a nonprofit, nonpartisan public policy research organization, whose mission is to engage in policy research and outreach to promote free markets and limited, effective government. Our scholars have written extensively on emerging technologies, cybersecurity and the national security implications of today's global supply chain.

According to the Department of Homeland Security's (DHS) website, drones—also referred to as unmanned aircraft systems (UASs) or unmanned aerial vehicles (UAVs)—may pose a variety of national security risks from numerous threat actors, including reconnaissance, intellectual property theft and even transportation of contraband or weaponized payloads.[1] Last October, FBI Director Christopher Wray testified before a Senate hearing, stating, "The FBI assesses that, given their retail availability, lack of verified identification requirement to procure, general ease of use, and prior use overseas, UAS will be used to facilitate an attack in the United States against a vulnerable target, such as a mass gathering."[2] Yet drones also promise to improve our daily lives in myriad ways, ranging from faster delivery services to assistance with search and rescue operations. In order to promote American technological leadership without unduly discouraging innovation, any effective policy solution must, among other things, seek to promote the adoption of security standards and education regarding supply chain and cybersecurity risks while avoiding a heavy regulatory hand.

---

[1] "Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges Fact Sheet," Department of Homeland Security, February 2017.
https://www.dhs.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf.

[2] Rich Schapiro and Tony Capra, "Terrorists likely to attack U.S. with drones, says FBI director," *NBC News*, October 10, 2018.
https://www.nbcnews.com/politics/national-security/terrorists-likely-attack-u-s-drones-says-fbi-director-n918586.

Cybersecurity, Supply Chain Risks and Drones

Unmanned aerial vehicles, commonly known as drones, UAVs or UASs, are a fast growing market. This is not surprising, as drones have a variety of positive and lawful uses, including weather forecasting, parcel delivery, crop monitoring, safety inspecting, rescue operations and aerial photography.[3] American businesses and individuals have embraced drones; estimates from the Federal Aviation Administration (FAA) suggest that 7 million hobbyist and commercial drones will have been sold by 2020.[4] Drone use has also become prevalent in U.S. government agencies, ranging from the Department of Defense to local police forces, despite intense debate over the ethical and legal justifications of some military and police uses, such as drone strikes and surveillance.

However, drones that lack proper security controls could be avenues for intellectual property theft and serious national security threats. Just last month the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued an alert warning that commercial drones manufactured by Chinese suppliers may be collecting and transmitting information back to China.[5] The alert did not specify any particular manufacturers of which to be wary. But it is worth noting that approximately 80 percent of drones used in the United States are made by Chinese drone manufacturer SZ DJI Technology Co., Ltd. (often known simply as DJI), based in Shenzhen, China.[6]

Founded in 2006, DJI specializes in drones used for aerial videography and photography. DJI drones have been used to film such popular television shows as *The Amazing Race*, *American Ninja Warrior*, *Better Call Saul* and *Game of Thrones*, among others.[7] DJI has garnered national attention on several occasions. In 2015, a DJI drone crashed on the south lawn of the White House. The drone was being operated by a member of the National Geospatial-Intelligence Agency (NGA) while under the influence of alcohol.[8] In response to the incident, the company installed firmware to create certain "no-fly" zones that would prevent future repetitions of the crash, as well as prevent drones from crossing national borders.

---

[3] Divya Joshi, "Exploring the latest drone technology for commercial, industrial and military drone uses," *Business Insider*, July 13, 2018. https://www.businessinsider.com/drone-technology-uses-2017-7.
[4] Brandi Jewett, "Drone Sales Could Reach 7 Million by 2020, FAA Says," *Government Technology*, March 25, 2016. https://www.govtech.com/public-safety/Drone-Sales-Could-Reach-7-Million-by-2020-FAA-Says.html.
[5] David Shortell, "DHS warns of 'strong concerns' that Chinese-made drones are stealing data," *CNN*, May 20, 2019. https://www.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html.
[6] China Power Team, "Is China at the forefront of drone technology?" Center for Strategic and International Studies, May 29, 2018. https://chinapower.csis.org/china-drones-unmanned-technology/.
[7] Frank Schroth, "DJI Wins 2017 Emmy for Technology and Engineering," *Dronelife*, August 31, 2017. https://dronelife.com/2017/08/31/dji-wins-2017-emmy-technology-engineering/.
[8] Staff, "Drone maker DJI bans Washington flights after White House crash," *BBC*, January 28, 2015. https://www.bbc.com/news/technology-31023750.

In 2017, a memo from the U.S. Immigration and Customs Enforcement's (ICE) SAC Intelligence Program in Los Angeles assessed "with moderate confidence that Chinese-based company DJI Science and Technology is providing U.S. critical infrastructure and law enforcement data to the Chinese government. SIP Los Angeles further assesses with high confidence the company is selectively targeting government and privately owned entities within these sectors to expand its ability to collect and exploit sensitive U.S. data."[9] The memo argued that DJI deliberately pitched itself to American critical industries and key federal, state and local law enforcement agencies, while employing aggressive dumping tactics to undercut the rest of the drone market. The memo also states, "the Chinese government is likely using information acquired from DJI systems as a way to target assets they are planning to purchase." The only example the memo provided was of Chinese companies buying vineyards in California shortly after a local wine producer started using DJI drones to monitor grape crops. DJI denied any unlawful spying on its part, saying the memo was "based on clearly false and misleading claims."[10]

Also in 2017, the United States Army released a memo prohibiting the use of DJI products out of concern for cybersecurity vulnerabilities. The memo stated:

> DJI Unmanned Aircraft Systems (UAS) products are the most widely used non-program of record commercial off-the-shelf UAS employed by the Army. The Army Aviation Engineering Directorate has issued over 300 separate Airworthiness Releases for DJI products in support of multiple organizations with a variety of mission sets. Due to increased awareness of cyber vulnerabilities associated with DJI products, it is directed that the U.S. Army halt use of all DJI products. This guidance applies to all DJI UAS and any system that employs DJI electrical components or software including, but not limited to, flight computers, cameras, radios, batteries, speed controllers, GPS units, handheld control stations, or devices with DJI software applications installed.[11]

In 2018, the Department of Defense (DOD) banned the use of all commercial off-the-shelf unmanned aircraft services. According to the DOD, "[o]n May 14, 2018 the DoD Inspector General found that DoD has not implemented an adequate process to access cybersecurity risks associated with using commercial-off-the-shelf (COTS) Unmanned Aerial Systems (UAS). Effectively

---

[9] SAC Intelligence Program Los Angeles, "(U) Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government," U.S. Immigration and Customs Enforcement, Department of Homeland Security, August 9, 2017. https://info.publicintelligence.net/ICE-DJI-China.pdf.
[10] Paul Mozer, "Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say," *New York Times*, November 29, 2017. https://www.nytimes.com/2017/11/29/technology/dji-china-data-drones.html.
[11] Malek Murison, "DJI, the US Army and 'Cyber Vulnerabilities'," *Dronelife*, August 5, 2017. https://dronelife.com/2017/08/05/dji-us-army-cyber-vulnerabilities/.

immediately, you must suspend purchases of COTS UAS for operational use until the DoD develops a strategy to adequately assess and mitigate the risks associated with their use."[12]

These two DOD memos address two separate but intertwined national security threats. The first is that drone suppliers from countries with a history of unlawful surveillance and economic espionage may be designed to gather and send information back to the manufacturer and potentially its government, which may be an adversary of the United States. The second is that commercially available drones often lack sufficient cybersecurity protections and are therefore likely to be compromised by various malicious cyber actors. Customers unaware of their supplier's security standards may thereby inadvertently be putting themselves at risk. Both of these concerns will be addressed below.

Supply Chain Risks Specific to Chinese Suppliers

Supply chain integrity is not an issue unique to drones. The publicly discussed concerns over Chinese telecommunications companies Huawei and ZTE and corresponding allegations that the Chinese government uses Chinese companies to unlawfully spy on Americans resulted in Congress banning both Huawei and ZTE from the federal supply chain.[13] Huawei and ZTE, while two of the most prominent examples, are likely not the only threat to the government's supply chain. The looming adoption of 5G technology has drawn attention primarily to telecommunication companies, but supply chain threats can come from any interconnected technological system.

When evaluating the likelihood of any type of supply chain risk, it is crucial to consider both the history and structure of the supplier, including previous instances of cyber espionage and close ties with hostile foreign government entities or figures, as well as the history and legal structure of the supplier's home country, including the likelihood that said supplier could be forced by a hostile foreign government to disclose data that violates the privacy and security of Americans.[14]

The Chinese government recently passed a National Intelligence Law, which expands the Chinese government's authority to monitor foreign and domestic individuals and organizations. It grants legal authority to "National intelligence work institutions" to search premises and seize

[12] Haye Kesteloo, "Department of Defense bans the purchase of commercial-over-the-shelf UAS, including DJI drones effective immediately," *DroneDJ*, June 7, 2018. https://dronedj.com/2018/06/07/department-of-defense-bans-the-purchase-of-commercial-over-the-shelf-uas-including-dji-drones/.

[13] Catherine Shu, "New defense bill bans the U.S. government from using Huawei and ZTE tech," *TechCrunch*, August 2018. https://techcrunch.com/2018/08/13/new-defense-bill-bans-the-u-s-government-from-using-huawei-and-zte-tech/.

[14] Paul Rosenzweig and Kathryn Waldron, "Broadening the Lens on Supply Chain Security in the Cyber Domain," R Street Institute, April 15, 2019. https://www.rstreet.org/2019/04/15/r-street-policy-study-no-170-broadening-the-lens-on-supply-chain-security-in-the-cyber-domain/.

property when conducting defensive espionage. This new law raises concerns about increased surveillance and appears to grant the government access to previously private data. Article 14 of this new law requires organizations and individuals to cooperate with government intelligence institutions upon request. Those who violate the new intelligence law are subject to detention of up to 15 days, and can face criminal charges.[15]

This legal structure, which appears to apply to all entities operating in China, inherently increases the national security risks associated with the use of any Chinese supplier by public and private sector entities in the United States.

The U.S. government should therefore be concerned about the use of products and services from Chinese companies like DJI in the federal supply chain. The Army has already recognized this risk by prohibiting the use of DJI drones, but other government agencies may not yet show similar concern. On the other hand, DJI has previously shown willingness to install additional security measures as a result of U.S. government pressure. Consider the addition of geofencing technology after the 2015 White House lawn incident discussed above. Similarly, after the Army released its memo in 2017, DJI installed software that created a "privacy mode" that prevented the app used to control its drones from using internet traffic while a drone is in flight.[16] The company has stated, "Every day, American businesses, first responders, and U.S. government agencies trust DJI drones to help save lives, promote worker safety, and support vital operations, and we take that responsibility very seriously."[17] Words are cheap, but the company's actions suggest some of the risk of using a Chinese supplier can be mitigated for less critical drone uses through strong U.S. government action.

Drone Cybersecurity and Innovation

However, not all malicious actors seeking to take advantage of drones are necessarily foreign governments. As drones have increased in popularity, malicious cyber actors have sought a variety of ways to take advantage of this new technology. In 2016, a computer security team at John Hopkins University discovered multiple methods hackers might employ when trying to take control of a drone. According to Lanier Watkins, the senior cybersecurity expert on the team, "You see it with a lot of new technology. Security is often an afterthought. The value of our work is in showing that the technology in these drones is highly vulnerable to hackers."[18]

---

[15] Staff, "What you need to know about China's intelligence law that takes effect today," *Quartz*, June 28, 2017. https://qz.com/1016531/what-you-need-to-knowabout-chinas-intelligence-law-that-takes-effect-today.

[16] Li Tao, "Drone maker DJI introduces privacy mode after US Army ban," *South China Morning Post*, October 3, 2017. https://www.scmp.com/tech/china-tech/article/2113799/dronemaker-dji-introduces-privacy-mode-after-us-army-bans.

[17] Sam Byford, "After the US took down Huawei, could DJI be next?" *The Verge*, May 21, 2019. https://www.theverge.com/2019/5/21/18633744/dhs-alert-china-drones-dji-huawei.

[18] Kacey Deamer, "How Can Drones Be Hacked? Let Us Count the Ways," *Live Science*, June 10, 2016. https://www.livescience.com/55046-how-can-drones-be-hacked.html.

This is why policymakers must consider whether any regulation put in place will unnecessarily discourage or prevent new entrants into the drone manufacturing market. As my colleague Charles Duan has written regarding cybersecurity and other emerging technologies, lack of market competition can lead to a "monoculture," in which a flaw in one vendor's products allows hackers to undermine an entire system since it is all built upon the same model.[19] Over the past few years, independent hackers have posted instructions for hacking DJI drones on popular platforms like YouTube and Facebook as well as discussion forums for drone enthusiasts. While DJI has reportedly updated its drones to address these concerns, any market dominated by a single supplier is at a higher risk of exploitation by malicious cyber actors.[20]

Competition can encourage cybersecurity because it allows manufacturers to differentiate themselves by the amount of security offered. Monopolist suppliers have little incentive to invest in cybersecurity, since their products are the only option available. The commercial and recreational drone market is already predominantly composed of Chinese suppliers. Making it harder for American drone producers to enter the market may therefore actually discourage the implementation of security measures.[21]

We can already see evidence of the private market becoming aware of the need for security. As society becomes more aware of the security and privacy problems posed by drones, there has been increased demand for solutions. For example, attempting to combat privacy violations and economic espionage, San Francisco company Dedrone alerts customers when there is unexpected aerial drone activity in their vicinity. And as mentioned previously, many drones now incorporate geofencing to prevent commercial or hobby drones from flying into restricted airspace.[22] This can prevent drones from flying near places like the White House (as with the previously mentioned DJI drone) or airports.

Other proposed solutions are more creative, if far less scalable—Dutch company Guard From Above trains eagles to intercept drones in midair.[23] While I do not suggest the federal

---

[19] Testimony of Charles Duan, "5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation Submitted Statement of Charles Duan," 116th Congress, May 2019. https://www.rstreet.org/2019/05/23/5g-national-security-concerns-intellectual-property-issues-and-the-impact-on-competition-and-innovation-submitted-statement-of-charles-duan/.

[20] Ben Sullivan, "DJI Is Locking Down Its Drones Against a Growing Army of DIY Hackers," *VICE*, July 7, 2017. https://www.vice.com/en_us/article/3knkgn/dji-is-locking-down-its-drones-against-a-growing-army-of-diy-hackers.

[21] Testimony of Charles Duan, "5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation Submitted Statement of Charles Duan," 116th Congress, May 2019. https://www.rstreet.org/2019/05/23/5g-national-security-concerns-intellectual-property-issues-and-the-impact-on-competition-and-innovation-submitted-statement-of-charles-duan/.

[22] Drew Dixon, "Geofencing Stops Drones in Their Tracks," *Government Technology*, August 1, 2017. https://www.govtech.com/public-safety/Geofencing-Stops-Drones-in-Their-Tracks.html.

[23] "How we intercept drones, with birds of prey," Guard From Above, 2015-2018. https://guardfromabove.com/how-we-intercept-drones/.

government begin a bird-training program, I urge policymakers to seek equally creative solutions and allow innovators to do likewise. For example, Congress could require or incentivize the FAA (the current federal regulator of drones) to issue non-binding but heavily encouraged cybersecurity standards for drone manufacturers to adopt. Drone manufacturers that meet such standards might receive a certification they could then use when advertising their products, promoting their security superiority relative to competitors. In this way, drone manufacturers and policymakers could find their incentives aligned to promote cybersecurity. Promoting standards at the national level will help to standardize cybersecurity for drones, making it easier for consumers to judge the risks attached to any drone they buy. These standards could be reevaluated on an annual basis to capture changes in technology and best cybersecurity practices. (Similar types of programs have been promoted as possible avenues for mitigating cybersecurity risks for other types of emerging technologies, such as autonomous vehicles.)[24]

Conclusion

I thank the Committee for the opportunity to testify on the importance of encouraging innovation while limiting supply chain risks when it comes to drones. If I can be of any assistance to members of the Committee, please feel free to contact me or my colleagues at the R Street Institute.

Kathryn Waldron
Research Associate, Cybersecurity and National Security
kwaldron@rstreet.org

[24] Caleb Watney and Cyril Draffin, "Addressing New Challenges in Automotive Cybersecurity," R Street Institute, November 2017. https://www.rstreet.org/wp-content/uploads/2018/04/118-1.pdf.