American University National Security Law Brief

Volume 12 | Issue 2 Article 3

2022

The American Security Drone Act: America's Paper Tiger vs. China's Trojan Horse

Susan E. Upward

THE AMERICAN SECURITY DRONE ACT: AMERICA'S PAPER TIGER VS. CHINA'S TROJAN HORSE

LIEUTENANT COLONEL SUSAN E. UPWARD*

The skies above America have been increasingly inundated with small unmanned aircraft systems (sUAS) operated by both government agencies and civilians alike. The majority of these drones are manufactured by Da-Jiang Innovations (DJI), a Chinese company that continues to emerge as a national security threat. The risk posed by these drones stems not only from physical access to American airspace, but also from the surreptitious transmittal of information back behind the "Great Firewall of China" via DJI mobile device applications. However, current pending legislation is inadequate to effectively counter this threat. Instead, the United States should take a more comprehensive approach – use existing laws to deny DJI access to U.S. airspace, develop new legislation to curtail access to sensitive information in cyberspace, and take measures to counter consumer reliance on foreign sUAS by investing in the American drone manufacturing industry.

*Judge Advocate, United States Marine Corps. A native of Toronto, Ontario, Canada, LtCol Upward enlisted in the Marine Corps in February 2004 and became a U.S. citizen in September of the same year. After commissioning in 2005, she spent seven years of her military career as an Air Support Control Officer, including two tours managing airspace and controlling both manned and unmanned aircraft in support of Operation Iraqi Freedom, before she was selected to attend law school. She holds a B.A. in English from Valparaiso University; M.A. in Military Studies from American Military University; J.D. from Syracuse University College of Law; and LL.M. in Homeland and National Security Law from Western Michigan University's Cooley Law School. She is currently stationed at Marine Corps Air Station Cherry Point, North Carolina, as the Legal Services Support Team Officer-in-Charge. The views and opinions expressed in this chapter are those of the author and do not necessarily represent the views of the Department of Defense or the United States Marine Corps.

TABLE OF CONTENTS

INTRODUCTION

In appearance [the United States] is very powerful but in reality it is nothing to be afraid of, it is a paper tiger. Outwardly a tiger, it is made of paper, unable to withstand the wind and the rain. I believe the United States is nothing but a paper tiger.
– Mao Tse-tung[1]

O unhappy citizens, what madness? Do you think the enemy's sailed away? Or do you think any Greek gift's free of treachery? Is that Ulysses' reputation? Either there are Greeks in hiding, concealed by the wood, or it's been built as a machine to use against our walls, or spy on our homes, or fall on the city from above, or hides some other trick. Trojans, don't trust this horse. Whatever it is, I'm afraid of Greeks even those bearing gifts.
– Laocoon[2]

Over the last decade, a modern-day struggle between a proverbial trojan horse and a literal paper tiger has been playing out on the global stage. But the adversaries in this 21st-century story are not the Greeks and the Trojans, nor is the infamous gift from afar a giant wooden horse filled with enemy soldiers. Here, the conflict is a technological cold war between China and the United States,

[1] Interview with Mao Tse-Tung (July 14, 1956), "U.S. Imperialism is a Paper Tiger," Foreign Languages Press, Peking, China, https://www.marxists.org/reference/archive/mao/selected-works/volume-5/mswv5_52.htm.
[2] VIRGIL, THE AENEID BOOK II (A. S. Kline, trans., Poetry In Translation 2002), https://www.poetryintranslation.com/PITBR/Latin/VirgilAeneidII.php#anchor_Toc536009309.

and the gift from the former to the latter was a fleet of small drones to law enforcement and emergency services agencies across the country.[3] Publicized as a good-faith gesture to aid America in disaster relief, the danger is not only the drone itself and any possible evil uses therein, but the mobile device applications, or "apps," that accompany the drones and can be surreptitiously used to send information back to the Chinese government.[4]

One of the United States' answers to this threat from its foreign "near-peer" is the American Security Drone Act of 2021 – a bill that bans the procurement and use of Chinese drones by federal agencies.[5] But the bill falls ineffectually short of addressing the real perils that Chinese small unmanned aircraft systems (sUAS) pose – the majority of these drones are used by civilians, state and local law enforcement officials, and public safety agencies, all of whom are unaffected by the Act.[6] Moreover, the bill does nothing to address the unauthorized collection and transfer of data back to China, who has a reputation for secretly harvesting hordes of information for nefarious purposes.[7]

If the United States wants to truly mitigate the threat of Chinese drones, then a more comprehensive approach is required. The federal government can use existing laws and methods to curtail the number of Chinese drones flying in domestic airspace, while also penning new legislation to ensure that sensitive information collected by these sUAS is protected from nonconsensual transmittal to any entity, foreign or otherwise. Because state and local entities are the biggest

---

[3] Georgia Gee, *DJI and Draganfly Tried to Use the Pandemic to Get Law Enforcement to Use More Drones*, SLATE (Feb. 5, 2021, 9:30 AM), https://slate.com/technology/2021/02/dji-draganfly-police-departments-drones-pandemic.html.
[4] Katy Stech Ferek, *Lawmakers Seek Ban on Chinese Drone Purchases by Federal Agencies*, WALL STREET JOURNAL (Sept. 18, 2019, 4:49 PM), https://www.wsj.com/articles/lawmakers-seek-ban-on-chinese-drone-purchases-by-federal-agencies-11568818826; JOHN VENABLE & LORA RIES, BACKGROUNDER NO. 3521, HERITAGE FOUND., CHINESE-MADE DRONES: A DIRECT THREAT WHOSE USE SHOULD BE CURTAILED 4 (2020).
[5] *See* Julian E. Barnes, *China Poses Biggest Threat to U.S., Intelligence Report Says*, N.Y. TIMES (Apr. 13, 2021), https://www.nytimes.com/2021/04/13/us/politics/china-national-security-intelligence-report.html. China is often called a "near-peer" competitor in national security discourse because it is "challenging the United States in multiple arenas – especially economically, militarily and technologically – and is pushing to change global norms."
[6] VENABLE & RIES, *supra* note 4, at 4.
[7] *Id.* at 7.

consumers of sUAS, the federal government needs to support these actions against China by concurrently taking immediate actions to accelerate the American drone manufacturing market. Otherwise, without a viable, cost-effective, domestic alternative, the United States will be hard-pressed to keep consumers from choosing the Chinese trojan horse to meet their sUAS needs.

I. CHINA'S TROJAN HORSE: DJI DRONES AND APPS

The clear and present danger to the United States is from a Chinese Company called Da-Jiang Innovations (DJI), the world's largest manufacturer of sUAS.[8] At the advent of the global COVID-19 pandemic in April 2020, DJI donated drones to approximately 45 law enforcement and first responder agencies across 22 states in what the company promoted to be a "goodwill disaster relief program."[9] The drones appeared to be an effective tool to help local law enforcement in monitoring social distancing and broadcasting coronavirus information, even though some of the sUAS were also outfitted with thermal cameras to "detect potential coronavirus symptoms, such as high temperature and increased heart rate."[10] But this intrusion on a citizen's person and the infringement on civil liberties therein is not the most offensive part of the DJI drones; even more disconcerting was where the collected data was going.[11]

In July 2020, two separate cybersecurity firms analyzed the apps that accompanied DJI's drones and determined that they were the equivalent of an electronic trojan horse, allowing China to access "terabytes of data [from] a single flight while surveilling American citizens, cities, and infrastructure."[12] First, a DJI app that allows users to control the drone was reverse-engineered and researchers found that it was "collecting sensitive user data and that its coding enabled the app's

---

[8] *Id.* at 5.
[9] Gee, *supra* note 3.
[10] *Id.*
[11] *See id.* ("'To have my vitals monitored by drones without my knowledge of [sic] permission is beyond words,' wrote one alarmed resident in an e-mail to the country government. 'This is straight out of an Orwellian nightmare.'").
[12] VENABLE & RIES, *supra* note 4, at 5.

developer to download and execute code whenever it chose," meaning that "DJI could readily identify specific targets of interest, access their contacts and Internet network, and ultimately compromise the user's phone."[13] Even more troubling than accessing the user's personal data, researchers found that "once a device has been exploited, [DJI] could track the owner – and use the phone to attack other users through WiFi networks."[14]

The other app that was studied was used by consumers to edit videos and photographs taken on DJI action cameras.[15] When analyzed, researchers found that the information collected and transmitted unknowingly by users via this app was shockingly more pervasive than DJI's flight control app:

- Uses libraries that request personal data about user's religious and political affiliation, as well as security setting from connected social network application programming interfaces;
- Sends that data *without user consent* via unsecured mean to third-party servers leading to potential disclosure or modification while in transit:
- Sends data to servers behind the Great Firewall of China; and
- Terms of Use Agreement allows user data to be shared with the Chinese government.[16]

Because the data collected by the drone can be accessed by the manufacturer via both apps, it can also be accessed by the Chinese government that has "a history of imbedding surreptitious endeavors into seemingly good-natured or even charitable transactions by its government and/or Chinese corporations."[17] The information, photos, and videos captured by unknowing government agencies or even U.S. citizens could be used for a multitude of nefarious uses, including "pilfering

[13] *Id.* at 6.
[14] *Id.*
[15] *Id.*
[16] *Id.* at 6-7 (emphasis in original); *see The Complete Guide to the Great Firewall of China (GFoC)*, GOCLICKCHINA (June 15, 2021), https://www.goclickchina.com/insights/complete-guide-to-the-great-firewall-of-china-gfoc/ ("The Great Firewall of China refers to the set of legal and technological measures deployed by the People's Republic of China to regulate its domestic internet usage … [and] is an all-encompassing term to explain the Chinese government's proactive approach to regulating external influences over cyberspace").
[17] VENABLE & RIES, *supra* note 4, at 5; *see infra* p. 15-19 and notes 49-57.

intellectual property and technology [by] hacking data from U.S. companies, military, and government agencies," accessing and using images to be "manipulated and disseminated through the Internet in targeted campaigns" of social media manipulation, and "using collected data to influence U.S. leaders at the federal, state, and local levels."[18]

Unsurprisingly, DJI has strongly denied the security allegations, repeatedly stating that "nothing is *automatically* transferred to China" and "users can prevent their drones from transmitting data back to the company or connecting to the internet – and that the Chinese government has never sought the data that DJI does have."[19] But as the Federal Bureau of Investigation (FBI) warned in July 2020, DJI would "have no choice to hand it over to the Chinese government if asked – the privacy and due process protections that are sacrosanct in the United States are simply non-existent in China."[20] This is even more likely given the continued discovery of an obfuscated symbiotic relationship between DJI and the Chinese government. Just as recently as February 2022, and despite DJI's public attestations to the contrary, it was discovered that "four investment bodies owned or administered by Beijing have invested in [DJI] in recent years, including a state asset manager that has pledged to play a key role in promoting partnerships between private enterprises and the Chinese military."[21]

II. AMERICA'S PAPER TIGER: THE AMERICAN SECURITY DRONE ACT

Even before the private cybersecurity firms completed their research, American legislators were crafting an appropriate response to mitigate the domestic threat posed by Chinese drones. In

---

[18] VENABLE & RIES, *supra* note 4, at 7-8.
[19] Gee, *supra* note 3 (emphasis added); Ferek, *supra* note 4.
[20] VENABLE & RIES, *supra* note 4, at 8 (quoting Christopher Wray, FBI Dir., *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*, Remarks at the Hudson Institute, Video Event: China's Attempt to Influence U.S. Institutions (July 7, 2020), https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states).
[21] Cate Cadell, *Drone Company DJI Obscured Ties to Chinese State Funding, Documents Show*, WASHINGTON POST (Feb. 1, 2022, 10:00 AM), https://www.washingtonpost.com/national-security/2022/02/01/china-funding-drones-dji-us-regulators/.

September 2019, Senator Rick Scott introduced the American Security Drone Act of 2020 with bipartisan co-sponsorship.[22] Almost identical to its progeny in 2021, this version of the Act banned federal agencies from procuring or using commercial off-the-shelf drones manufactured or assembled by Chinese companies but was inexplicably removed from the final Fiscal Year 2021 National Defense Authorization Act (NDAA).[23]

Undeterred, Scott reintroduced the bill in January 2021 with the same bi-partisan support.[24] The new bill mirrors the same ban on purchasing, operating, or using federal funds to acquire sUAS and "associated elements" manufactured or assembled by "covered foreign entities," which includes companies like DJI that are either domiciled in or subject to influence or control by China, as deemed by the Secretary of Homeland Security.[25] The 2021 version of the Act also carved out specific exceptions for certain federal entities to conduct "research, evaluation, training, testing, or analysis … [when it] is required in the national interest of the United States," and for specific programs in consultation with the Secretary of Homeland Security.[26] Finally, the proposed legislation requires "all executive agencies [to] account for existing inventories" of UAS that will fall under the provisions of the bill, and for the creation of a government-wide policy for procurement of UAS systems, to include specifications "to address the risks associated with processing, storing and transmitting Federal information in a UAS."[27]

---

[22] S. 2502, 116th Cong. (2019) (Bill was co-sponsored by Scott (Republican – Florida); Marsha Blackburn (Republican, Tennessee); Richard Blumenthal (Democrat - Connecticut); Tom Cotton (Republican, Arkansas); Josh Hawley (Republican, Missouri); Christopher Murphy (Democrat, Connecticut); and Marco Rubio (Republican, Florida)).
[23] *Id.*; S. 4049, 116th Cong. (2020); Venable & Ries, *Why Did Congress Strip the Chinese Drone Ban From the NDAA?*, HERITAGE FOUND. (Feb. 8, 2021), https://www.heritage.org/technology/commentary/why-did-congress-strip-the-chinese-drone-ban-the-ndaa.
[24] American Security Drone Act of 2021, S. 73, 117th Cong. (2021).
[25] *Id.* § 2, 7 ("Associated elements" includes "communication links and the components that control" the sUAS).
[26] *Id.* § 3 (The Secretary of Homeland Security, the Secretary of Defense and Attorney General have exemptions, as do the Federal Aviation Administration Center of Excellence for UAS, the National Transportation Safety Board, and the National Oceanic Atmospheric Administration).
[27] *Id.* § 7, 9.

III. WHO THE ACT IMPACTS

At face value, the Act is billed as a viable and forceful blockade of Chinese-made drones from future procurement and use in the United States. But the truth is that even before the ink was dry on the first version of the American Security Drone Act of 2019, most federal agencies heeded the warnings of national security experts and had either grounded or divested their organizations of their Chinese-drone fleets.[28]

For instance, the Department of Defense (DOD) has progressively taken measures over the past four years to eliminate any use of Chinese drones in military operations. DJI sUAS products were once "the most widely used non-program of record commercial off-the-shelf UAS employed by the Army" until August 2017, when Army leadership ordered the complete cessation of DJI equipment use, to include uninstalling all DJI apps and removing all batteries and storage media from DJI devices.[29] In May 2018, the other services followed suit, as the DOD implemented a blanket ban on both the purchase and use of all commercial off-the-shelf drones.[30] Congress then codified the ban in the NDAA for Fiscal Year 2020, specifically prohibiting the Secretary of Defense from operating, or entering into or renewing contracts to procure Chinese UAS.[31]

Besides the DOD, the federal agency that appeared would be most affected by the American Security Drone Act when it was written was the Department of the Interior (DOI). Charged with protecting and managing "the nation's natural resources and cultural heritage," the DOI is

---

[28] *See* Carrick Detweiler, CEO of Drone Amplified, quoted in Matt O'Brien, *Gov't Use of Chinese Drones in Limbo as Congress Weighs Ban,* ABC NEWS (Jun. 1, 2021, 11:15 AM), https://abcnews.go.com/Politics/wireStory/govt-chinese-drones-limbo-congress-weighs-ban-78019005.rien ("Everyone I talk to in the federal government is moving away from DJI whether or not [the Act] is passed").

[29] Memorandum for Rec. from Dep't of the Army on Discontinue Use of Dajiang [sic] Innovation (DJI) Corp. Unmanned Aircraft Sys. (Aug. 2, 2017) (available at https://www.suasnews.com/2017/08/us-army-calls-units-discontinue-use-dji-equipment/).

[30] Memorandum from Dep Sec'y of Def. on Unmanned Aerial Vehicle Sys. Cybersecurity Vulnerabilities (May 23, 2018) (available at https://sofrep.com/fightersweep/us-department-of-defense-memo-stops-use-and-purchases-of-commercial-off-the-shelf-cots-unmanned-aerial-systems-uas/).

[31] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92 § 848, 133. Stat. 1198, 1508 (2019).

responsible for overseeing more than 500 million acres of land, which is approximately one-fifth of the entire United States landmass.[32] sUAS has obvious utility in completing this mission, allowing the DOI to more efficiently observe a vast amount of rugged terrain from above. In 2018 alone, DOI estimates that it "saved more than $14 million in taxpayer dollars" and flew "more than 10,000 flights to manage fires, survey erosion, monitor endangered species and inspect dams … [to include using] drones to rescue a Hawaii resident trapped by lava flows."[33] But after multiple warnings about DJI's cybersecurity concerns, DOI grounded all of its approximately 800 Chinese-made drones in January 2020, and "its drone program has been largely on hiatus since then, except for some emergency flights that are granted a waiver."[34]

However, not all federal agencies have voluntarily parted with their Chinese drones. In fact, in July 2021, within days both before and after the DOD released another statement reiterating the national security threat posed by DJI, the Secret Service purchased eight DJI sUAS and the FBI purchased 19, stating that the DJI drones were "the only commercially available consumer [drone] to combine all [its] required capabilities at an acceptable cost."[35] To that end, it may take legislation like the American Security Drone Act to end some federal agencies from taking the path of least resistance and their insistent reliance on Chinese-made drones.

IV. WHO THE ACT MISSES

For the most part, the American Security Drone Act and its ultimatum to federal departments does not affect the largest consumers of DJI products – state and local law

---

[32] U.S. DEP'T OF THE INTERIOR, ABOUT INTERIOR, https://www.doi.gov/about (last visited Dec. 10, 2021); Ferek, *supra* note 4.
[33] Ferek, *supra* note 4.
[34] VENABLE & RIES, *supra* note 4, at 10; O'Brien, *supra* note 24.
[35] Lachlan Markay, *U.S. Government Buying Risky Chinese Drones*, AXIOS (Sept. 22, 2021), https://www.axios.com/federal-law-enforcement-china-drone-4b33aca2-b6f5-43d0-8d36-be1d447af1a0.html; Press Release, Dep't of Defense, Dep't Statement on DJI Sys. (July 23, 2021), https://www.defense.gov/News/Releases/Release/Article/2706082/department-statement-on-dji-systems/.

enforcement and emergency services.[36] For police, sUAS are invaluable to "map cities, search for suspects or victims, investigate crime scenes, and monitor traffic," while for fire and rescue agencies, sUAS are used to provide first responders with an eye-in-the-sky from a view "that was previously either unavailable or extremely difficult to obtain in a safe and timely manner."[37] With limited resources and tight budgets, "these systems offer shorter response times, greater utility, and markedly lower costs to acquire and operate than manned helicopters."[38] As a result, the use of sUAS in these agencies has skyrocketed, and a vast majority of them are from DJI:

- In 2018, a report estimated that at least 910 state and local police, sheriff, fire, and emergency services agencies in the U.S. have purchased drones; more than 520 of those agencies have purchased a drone from DJI.[39]
- In 2019, more than 120 people affiliated with public-safety agencies said their organization intended to buy a DJI-drone within the next year.[40]
- In 2020, approximately 1,578 state and local police, sheriff, fire, and emergency services agencies in the U.S. had already acquired drones, and more than half of those agencies reported that their drones were manufactured in China.[41]
- In 2021, DJI invited law enforcement agencies that were already registered with the Federal Aviation Administration (FAA) to apply for additional drones to aid their coronavirus response. DJI said it received several hundred responses from police departments, as well as

[36] *See generally* American Security Drone Act of 2021, S. 73, 117th Cong. (2021).
[37] *Id.*
[38] *Id.* at 1.
[39] Ferek, *supra* note 4.
[40] *Id.*
[41] VENABLE & RIES, *supra* note 4, at 4 (The number of agencies physically in possession of drones is probably much higher; this estimation only included agencies that actually reported their drones).

fire departments and state patrols, and the company ultimately offered 100 sUAS to 45 agencies.[42]

With so many state and local entities having already procured DJI sUAS assets and using them in daily operations, the threat is already embedded within these non-federal government agencies. The Act's ban on using federal funds will also have minimal effect moving forward – not only did several agencies receive DJI drones as a gift, but a 2019 study identified only "14 public-safety agencies that used federal money to purchase drones."[43] Moreover, the Act does not account for civilian owners and operators – considering that "eighty percent of all commercial drones sold in the United States are Chinese," the physical and cybersecurity risks embedded in DJI drones already saturates the American airspace and airwaves.[44]

V. A TIGER WITH TEETH: DOUBLE ENVELOPMENT

If the United States truly wants to mitigate the risk associated with the proliferation of Chinese drones domestically, it will need to employ much stronger tactics than simply banning federal agencies from buying or using them. Instead, the American government would be better off confronting the problem on two fronts. Known in military parlance as a double envelopment, the U.S. should simultaneously attack both of the enemy's flanks – cut off physical access by DJI drones and apps, while concurrently employing new measures to address the cybersecurity intrusions.[45]

A. First Front: Deny Physical Access

First, there is no need to wait for new legislation to severely curtail DJI's access to American airspace today – FAA regulations already in place could severely limit, if not legally eliminate the

---

[42] Gee, *supra* note 3.
[43] Ferek, *supra* note 4.
[44] Venable & Ries, *supra* note 19.
[45] *See* DEP'T OF THE ARMY, FM 3-90-1, OFFENSE AND DEFENSE VOL. 1 § 1-11, 1-12 (2013).

ability of DJI drones to fly anywhere over the homeland. The exclusive sovereignty of U.S. airspace gives the FAA broad authority under 49 U.S.C. Chapter 41 to prescribe regulations on aircraft flight in order to protect other aircraft and "individuals and property on the ground."[46] In determining what regulations to enact and enforce, the FAA uses a myriad of safety considerations, including attention to "regulating air commerce in a way that best promotes safety and fulfills *national defense* requirements."[47] Under that rubric, the FAA has frequently used these provisions to ban or ground aircraft under a variety of circumstances:

- In 2015, the FAA banned all private foreign aircraft from flying in U.S. airspace except with diplomatic clearance from the Secretary of State for approximately one month. Ordering that "all U.S. territorial airspace is national defense airspace," pilots were warned that non-compliance could result in interception and detention, as well as other unspecified "penalties."[48]
- In 2019, the FAA grounded all Boeing 737 Max-type aircraft following two fatal crashes abroad in the span of five months.[49]
- In January 2020, the FAA banned certain aircraft "owned and operated by Bahamasair from entering the United States … because they lack[ed] a particular onboard technology required" by FAA regulations.[50]

---

[46] 49 U.S.C. § 40103 (2021) (emphasis added); *see also* § 40102 (2011) (Chapter 41 does include sUAS, as "aircraft" is defined as "any contrivance invented, used, or designate to navigate, or fly in, the air").
[47] 49 U.S.C. § 40101 (2011) (emphasis added).
[48] Ashley Burke, *FAA Banned Canadian Private Planes from U.S. Airspace for 1 Month,* CBC (Feb. 20, 2016, 5:00 AM), https://www.cbc.ca/news/politics/pilots-banned-us-airspace-1.3456352 (The ban almost exclusively affected Canadian aircraft that transit American airspace, even though the point of origin and destination are both in Canada, a long-time ally and generally low national security threat to the United States).
[49] Emergency Order of Prohibition from FAA to Operators of Boeing Company Model 737-8 and Boeing Company Model 737-9 Airplanes (Mar. 23, 2019), https://www.faa.gov/sites/faa.gov/files/2021-08/Emergency_Order.pdf.
[50] Chris Loh, *Why Bahamasair's Boeing 737-500s Are Banned From US Airspace*, SIMPLE FLYING (Jan. 10, 2020), https://simpleflying.com/bahamasair-boeing-737-500-banned-us-airspace/.

- In July 2020, the FAA "revoked permission for Pakistan International Airlines to conduct charter flights in the United States, citing … concerns over Pakistani pilot certifications."[51]

For sUAS specifically, any person operating a drone "for the purposes of flight," to include a government agency, is required to register and appropriately mark the aircraft.[52] To further restrict the use of DJI drones, the FAA could simply refuse to register new applications and revoke the registrations that already exist.[53]

Even beyond the FAA's power to regulate, the U.S. government can take steps to ban DJI equipment and technology as it has previously done with other troublesome Chinese companies, with mixed success. For instance, in August 2018, legislators passed a very similar measure to the American Security Drone Act, banning all federal agencies from procuring or using telecommunications equipment produced by Huawei, a Chinese mobile telecommunications company.[54] This was followed in May 2019 when President Donald Trump signed an even more sweeping executive order that effectively served as a blanket ban for Chinese telecommunications companies, particularly Huawei, from selling equipment to anyone nationwide because "foreign adversaries [were] increasingly creating and exploiting vulnerabilities in information and communications technology and services … in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people."[55]

---

[51] *U.S. Bans Pakistan International Airlines Flights Over Pilot Concerns*, REUTERS (July 10, 2020, 5:56 AM), https://www.ndtv.com/world-news/us-bans-pakistan-international-airlines-flights-over-pilot-concerns-2260182.
[52] 14 C.F.R. § 107.13 (2021) (citing 14 C.F.R. § 91.203 (2021); 14 C.F.R. ch. I, subch. C, Pt. 48 (2021).
[53] 14 C.F.R. § 48.100 (explaining that for sUAS "operated for any purpose other than exclusively limited recreational operations," a certificate of aircraft registration is effective only for three years unless otherwise revoked or canceled at the sole discretion of the FAA).
[54] John S. McCain National Defense Authorization Act for Fiscal Year 2019, 115 Pub. L. 232, §839, 132 Stat. 1636 (2018).
[55] Exec. Order No. 13,873, 84 Fed. Reg. 22,689 (May 15, 2019).

In response to being essentially blacklisted, Huawei filed lawsuits and alleged that the U.S. government's bans were unconstitutional, but both lawsuits have been summarily dismissed.[56] Meanwhile, Huawei, like DJI, has continuously engaged in "public disavowals" of its role in China's state surveillance program, even though a recent report using marketing presentations from the company's public website "show Huawei pitching how its technologies can help government authorities identify individuals by voice, monitor political individuals of interest, manage ideological reeducation and labor schedules for prisoners, and help retailers track shoppers using facial recognition."[57] This only confirms what the United States has been saying for years: DJI is "Huawei on wings," and any Chinese company that blatantly embeds surveillance technology into its equipment is a national security threat that warrants swift and stern action from the administration.[58]

A. Second Front: Defend Cybersecurity Vulnerabilities

It is not just equipment that poses a risk – mobile apps like TikTok, a popular social media app owned by a company based in Beijing "that allows users to create, watch, and share 15-second videos shot on cellphones," has also been identified as a national security threat.[59] A year after successfully blacklisting Huawei, President Trump signed another executive order that not only attempted to ban TikTok from operating in the U.S. by blocking downloads of the app and

---

[56] *See generally* Huawei Techs. USA, Inc. v. United States, 440 F.Supp.3d 607 (E.D. Tex. 2020) (holding that the FY19 NDAA did not violate the Bill of Attainder Clause, Due Process Clause, or the principle of separation of powers); Huawei Techs. USA, Inc. v. FCC, 2 F.4th 421 (5th Cir. 2021) (holding that the Federal Communication Commission's ruling designating Huawei a national security threat and banning American telecommunications operators from buying the company's telecom equipment was a reasonable interpretation and did not exceed the agency's statutory authority under the framework established in Chevron U.S.A., Inc. v. NRDC, 467 U.S. 837, 842-44 (1984)).
[57] Eva Dou, *Documents Link Huawei to China's Surveillance Programs*, WASH. POST (Dec. 14, 2021, 4:00 AM), https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.
[58] Aila Slisco, *FCC Commissioner Calls Chinese Drone Company a Potential 'Airborne Version of Huawei'*, NEWSWEEK (Oct. 19, 2021), https://www.newsweek.com/fcc-commissioner-calls-chinese-drone-company-potential-airborne-version-huawei-1640615; Timothy Nerozzi, *Biden Admin Says Huawei is National Security Threat*, FOX BUSINESS (Dec. 15, 2021), https://www.foxbusiness.com/politics/biden-admin-huawei-national-security-threat.
[59] Deborah D'Souza, *What is TikTok?*, INVESTOPEDIA (July 22, 2021), https://www.investopedia.com/what-is-tiktok-4588933

prohibiting internet companies from carrying the company's traffic, but also economically sanctioned TikTok by outlawing transactions between American citizens and TikTok's parent company, ByteDance, and forced the Chinese owners to divest a majority share of TikTok to an American company.[60]

TikTok also filed suit challenging the ban, but unlike their Huawei countrymen, were successful in getting injunctive relief because while "the United States has long used economic sanctions to prohibit transactions that threaten national security," in this case, the President "overstepped his authority in using his emergency economic power to try to effectively put the wildly popular app out of business."[61] However, TikTok did not get away from the courthouse scot-free – the company has agreed to pay $92 million to settle a large class-action lawsuit for "flouting U.S. privacy laws by surreptitiously harvesting … Plantiffs' private information" without consent, and then sending that data to multiple servers in China.[62]

In that context, if the United States wants to curtail China's reach into sensitive domestic information by drone, phone, or app, then it must get its own house in order. The data protection privacy laws that were circumvented in the TikTok class action suit is America's critical vulnerability, and one that China has repeatedly taken advantage of. Currently, "the United States does not have any centralized, formal legislation at the federal level regarding this issue," leaving data protection

---

[60] Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020); Rishi Iyengar, *TikTok Owner Gets Another Week to Sell it U.S. Business*, CNN BUSINESS (Nov. 26, 2020, 3:06 PM), https://www.cnn.com/2020/11/26/tech/tiktok-cfius-deadline-extended-december/index.html; Bobby Allyn, *U.S. Judge Halts Trump's TikTok Ban, The 2nd Court to Fully Block the Action*, NPR (Dec. 7, 2020, 8:36 PM), https://www.npr.org/2020/12/07/944039053/u-s-judge-halts-trumps-tiktok-ban-the-2nd-court-to-fully-block-the-action?t=1609087334425.

[61] Allyn, *supra* note 55; Tiktok Inc. v. Trump , 490 F. Supp. 3d 73 (D.D.C. 2020), *injunction granted*, 507 F. Supp. 3d 92 (D.D.C. 2020), *appeal dismissed*, TikTok Inc. v. Biden, No. 20-5381, 2021 U.S. App. LEXIS 22070 (D.C. Cir. Jul. 14, 2021) (The administration originally appealed the injunction, but when President Biden rescinded Executive Order 13,942, the parties entered into a joint stipulation to dismiss the case (Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021)).

[62] In re Tiktok, Inc., Consumer Privacy Litig., No. MDL No. 2948, 2021 U.S. Dist. LEXIS 188949 (N.D. Ill. Sep. 30, 2021); Allyn, *Class-Action Lawsuit Claims TikTok Steals Kids' Data and Sends it to China*, NPR (Aug. 4, 2020, 1:39 PM), https://www.npr.org/2020/08/04/898836158/class-action-lawsuit-claims-tiktok-steals-kids-data-and-sends-it-to-china; Allyn, *TikTok to Pay $92 Million to Settle Class-Action Suit Over Theft of Personal Data*, NPR (Feb. 25, 2021, 6:11 PM), https://www.npr.org/2021/02/25/971460327/tiktok-to-pay-92-million-to-settle-class-action-suit-over-theft-of-personal-data.

mostly in the hands of the private sector.[63] Instead, Congress has enacted a number of federal laws designed to protect individuals' personal information, piecemealed between certain industries and bifurcated in regulating certain subcategories of data.[64] On top of that hodgepodge of laws and federal agencies responsible for enforcing them, several states have "developed their own statutory frameworks for data protection."[65] Indeed, Congress may need to expressly preempt some state laws in order to facilitate a comprehensive national approach, but that is what is needed – a single federal data protection law to stop unauthorized collection and transfer of data to China or any other foreign entity.[66]

VI. SUPPORTING EFFORT: WINNING HEARTS AND MINDS AT HOME

While the two-front attack on DJI and China is the main effort, the United States must also engage in indirect actions to shape the battlefield and ensure mission success. One critical supporting effort to counter the domestic proliferation of Chinese drones is to engage both the citizenry and local and state leaders who "do not appear to recognize the threat. … Cities are acquiring or willingly accepting drones from China *without considering the repercussions*, and the employment of those systems is growing unabated."[67] A targeted information campaign coupled with meaningful engagement to answer questions is critical to ensure that there is widespread understanding of the threat DJI drones pose to individuals, organizations, and the nation as a whole.[68]

---

[63] *Data Protection Law*, HG.ORG, https://www.hg.org/data-protection.html.
[64] STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION (2019).
[65] *Id.*
[66] *Id.*; *see, e.g.*, Data Protection Act of 2021, S. 2134, 117th Cong. (2021) (First introduced in 2021, the bill would create a new federal Data Protection Agency responsible for "regulating high-risk data practices and the collection, processing, and sharing of personal data").
[67] VENABLE & RIES, *supra* note 4, at 11 (emphasis in original).
[68] *Id.* at 12.

However, any movement that aims to get Americans to self-regulate and reject DJI drones must be necessarily accompanied by a viable alternative product, preferably made in the U.S.A. Yet, to date, "Western-based companies have not been able to compete with DJI's complete supply-chain integration, user-friendly software design, and Chinese manufacturers' incredibly low pricing."[69] As such, DJI has been able to exploit the sUAS space because it has few challengers globally, let alone domestically. In 2019, DJI comprised approximately 70 percent of the global drone market and almost 77 percent of the U.S. market – a daunting number alone, but even more so when it is considered that the next closest competitor is Intel with only 3.7 percent of the domestic market.[70] Accordingly, jump-starting the U.S. drone market that has been crippled by "the predatory business practices of the Chinese government" is a critical supporting effort to counter the infestation of Chinese drones.[71]

To that end, in June 2019, President Trump invoked the Defense Production Act and declared that "the domestic production capability for [sUAS] is essential to the national defense" as a "critical capability."[72] While that may seem like an extreme measure, federal agencies should use any opportunity from the executive branch's emergency grant of authority "to encourage technological growth and price-point reduction" in American sUAS systems.[73] The DOD has already invested approximately $13.4 million in contracts to five small domestic drone companies, including Skydio, a California-based startup that has separately raised "$100 million in investment

---

[69] *Id.* at 5.
[70] Blake Schmidt & Ashlee Vance, *DJI Won the Drone Wars, and Now It's Paying the Price*, BLOOMBERG BUSINESSWEEK (Mar. 26, 2020, 12:01 AM), https://www.bloomberg.com/news/features/2020-03-26/dji-s-drone-supremacy-comes-at-a-price.
[71] VENABLE & RIES, *supra* note 4, at 11.
[72] 50 U.S.C. § 4501 et. seq. (LexisNexis, Lexis Advance through Pub. L. No. 117-70, approved Dec. 3, 2021, with a gap of Pub. L. No. 117-58); Presidential Determination Pursuant to Section 303 Defense Production Act of 1950, as Amended, 84 Fed. Reg. 27,701 (June 13, 2019).
[73] VENABLE & RIES, *supra* note 4, at 12.

for its autonomous enterprise and public sector drone technology."[74] The Departments of Justice and Homeland Security could also follow suit and pump more funds into the U.S. drone market by expanding their grant programs for continued research and development of domestic sUAS platforms.[75]

Lawmakers are already working towards crafting and enacting legislation aimed at making the United States more economically competitive with China in the science and technology realm. The America Creating Opportunities for Manufacturing, Pre-Eminence in Technology, and Economic Strength (America COMPETES) Act of 2022 was focused, among other things, primarily on subsidizing manufacturing of domestic semiconductors, as well as "research on artificial intelligence, quantum computing, and other critical technologies."[76] But while it specifically provided for direct support to such technologies such as solar equipment manufacturing in order to shore up a "viable" domestic supply chain and to reduce reliance on Chinese products and components, it fails to provide the same enumerated commitment to drone production.[77] Regardless of the methodology, the United States must take immediate actions to accelerate the domestic drone manufacturing market and make homegrown sUAS a more attractive option for cash-strapped and resource-depleted communities, as well as budget-conscious consumers.

---

[74] *Id.* at 11; Darrell Etherington, *Autonomous Drone Startup Skydio Raises $100 Million and Launches the X2 Commercial Drone*, TECHCRUNCH (July 13, 2020, 11:41 AM), https://techcrunch.com/2020/07/13/autonomous-drone-startup-skydio-rises-100-million-and-launches-the-x2-commercial-drone/.

[75] VENABLE & RIES, *supra* note 4, at 12.; *see, e.g.*, FED. AVIATION ADMIN., *U.S. Department of Transportation Announces $5.8 Million in 33 Unmanned Aircraft System Research Grants to Universities* (Jan. 13, 2021), https://www.faa.gov/newsroom/us-department-transportation-announces-58-million-33-unmanned-aircraft-system-research (The FAA grants were focused on studying how to "safely and efficiently integrate UAS into [the] nation's airspace system" in eight research areas, and did not include the actual manufacturing of sUAS).

[76] Raquel Leslie & Brian Liu, *House of Representatives Passes China Competition Bill*, LAWFARE (Feb. 7, 2022, 11:01 AM), https://www.lawfareblog.com/house-representatives-passes-china-competition-bill; H.R. 4521, 117th Cong. (as passed by House , Feb. 4, 2022).

[77] H.R. 4521, § 20302; *see also* § 10306(o), § 50104 (H.R. 4521, 117th Cong. (2022) was passed by the Senate on Mar. 28, 2022. Renamed the United States Innovation and Competition Act of 2021, the amended legislation removed the support for solar equipment manufacturing, but in § 2506, kept subsidizes for domestic semiconductor manufacturing. The amended Act also incorporated the provisions of the American Security Drone Act in § 4401 – § 4411. Interestingly, immediately following the unmanned aircraft provisions of the amended act the Senate added § 4431 – § 4432: a prohibition on the use of the TikTok on federal government devices.

CONCLUSION

The United States can no longer afford to be blissfully unaware or simply ignore the fact that the trojan horse in the shape of a Chinese drone is already on its shores and flying over the American heartland. DJI drones are prolific in the United States, used both by civilians for recreational purposes, as well as state and local law enforcement and emergency services as a budget-friendly eye-in-the-sky. The nation's insatiable appetite for sUAS and their utility will only continue to grow, and the American Security Drone Act is wholly inadequate to address the ever-increasing threat China poses in this space. The bill is more bluster than substance – a strong political statement in the ongoing technological cold war with China, but failing to address the fundamental issues that face the U.S. in combating DJI's drones. Undoubtedly, some federal agencies insist on continuing to purchase DJI drones, so a measure must be taken to ensure they cease and desist with this risky practice. But to truly mitigate the risk Chinese drones pose to the United States' national security, a more effective methodology would be to execute a pincer movement on DJI – ban DJI's equipment and physical access to American airspace, while simultaneously curbing their ability to illegally mine personal and sensitive data via their mobile apps, including the impermissible transfer of that information back to Beijing.

However, all of these offensive actions will be less effective without more defensive measures at home. America's Achilles' heel is its lack of an all-encompassing federal law to protect data instead of the current mishmash of federal and state laws divided by sector and split into types of data that clearly is not working to keep foreign adversaries at bay. Additionally, the federal government must engage and educate citizens and state and local governments alike on the inherent risks of using DJI drones, while simultaneously resuscitating the American drone manufacturing industry by any means necessary. Only a whole-of-government approach will effectively counter China's known modus operandi of embedding furtive intent in otherwise seemingly innocuous

technology from companies intrinsically linked to the Chinese government. Another paper tiger is simply not enough.