The Heritage Foundation

BACKGROUNDER
No. 3521 | AUGUST 19, 2020
CENTER FOR NATIONAL DEFENSE

Chinese-Made Drones: A Direct Threat Whose Use Should Be Curtailed

John Venable and Lora Ries

KEY TAKEAWAYS

Drone use in the U.S. is increasing rapidly, but this raises substantial privacy and security concerns, especially concerns about data falling into the wrong hands.

Chinese drones dominate the U.S. market—despite minimal data protections, data transfer to Chinese firms, and mandatory data-sharing with the Chinese Government.

The U.S. must stop unauthorized data collection and transfer to foreign-based corporations or governments before it is used to threaten U.S. citizens or interests.

Commercial drone use is exploding in the United States, particularly with city, county, and state governments. These systems offer shorter response times, greater utility, and markedly lower costs to acquire and operate than manned helicopters. Moreover, the technology and associated capabilities are advancing so rapidly that even facial recognition is now included in many off-the-shelf systems. With miniaturization, those systems may soon have the ability to instantly determine the identity of people in crowds using a database of billions of social media images currently found on sites like Facebook and YouTube. The potential to exploit that data goes well beyond marketing and, in the wrong hands, could harm national security. The United States government needs to address and stop the collection and transfer of data by drones to any foreign-based corporation before this incredible capability is turned against us.

This paper, in its entirety, can be found at **http://report.heritage.org/bg3521**

The Heritage Foundation | 214 Massachusetts Avenue, NE | Washington, DC 20002 | (202) 546-4400 | heritage.org

Drone Types and Capabilities

Unmanned aircraft systems (UAS) or "drones" come in four weight-based sizes with capabilities that increase with each increment of scale.

- Small drones are the most common and weigh less than 20 pounds. The vast majority of drones employed by civilian and government users at and below the state level fall into this category.
- Medium drones weigh less than 55 pounds and are limited to an altitude of 3,500 feet above the ground.
- Large drones (up to 1,320 pounds) and very large drones (greater than 1,320 pounds)[1] are almost exclusively used by the federal government and U.S. military.

While the technology embedded in the latter two may seem excessive to state and local governments and private users, miniaturization will undoubtedly allow many of their capabilities to migrate into the medium and small drones over the decade ahead.[2]

In commercial drones, the video cameras, the images they collect, and the data they produce are the value center of the devices, and full-motion video (FMV) is the most widely available sensor on drones of all sizes.[3] These video surveillance systems generally have telescopic/zoom-in features with small drone daylight cameras that currently offer up to 30x optical and an additional 6x digital zoom for a total magnification of 180x.[4] Nighttime options are equally impressive and include thermal imaging and low-light cameras with 20x zoom and 1080-pixel high definition.[5] These off-the-shelf, commercially available drones have the ability to collect surprisingly detailed information on surveilled areas and subjects of interest, and they can transmit that real-time video feed directly to the Internet through a 4G connection or through base stations that are connected to the Internet.[6]

To complement those capabilities, facial recognition and artificial intelligence (AI) software are now available in drones priced as low as $600.[7] While those capabilities are relatively rudimentary and limited in function,[8] the technology surrounding facial recognition has exploded over the past several years. Clearview AI, a U.S. start-up company, introduced technology in 2019 that uses artificial intelligence to compare an uploaded photo against a database of billions of images compiled from social media sites, like Facebook and YouTube, to find a match, often in milliseconds.[9] It has since been used by the U.S. Departments of Defense (DOD) and Homeland Security (DHS), the FBI, and hundreds of state and local police agencies, and the entire process can be accomplished on a smartphone.[10]

With a connection to the Web, commercial drones will soon be able to exploit the kind of AI now being developed for government agencies,[11] and with miniaturization, the collection capabilities currently found on larger drones will likely migrate to the small-drone market over the next decade. As such, it is useful to briefly explore the open-source capabilities now being fielded on large UAS platforms.

Finding points or subjects of interest in the field-of-view (or "soda straw") coverage offered by FMV cameras significantly limits the surveillance capability of any drone. In an effort to expand both the field of view and operator situational awareness, the military developed and acquired wide-area surveillance capabilities and wide-area motion imagery (WAMI) sensors.

WAMI systems are very large video cameras capable of recording the activities and movements within city-sized areas in high resolution. The Air Force's Gorgon Stare carried by MQ-9 Reapers is one such system. It can track thousands of targets simultaneously and conduct several surveillance operations on separate targets concurrently. This system allows analysts to play back the video of a person of interest (POI) to see where he lives, who his friends are, and then, in turn, who those friends associate with[12]—a feature similar to a modern digital video recorder found in most homes. This high definition monitoring is streamed in real time[13] to analysts and systems that can process the images of the POI for identification.

The weight of Gorgon Stare and similar state-of-the-art surveillance systems is significant, but technological advances continue apace, and their weight and size are dropping rapidly. For example, CorvusEye 1500 is a relatively new WAMI system that provides surveillance over an area three kilometers in diameter—and it weighs just 83 pounds.[14] This year, Logos Technologies introduced a new system called Redkite that quadruples CorvusEye 1500's surveilled area to 12 kilometers and, at 30 pounds, can now be carried on medium-sized drones. With the number of companies working to take the lead in this growing business area, there is little doubt that efforts to miniaturize that technology will continue and, if it follows the path of cell phones,[15] the weight will drop to allow small drones to readily carry and employ WAMI systems.

The capabilities associated with Clearview, WAMI, and Gorgon Stare are not currently known to be available in small drones. However, with Internet connectivity and advances in miniaturization, the potential benefits these systems will bring to state, city, and county agencies are significant—as are the potential negative impacts.

State and Local Government Agencies' Drone Use

The use of commercial drones in the United States is exploding. According to the Federal Aviation Administration (FAA), which registers drones in the U.S., there were fewer than 50,000 commercial drones in operation at the end of 2016.[16] Today, there are more than 385,000.[17] The FAA forecasts the commercial UAS fleet to grow to over 835,000 by 2023, an average annual growth rate of 25 percent.[18]

Companies have started using drones to cut costs and increase operational efficiency in a variety of industries, including insurance, construction, and agriculture.[19] One of the most important sectors of growth in drone employment is for law enforcement and first responders at the state and local levels. As of March 2020, 1,578 state and local police, sheriff, fire, and emergency services agencies in the U.S. have acquired drones, an increase of 500 agencies since May 2018.[20] Just over 70 percent of those agencies are law enforcement, 20 percent are fire and rescue, and 10 percent are emergency management organizations.[21] Some possess a single drone, while others operate fleets of 10 or more, and their capabilities are having an extraordinary impact.

Police use drones to map cities, search for suspects or victims, investigate crime scenes, and monitor traffic. Fire and rescue agencies use drones as intelligence, surveillance, and reconnaissance tools "to provide command officers and emergency operations centers information that was previously either unavailable or extremely difficult to obtain in a safe and timely manner."[22] If the technology now resident in large military drones continues to migrate into smaller systems, their capabilities will substantially advance police, fire, and rescue efforts and operations.

However, the data those drones collect while flying over metropolitan areas would hold the precise location of critical infrastructure and sensitive information, such as the locations of civic leaders, their movements, and interactions. If that data fell into the wrong hands—or was even collected by an entity with hostile intent—it could be used against individuals, officials, and agencies in ways that far exceed the benefits of those systems.

Compounding this concern is the fact that the vast majority of drones used by law enforcement and first responder agencies, more than 970, are manufactured in China, and the way many of those systems were "introduced" to U.S. law enforcement agencies is troubling.[23] The leading Chinese drone manufacturer of small drones, D-Mada Jiang Innovations (DJI), donated 100 drones to 45 law enforcement and first responder organizations across 22 states in a good will "disaster relief program" to combat the COVID-19 crisis on April 1, 2020.[24] Those "gifts" are now being used in major metropolitan areas to monitor social distancing, fevers, and coughs among the public—as well as broadcasting messages to homeless encampments and to enforce stay-at-home orders.[25]

While this type of surveillance is common in China, it has rightfully raised privacy and civil liberties concerns in the U.S. Drones have the technology to collect terabytes of data in a single flight while surveilling American citizens, cities, and infrastructure. Furthermore, this sensitive data collected by the Chinese-donated drones can be accessed by the drone manufacturer—and, thereby, the Chinese government. Beijing has a history of imbedding surreptitious endeavors into seemingly good-natured or even charitable transactions by its government and/or Chinese corporations. Before we explore those details, it is important to know just how big a foothold Chinese corporations have in the U.S. commercial drone industry.

China Dominates the U.S. Drone Market

In 2019, $1.2 billion were invested in the global drone industry.[26] That year, a single, privately owned Chinese drone manufacturer, DJI, held app roximately *70 percent* of the global consumer drone market.[27] That market is expected to be worth $43.1 billion by 2024.[28]

North America has the largest market for commercial drones,[29] where DJI dominates as well. Of the top 10 drone manufacturers that supply the U.S. market, DJI towers over the others with nearly 77 percent of market share.[30] The next closest company is Intel (Santa Clara, California) with a mere 3.7 percent of the market.[31] The remaining manufacturers are:

- Yuneec (Hong Kong, China): 3.1 percent market share;
- Parrot (Paris, France): 2.2 percent market share;
- GoPro (San Mateo, California): 1.8 percent market share;
- 3DR (Berkeley, California): 1.5 percent **market share**;
- Holy Stone (Taipei, Taiwan): 0.8 percent market share;
- Autel (Bothell, Washington): 0.8 percent market share;
- SenseFly (Lausanne, Switzerland): 0.3 percent market share; and

- Kespry (Menlo Park, California): 0.3 percent market share.[32]

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.[33]

While the user interface and technology associated with Chinese drones are attractive features, perhaps the biggest factor in Chinese drone manufacturers gaining control of the global market is pricing. A 2017 investigation by Homeland Security found that DJI had aggressively dropped its prices 70 percent in 2015, effectively pushing many competitors out of the U.S. market.[34] Those dumping techniques have allowed DJI and Yuneec to capture a total of 80 percent of the U.S. commercial drone market. Consumers, both private and public, have moved to buy their advanced, easy-to-use and markedly less expensive technology over other global competitor products without fully understanding just how much data these drones collect, where the data goes, and how it can be used.

The Road to Beijing

In early July of 2020, a security firm called Synacktiv reverse-engineered an Android application (app) called DJI GO 4 that allows owners to control drones—and what they discovered was more than troubling. They found the app was collecting sensitive user data and that its coding enabled the app's developer to download and execute code whenever it chose. The amount and type of user information collected meant that DJI could readily identify specific targets of interest, access their contacts and Internet networks, and ultimately compromise the user's phone. Once a device has been exploited, the developer (DJI) can track the owner—and use the phone to attack other users through WiFi networks.[35] But it is not just the drone software that puts users at risk.

A cybersecurity research and engineering firm, River Loop Security, recently analyzed an editing tool for videos and photographs taken on DJI action cameras known as the DJI's Mimo mobile app.[36] River Loop observed the network traffic between the Internet and mobile devices via the app,[37] and they found the DJI Mimo app:

- Uses libraries that request personal data about users' religious and political affiliation, as well as security settings from connected social network application programming interfaces;

- Sends that data *without user consent* via unsecured means to third-party servers leading to potential disclosure or modification while in transit;

- Sends data to servers behind the Great Firewall of China; and the

- Terms of Use Agreement allows user data to be shared with the Chinese government.[38]

Those findings should worry any company or government agency using DJI technology, as well as policymakers working to secure critical infrastructure.

The Chinese Communist Party: A Bad Actor

The Chinese government has a history of pilfering intellectual property and technology, as well as hacking data, from U.S. companies, military, and government agencies.[39] Collecting data from users via technology, applications, and devices is one of the Chinese Communist Party's (CCP) many tactics.

As a current example, TikTok is a free app owned by ByteDance, a Beijing-based tech company that offers users the ability to create novel, 15-second videos to share through social media. ByteDance is now being sued for harvesting personal user data and sending it to China without the consent—or even knowledge—of those users.[40] The lawsuit also accuses TikTok and ByteDance of taking user content, such as draft videos, without their consent and of having "ambiguous" privacy policies.[41]

While many believe the data is used to simply better profile users and target advertising, there have been several instances in which users' videos have been censored or accounts deleted because they criticized the CCP.[42] Although this is a relatively mild action, it shows the CCP's ability to trace an individual's behavior and penalize him or her. When one criticizes or goes against the CCP's narrative, the repercussions can be severe.

We have seen Beijing influence leaders on the global stage with the World Health Organization's President Tedros Ghebreyesus and his backing of the CCP's response to the COVID-19 crisis. We have likewise seen Beijing's influence affect U.S. corporations, including Nike and the National Basketball Association, whose overt support of China in the face of known human rights violations and its poor global pandemic response is beyond naïve. As such, it is not a stretch to envision Beijing using collected data to influence U.S. leaders at the federal, state, and local levels.

Similarly, Beijing has compiled recent images of U.S. protests and manipulated them to portray America as chaotic, unruly, and a society in decline. The CCP uses such manipulation to advance its narrative that China's authoritarian leadership is superior to democracy.[43] Apply those same tactics to the opportunities presented with the data captured by a police drone monitoring the movements of a crowd during a demonstration in a densely populated area, and it is not hard to imagine the associated images being captured, manipulated, and disseminated through the Internet in targeted campaigns to cause those civil demonstrations to spiral out of control.

Like any other form of data collection, the information collected by drones can be shared between organizations and used to support efforts over which the drone operators may have no knowledge or direct control.[44] For many city, county, and state government organizations, exchange of that data can seem innocuous or even entirely beneficial for coordinating emergency services between fire and/or police departments. Unfortunately, the hidden data transfer capabilities of these systems can be much more nefarious.

FBI Director Christopher Wray stated in a July 2020 speech on the Chinese government and CCP's threat to our economy and national security:

> [T]here is perhaps no more ominous prospect than a hostile foreign government's ability to compromise our country's infrastructure and devices. If Chinese companies like Huawei are given unfettered access to our telecommunications infrastructure, they could collect any of your information that traverses their devices or networks. Worse still: They'd have no choice but 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.[45]

Federal Government Prepared; State and Local Governments Unprepared

The U.S. government now recognizes the threat of using Chinese-manufactured drones and has issued multiple warnings and bans. In August 2017, the U.S. Army prohibited troops from using DJI drones due to cybersecurity concerns.[46] Also in August 2017, Homeland Security Investigations issued an intelligence bulletin, warning that DJI was providing critical infrastructure and law enforcement data to the Chinese government.[47] The bulletin stated that the most frequent uses for the DJI drones included mapping land, inspecting infrastructure, conducting surveillance, and monitoring hazardous materials.

In May 2018, then-Acting Secretary of Defense Patrick Shanahan issued a ban on the DOD's purchase and use of all commercial off-the-shelf drones until the department could devise a plan to address cybersecurity vulnerabilities.[48]

On September 5, 2018, the Secretary of the Department of Homeland Security warned that "[t]errorists are using drones on the battlefield to surveil and to destroy.... [C]riminals are using them to spy on sensitive facilities. Drones can also be used to disrupt communications or to steal data on nearby Wi-Fi."[49]

In May 2019, the Department of Homeland Security (DHS) issued an alert to U.S. companies about the risk of Chinese-manufactured drones sending American data to China, where intelligence services have unlimited access to the data.[50] And in June 2019, President Donald Trump extended the Defense Production Act to small UAS, stating "the domestic production capability for small unmanned aerial systems is essential to the national defense."[51]

The Entities List

The Department of Commerce's Bureau of Industry and Security publishes the names of certain foreign individuals or business entities that, because of their unscrupulous or nefarious actions, are subject to specific license requirements and policies for the export, re-export, and/or transfer (in-country) of specified items. These people and entities comprise what is known as the "Entity List," which is part of the Export Administration Regulations. Huawei has been placed on the Entities List because of its coercive and surreptitious efforts to field 5G network technology—and while DJI is not yet on the list, events during the past three years highlight the need to consider the corporation for inclusion therein.

DJI has had a direct role in supporting China's mass internment and suppression of the Uyghur people in Xinjiang. In 2017, the privately held company signed an agreement of cooperation with the Xinjiang Autonomous Region Public Security Department (XARPSD), which includes the deployment of DJI drones and a strategic-cooperation agreement on police drones for "stability maintenance" and "counter-terrorism."[52]

In mid-July, shocking drone footage reminiscent of the Nazi Holocaust of Jews was posted on Twitter that showed a DJI drone monitoring Chinese paramilitary police escorting Uighurs who were shackled and blindfolded at a train station in Xinjiang in the fall of 2019.[53] Analysis reveals the video was taken using a DJI M-series drone, and its operators are within 40 meters of the drone, imbedded within the paramilitary police.[54] With that, it became clear that "stability maintenance" and "counter-terrorism" are euphemistic terms for the abuse of the Uyghur people.

In October 2019, the U.S. Department of Commerce placed the XARPSD on the Entity List[55] and, because it is providing material assistance to the XARPSD, DJI should also be placed on that list. Congress has likewise started to legislate against government procurement of Chinese manufactured drones in the U.S. The American Security Drone Act of 2019 was introduced in both chambers of Congress with bipartisan support.[56] The bill would generally:

1. Ban federal procurement of commercial off-the-shelf drones or unmanned aircraft systems manufactured or assembled by a covered foreign entity, as determined by the Departments of Commerce, Homeland Security, State, or the Director of National Intelligence; or an entity subject to the influence or control by the government of the People's Republic of China or the Chinese Communist Party;

2. Prohibit federal operation of foreign commercial off-the-shelf drones and small unmanned aircraft systems; and

3. Prohibit the use of federal funds awarded through contract, grant, or cooperative agreement to purchase commercial off-the-shelf drones or UAS manufactured or assembled by a covered foreign entity.

In January of 2020, the Department of the Interior grounded all Chinese-made drones (approximately 800) in its fleet due to cybersecurity concerns with drones manufactured in China or made from Chinese parts.[57]

More recently, the Inspector General for DHS reported that drones present an emerging threat to the nation as their popularity grows,[58] stating that "[t]errorists, criminal organizations, and lone actors have used UAS for malicious purposes."[59] The report identified drone-related threats facing DHS, including transporting contraband, chemical, or other explosive/weaponized payloads; silently monitoring a large area from the sky for nefarious purposes; performing cybercrimes involving theft of sensitive information; and disrupting and invading the privacy of individuals.[60]

The Inspector General reminded Americans in its report of the drone that crashed on the White House lawn in January 2015, "illustrating a drone's ability to evade detection and create challenges for secure facilities."[61] He concluded in its report that the "DHS will remain vulnerable to increased security risks and emerging threats from unmanned aircraft until it expands its capability to counter illicit UAS activity."[62]

In July 2020, the Defense Department awarded five small companies a total of $13.4 million in contracts. This will eventually help jump-start the U.S commercial industrial base capabilities and defense-critical workforce. However, the bureaucratic hurdles associated with the contracting process could take months, if not years, to boost the domestic drone industry because it has been suppressed by the predatory business practices of the Chinese government, which has employed underhanded financial and business practices to drive competitors out of business.

In his July 2020 speech, FBI Director Wray stated bluntly, "China, as led by the Chinese Communist Party, is going to continue to try to misappropriate our ideas, influence our policymakers, manipulate our public opinion, and steal our data. They will use an all-tools and all-sectors approach—and that demands our own all-tools and all-sectors approach in response."[63] The federal government recognizes the threat China poses with small drones, and it is taking steps to counter it; however, the threat's potential has not registered below the federal level.

Unfortunately, state and local law enforcement and first responder agencies do not appear to recognize the threat that Chinese drones can pose. Cities are acquiring or willingly accepting drones from China *without considering the repercussions*, and the employment of those systems is growing unabated. Heeding Director Wray's advice, state and local law enforcement agencies, first responders, critical infrastructure industries, and others should steer clear of Chinese-manufactured drones. To protect our homeland, national security, and economic interests, government consumers of commercial drones in the U.S. should procure technology that minimizes such risks.

Recommendations

To counter the risks of Chinese-made drones or those using Chinese-made parts, the U.S. should enact the following recommendations.

- **The Administration should place DJI on the Entity List.** This is particularly crucial in light of the Homeland Security Investigation's findings, River Loop Security's findings, and DJI's assistance in the monitoring and facilitation of the appalling persecution of Uyghurs inside China.

- **The Administration should work with Congress to pass legislation that will stop the unauthorized collection and transfer of data by a Chinese drone company or subsidiary.** This should occur regardless of whether such collection is in or beyond the shores of the United States, as that company is likely to move or store that data in China.

- **The DOJ and the DHS, using their state and local committees, should engage state, city, and county agencies.** They should inform them of the threat and the potential repercussions from employing Chinese drones, including the evidence of, and repercussions for, employing this inexpensive technology in their communities.

- **The Departments of Commerce, Treasury, Defense, and Homeland Security should leverage the Defense Production Act authorities that President Trump has invoked.** This should be done to encourage technological growth and price-point reduction in the U.S. market for government use.

- **The DOJ, DHS, and the DOD should use and/or expand their grant programs to accelerate competition among U.S. manufacturers.** They should also encourage state and local agencies to procure drones that are not manufactured or assembled by an entity subject to the influence or control of the Chinese Communist Party.

Conclusion

The U.S. faces a growing national threat from Chinese drones. The vast majority of commercial drones used in the U.S. are manufactured in China, and their operating systems are impressive and worrisome. The technology is advancing rapidly, and the capabilities currently found in large drones is now being miniaturized and will likely migrate to smaller drones in the near term, which will significantly broaden the threat. The federal government has recognized the threat and put the brakes on procuring or using such risky technology—but the understanding of the risk and/or the willingness of state and local agencies to thwart those drones from collecting sensitive data is limited at best. It is time for state and local agencies to be informed of, and recognize, the threats involved in using Chinese-manufactured drones and immediately move to mitigate them.

John Venable is Senior Research Fellow for Defense Policy in the Center for National Defense, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy. **Lora Ries** is Senior Research Fellow for Homeland Security in the Center for Technology Policy of the Davis Institute.

Endnotes

1. Penn State University, “Classification of the Unmanned Aerial Systems,” College of Earth and Mineral Sciences, https://www.e-education.psu.edu/geog892/node/5 (accessed June 21, 2020).
2. Jim Fisher, “Drone Regulations: What You Need to Know,” *PC Magazine*, January 29, 2020, https://www.pcmag.com/news/drone-regulations-what-you-need-to-know (accessed June 21, 2020).
3. Arthur Holland Michel, “Unarmed and Dangerous: The Lethal Application of Non-Weaponized Drones,” Bard College Center for the Study of the Drone, p. 9, https://dronecenter.bard.edu/projects/unarmed-and-dangerous/unarmed-and-dangerous-2/ (accessed June 21, 2020).
4. Yuneec, “E3OZ,” https://www.yuneec.com/en_US/accessories/cameras/e30z/overview.html (accessed June 21, 2020).
5. “Best Infrared Drones (Buying Guide): Yuneec Typhoon H with CGOET Thermal Imaging and Low-Light Camera,” SpireDrones, 2020, https://buythebestdrone.com/best-infrared-drones/ (accessed June 21, 2020).
6. Utsav Chopra, “Leverage FlytNow to Manage Fleet of Pixhawk and CubePilot Drones Over 4G, LTE, 5G,” DIY Drones, June 29, 2020, https://diydrones.com/profiles/blogs/list/tag/fleet+of+drones (accessed July 24, 2020).
7. “7 Best Drones with Facial Recognition,” The Droid Guy, March 3, 2020, https://thedroidguy.com/7-best-drones-with-facial-recognition-1077684 (accessed June 21, 2020).
8. Hwai-Jung Hsu and Kuan-Ta Chen, “Face Recognition on Drones: Issues and Limitations,” Institute of Information Science, September 28, 2019, https://www.iis.sinica.edu.tw/~swc/pub/face_recognition_on_drones.html (accessed June 21, 2020).
9. Kashmir Hill, “The Secretive Company That Might End Privacy as We Know It,” *The New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (accessed July 11, 2020).
10. Donnie O’Sullivan, “This Man Says He’s Stockpiling Billions of Our Photos,” CNN Business, February 10, 2020, https://www.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html (accessed August 8, 2020), and Donnie O’Sullivan, “Clearview AI’s Founder Hoan Ton-That Speaks Out,” Youtube, March 6, 2020, https://www.youtube.com/watch?v=q-1bR3P9RAw (accessed August, 6, 2020).
11. Project Maven, also known as the Algorithmic Warfare Cross-Function Team, was launched in April 2017 to develop and integrate computer-vision algorithms to help the military process the thousands of hours of full-motion video data it collects during counterinsurgency and counterterrorism operations. The Pentagon had planned to mate baseline algorithms with warfighting systems by the end of 2017. “What Is Project Maven? The Pentagon AI Project Google Employees Want Out Of,” Global News, April 5, 2018, https://globalnews.ca/news/4125382/google-pentagon-ai-project-maven/ (accessed June 21, 2020).
12. Michel, “Unarmed and Dangerous: The Lethal Application of Non-Weaponized Drones,” pp. 11–12.
13. “L3Harris Corporation: Wide-Area Airborne Motion Imagery Solution Video,” L3Harris, https://www.harris.com/solution/corvuseye-1500 (accessed June 23, 2020).
14. “Exelis CorvusEye Provides Wide-Area Airborne Surveillance Capable of Viewing 10 Separate Areas in 3-Kilometer Region,” Businesswire, May 13, 2014, https://www.businesswire.com/news/home/20140513005143/en/Exelis-CorvusEye-wide-area-airborne-surveillance-capable (accessed July 12, 2020).
15. The first cell phone weighed 2.5 pounds (1134 grams) and had a battery life of 30 minutes. An iPhone 7 weighed 138 grams, included markedly more capability, and had a battery life of 14 hours. “How Much Did the First Handheld Cell Phone Weigh?” GCN, https://gcn.com/blogs/tech-trivia/2011/09/what-did-the-first-cell-phone-weigh.aspx (accessed August 3, 2020), and Anthony Bouchard, “Weight, Size, and Battery Life: iPhone 7 vs. iPhone 6,” iDownloadBlog, September 7, 2016, https://www.idownloadblog.com/2016/09/07/weight-size-battery-iphone-7-vs-iphone-6s/ (accessed July 24, 2020)
16. Federal Aviation Administration, “Unmanned Aircraft,” Table, p. 50, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/unmanned_aircraft_systems.pdf (accessed July 6, 2020).
17. Ibid.
18. Office of the Inspector General, “DHS Has Limited Capabilities to Counter Illicit Unmanned Aircraft Systems,” OIG–20–43, Department of Homeland Security, June 25, 2020, p. 2, https://www.oig.dhs.gov/sites/default/files/assets/2020-06/OIG-20-43-Jun20.pdf (accessed July 1, 2020).
19. “Drone Market Outlook: Industry Growth Trends, Market Stats and Forecast,” *Business Insider*, March 3, 2020, https://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts (accessed July 7, 2020).
20. Dan Gettinger, “Public Safety Drones,” 3rd ed., Bard College Center for the Study of the Drone, March 2020, p. 1, https://dronecenter.bard.edu/projects/public-safety-drones-project/public-safety-drones-3rd-edition/ (accessed May 18, 2020). Gettinger notes that this tally does not include agencies with undisclosed drone programs, federal agencies, agencies that use drones owned by others, or private citizens.
21. Ibid., p. 2.
22. Anthony Tisdall and Bear Afkhami, “Eyes in the Sky: How Firefighters Can Use Drones During All-Hazards Incidents,” September 18, 2019, https://www.firerescue1.com/fire-products/drones/articles/eyes-in-the-sky-how-firefighters-can-use-drones-during-all-hazards-incidents-s1oJQPw6yFfQOZkA/ (accessed July 9, 2020). It is worth noting that DJI sponsors firefighting drones on this Web page.

23. Of the 970 agencies, 924 own a DJI model, and 46 agencies own a Yuneec model. Gettinger, "Public Safety Drones," p. 7.

24. Mary Meisenzahl, "'We Are Trying to Save Lives, Not Be Big Brother': U.S. Police Are Facing Backlash for Using 'Dystopian' Drones to Ask People to Stay Home," *Business Insider*, April 23, 2020, https://www.businessinsider.com/us-police-drones-enforce-coronavirus-stay-at-home-orders-2020-4 (accessed June 12, 2020).

25. Ibid.

26. E. Mazareanu, "Commercial Drones Investments 2008 to 2019," *Statista*, June 19, 2020, https://www.statista.com/statistics/1117058/global-commercial-drone-investments/#statisticContainer (accessed July 8, 2020).

27. Divya Joshi, "Here Are the World's Largest Drone Companies and Manufacturers to Watch and Stocks to Invest in 2020," *Business Insider*, December 20, 2019, https://www.businessinsider.com/drone-manufacturers-companies-invest-stocks (accessed July 6, 2020).

28. Mazareanu, "Commercial Drones Investments 2008 to 2019."

29. Katharina Buchholz, "Commercial Drones are Taking Off," *Statista*, February 28, 2019, https://www.statista.com/chart/17201/commecial-drones-projected-growth/ (accessed August 3, 2020). The Asia–Pacific region is expected to be the largest commercial drone market by 2024, with $18.4 billion in U.S. dollars. See also E. Mazareanu, "Projected Global Commercial Drone Market Size in 2024, By Region" *Statista*, June 17, 2020, https://www.statista.com/statistics/878022/global-commercial-drone-market-size-by-region/ (accessed July 8, 2020).

30. Lukas Schroth, "Drone Manufacturer Market Shares: DJI Leads the Way in the U.S.," September 26, 2019, https://www.droneii.com/drone-manufacturer-market-shares-dji-leads-the-way-in-the-us (accessed May 14, 2020).

31. Ibid.

32. Ibid.

33. Harrison Wolf, "3 Reasons Why China Is the Global Drones Leader," World Economic Forum, September 19, 2018, https://www.weforum.org/agenda/2018/09/china-drones-technology-leader/ (accessed July 6, 2020).

34. Ibid.

35. Dan Goodin, "Chinese-Made Drone App in Google Play Spooks Security Researchers," Ars Technica, July 24, 2020, https://arstechnica.com/information-technology/2020/07/chinese-made-drone-app-in-google-play-spooks-security-researchers/ (accessed July 25, 2020)

36. "DJIMimo: My Moment," DJI, https://www.dji.com/mimo (accessed June 16, 2020).

37. River Loop Security, "Analyzing Data Use By the DJI Mimo App," May 12, 2020, https://www.riverloopsecurity.com/blog/2020/05/dji_mimo/ (accessed July 10, 2020).

38. Ibid.

39. See Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," Remarks made at the Hudson Institute, 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 (accessed July 9, 2020).

40. Rachel Sandler, "Congress Worries TikTok Is a National Security Threat," *Forbes*, October 24, 2019, https://www.forbes.com/sites/rachelsandler/2019/10/24/congress-worries-tiktok-is-a-national-security-threat/#44743c3036cd (accessed June 21, 2020).

41. Queenie Wong, "TikTok Accused of Secretly Gathering User Data and Sending It to China," CNET, December 2, 2019, https://www.cnet.com/news/tiktok-accused-of-secretly-gathering-user-data-and-sending-it-to-china/ (accessed June 21, 2020).

42. Ryan Browne, "TikTok Lifts Ban on U.S. Teen who Criticized China's Treatment of Muslims," CNBC, November 28, 2019, https://www.cnbc.com/2019/11/28/tiktok-lifts-ban-on-us-teen-who-criticized-china-treatment-of-muslims.html (accessed July 12, 2020). See also Drew Harwell and Tony Romm, "TikTok's Beijing Roots Fuel Censorship Suspicion as It Builds a Huge U.S. Audience" *The Washington Post*, September 15, 2019, https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/ (accessed July 12, 2020).

43. Javier Hernández, "As Protests Engulf the United States, China Revels in the Unrest," *The New York Times*, June 2, 2020, https://www.nytimes.com/2020/06/02/world/asia/china-george-floyd.html (accessed July 12, 2020).

44. Michel, "Unarmed and Dangerous, The Lethal Application of Non-Weaponized Drones." p. 5.

45. Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States."

46. Rory Cellan-Jones, "U.S. Warns of Threat from Chinese Drone Companies," BBC, May 21, 2019, https://www.bbc.com/news/technology-48352271 (accessed May 18, 2020).

47. U.S. Department of Homeland Security, "Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government," Immigration and Customs Enforcement, August 9, 2017, p. 1, https://info.publicintelligence.net/ICE-DJI-China.pdf (accessed May 18, 2020).

48. Gary Mortimer, "U.S.–DOD Pulls the Plug on COTS Drones," SUAS News, June 7, 2018, https://www.suasnews.com/2018/06/us-dod-pulls-the-plug-on-cots-drones/ (accessed May 18, 2020).

49. News release, Kirstjen Nielsen, "Rethinking Homeland Security in an Age of Disruption," US Department of Homeland Security, September 5, 2018, https://www.dhs.gov/news/2018/09/05/secretary-nielsen-remarks-rethinking-homeland-security-age-disruption (accessed July 1, 2020).

50. David Shepardson, "DHS Warns of Data Threat from Chinese-Made Drones," Reuters, May 20, 2019, https://www.reuters.com/article/us-usa-drones-china/dhs-warns-of-data-threat-from-chinese-made-drones-idUSKCN1SQ1ZY (accessed May 15, 2020). Footnote sequencing. 53 appears twice. 52 not at all

51. Donald J. Trump, "Memorandum on Presidential Determination Pursuant to Section 303 of the Defense Production Act of 1950, As Amended," June 10, 2019, https://www.whitehouse.gov/presidential-actions/memorandum-presidential-determination-pursuant-section-303-defense-production-act-1950-amended/ (accessed July 20, 2020).

52. International Cyber Policy Centre, "Activities in Xinjiang," Mapping China's Tech Giants, https://chinatechmap.aspi.org.au/#/company/dji (accessed July 19, 2020).

53. The drone used in this operation has a 30x optical zoom, something only the DJI Zenmuse Z30 offers. See Lily Kuo, "China Footage Reveals Hundreds of Blindfolded and Shackled Prisoners," *The Guardian*, September 21, 2019, https://www.theguardian.com/world/2019/sep/23/china-footage-reveals-hundreds-of-blindfolded-and-shackled-prisoners-uighur (accessed August 3, 2020), and Andrew Marr, "China's Ambassador Denies Abuse of Uighurs in Xinjiang During Andrew Marr Interview: Video," The Andrew Marr Show, BBC, July 19, 2020, https://www.theguardian.com/world/video/2020/jul/19/chinas-ambassador-tells-andrew-marr-there-are-no-concentration-camps-in-xinjiang-video (accessed July 19, 2020).

54. Visual evidence within a video posted on YouTube on or about September 16, 2019, and reposted on Twitter by Daniel Sinclair on September 26, 2020. Daniel Sinclair, September 26, 2019, Twitter, https://twitter.com/_DanielSinclair/status/1177259835349487619 (accessed July 19, 2020).

55. U.S. Department of Commerce, "Commerce Department to Add Nine Chinese Entities Related to Human Rights Abuses in the Xinjiang Uighur Autonomous Region to the Entity List," May 22, 2020, https://www.commerce.gov/news/press-releases/2020/05/commerce-department-add-nine-chinese-entities-related-human-rights (accessed July 19, 2020).

56. American Security Drone Act, S. 2502, 116th Cong., 1st Sess., https://www.congress.gov/bill/116th-congress/senate-bill/2502?q=%7B%22search%22%3A%5B%22drone%22%5D%7D&s=1&r=2 (accessed August 3, 2020), and American Security Drone Act, H.R. 5125, 116th Cong., 1st. Sess., https://www.congress.gov/bill/116th-congress/house-bill/5125?q=%7B%22search%22%3A%5B%22S.2502+-+American+Security+Drone+Act+of+2019%22%5D%7D&s=1&r=2 (accessed August 3, 2020).

57. Bill Chappell, "Interior Department Grounds Chinese-Made Drones, Months After It Approved Them," NPR, January 29, 2020, https://www.npr.org/2020/01/29/800890201/interior-department-grounds-all-of-its-drones-citing-cybersecurity-other-concern (accessed July 12, 2020).

58. Office of the Inspector General, "DHS Has Limited Capabilities to Counter Illicit Unmanned Aircraft Systems," p. 1.

59. Ibid.

60. Ibid., p. 2.

61. Ibid.

62. Ibid., p. 1.

63. Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party."