Bringing Down the Hammer
ON CHINESE TECH

by Dawn M.K. Zoldi (Colonel, USAF Retired)

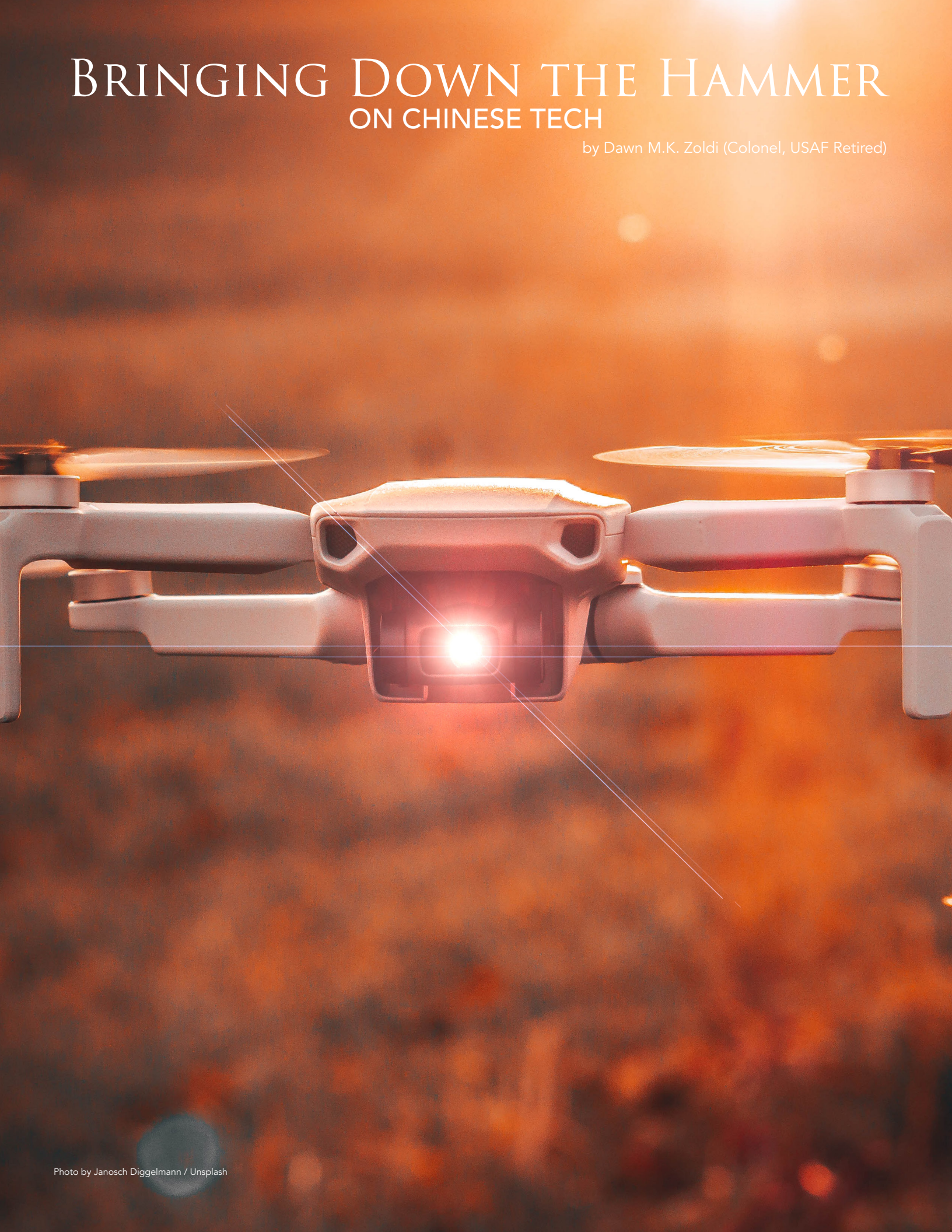

Photo by Janosch Diggelmann / Unsplash

Law is what you must do; policy is what you should do. With regard to country-of-origin bans on technology, either one has the effect of the proverbial hammer. Of late, the U.S. government has been wielding that hammer consistently against China in what amounts to an all-out tech war. The most visible fronts have involved Huawei, ByteDance (TikTok), and TenCent (WeChat). However, a lesser-known conflict relating to the commercial drone sector involves Da Jiang Innovations (DJI), a Chinese technology company headquartered in Shenzhen, Guangdong. It is a three-pronged assault based on cybersecurity, national security, and human rights concerns. Will the U.S. commercial drone ecosystem get hammered in this conflict?

THE CHINESE DRONE MARKET

To understand the common operational picture, context matters. The U.S. federal government has been using Chinese drones extensively. The Department of the Interior (DOI) was using them for wildfire tracking.[349] The Department of Agriculture was using them to research farming progress out West.[350] The Department of Transportation uses drones for data collection.[351] The Department of Homeland Security (DHS) had been using DJI drones for law enforcement investigations, surveillance of drug routes along the coast, and other sensitive missions.[352] Finally, the Department of Defense (DOD) employs small drones for various military purposes.

Drones are ubiquitous and becoming even more so. In the United States, current drone registrations with the Federal Aviation Authority (FAA) have already outpaced the agency's 2023 projections.[353] Further, beyond the U.S. federal market, drones are a big business. The global commercial drone market is currently worth USD 22.5 billion and is projected to reach USD 42.8 billion by 2025.[354]

The overwhelming majority of those drones are made by DJI. Specifically, DJI drones account for approximately 70 percent of the total commercial drone market.[355] Commercial drone uses include construction, energy, infrastructure inspections, agriculture, media and entertainment, telecoms, mining, and mapping, to name a few. DJI products account for the lion's share of the public safety drone market too, comprising 91 percent of the drones being used in that sector.[356]

Public safety agencies, including law enforcement entities, are using them for a host of purposes, such as crime scene investigation, hazardous materials response, damage assessment, incident command and control, mapping, target searches, special teams support, training, and COVID-19 applications (e.g. public information and decontamination). With regard to the last, after the pandemic hit, in the spring of 2020, DJI gave away 100 drones to 43 different law enforcement agencies across 22 states to assist with coronavirus response efforts. This elicited a bipartisan outcry from Congress.[357]

CYBERSECURITY CONCERNS

In 2017, the U.S. Army went on the offensive against DJI when it issued a memo to its troops to "cease all use, uninstall all DJI applications, remove all batteries/storage media from devices, and secure equipment for follow on direction."[358] The U.S. Navy and Air Force followed suit, ultimately leading to a comprehensive DOD policy ban in 2018.[359] Multiple other federal agencies instituted similar policy bans, including the DOI and Department of Justice (DOJ).[360] Others tethered grant money to additional reviews of the drone's country of origin.[361] Contemporaneously, the DHS office responsible for protecting critical infrastructure, the Cybersecurity and Infrastructure Security Agency (CISA), sounded the alarm across the industry, warning of "the cyber and data security risks associated with information or communications technologies designed, manufactured, or sold by commercial enterprises operating under the control or influence of a foreign authoritarian state."[362] Espionage and theft of proprietary information were referenced as the primary associated risks.

The Executive upped the ante yet again in June 2019, when President Donald Trump issued a finding under the Defense Production Act (DPA) that small unmanned aircraft systems (sUAS) production is critical to U.S. national security. This sparked a pivoting of both efforts and resources to a made-in-the-U.S.A. drone focus.[363]

Two months later on the legislative side, Congress codified the DOD ban into law in Section 848 of the Fiscal Year 2020 National Defense Authorization Act (FY20 NDAA). This culminated in a Defense Innovation Unit project, the Blue sUAS list, through which five companies' drones were placed on the General Services Administration list for federal purchase.[364]

In March 2020, the American Security Drone Act (ASDA, SB 2502) flew through the Senate Homeland Security and Governmental Affairs Committee with unanimous bipartisan support. This proposed law would have banned federal agencies from acquiring Chinese drones and drones made with Chinese components and prohibited the use of federal grant money to buy Chinese drones or drone components. At the close of 2020, the ASDA inexplicably stalled in the conference version of the bill.[365]

In early 2021, a bipartisan group reintroduced an updated version of the ASDA in the 117th Congress.[366] This newest iteration largely tracks its predecessor. It would, with limited exceptions, prohibit the federal government from purchasing, operating, doling out federal funds, or using the government-issued purchased cards to buy "covered unmanned aircraft systems (UAS) from covered foreign entities."[367]

While reasonable minds can differ on the nature and extent of cybersecurity concerns associated with Chinese drones, there is general agreement that vulnerabilities exist. In July 2020, *The New York Times* reported on the collaborative research findings of U.S.-based GRIMM and

French-based Synacktiv, analyzing the privacy and security vulnerabilities of the Android DJI GO 4 app used to fly DJI drones.[368] Although code for the app was heavily obfuscated and difficult to analyze, researchers found issues: the app circumvents GooglePlay Store rules by directly providing updates outside of the store and without user knowledge, the app continues running and can restart itself when closed unless the user force quits it, and it allows a Chinese social media (Weibo) software development kit (SDK) interface to collect private user identifiable information that could be correlated down to the user level.[369]

While the study revealed no actual evidence that code is arbitrarily being executed on drone operators' phones, the possibility for this to occur exists. And there is precedent for such activity as China has previously hacked the Office of Personnel Management, Marriott, and Anthem.[370]

Photo by Mojtaba Mosayebzadeh / Unsplash

In early 2021, even before this GRIMM news, River Loop Security, a company which specializes in solving complex cybersecurity challenges in the Internet of Things and embedded devices space, published an analysis of DJI's Mimo app. This app connects the handheld DJI Osmo series of action cameras through the user's mobile phone to upload content to DJI-owned servers hosted in China.

Among other findings, they identified that the DJI Mimo app:

1. Uses libraries that request personal data about users' religious and political affiliation, as well as security settings from connected social network APIs
2. Sends data through insecure means to servers behind the Great Firewall of China, where it is accessible to the Chinese Government
3. Requests from users (via the operating system) access to fine and coarse location data, the ability to manipulate WiFi state, read SMS messages, and read logs
4. Fails to meet basic security practices for users' data, leading to potential disclosure or modification in transit
5. Terms of Use Agreement allows user data to be shared with the Chinese Government
6. Even without user consent, sends sensitive information via unsecured means to third-party servers, where the Terms of Use Agreement supports cooperation with the Chinese Government[371]

DJI disputes these claims and points to a March 2020 Booz Allen Hamilton (BAH) study of U.S. government-specific DJI drones. In the end, the BAH conclusion was consistent with the GRIMM report—there were indeed information-access vulnerabilities, but "no evidence that any actual data has been passed back based on these vulnerabilities."[372]

That said, information is power. Cyber vulnerabilities can, in fact, open doors to access data, which can then be exploited through the application of Chinese law. China's National Intelligence Law, enacted on June 27, 2017, was part of a cluster of laws to allegedly tighten national security. Others include Cybersecurity (2016, which went into effect on June 1, 2017), Counterespionage (2014), National Security (2015), Counterterrorism (2015), Foreign Non-Governmental Organization Management (2016), Ninth Amendment to the PRC Criminal Law (2015), and Management Methods for Lawyers and Law Firms (both 2016, which punish statements or actions deemed to threaten national security).[373] As a group, these laws require affirmative legal duties for Chinese and, in some cases, foreign citizens, companies, or organizations operating in China. Specifically, these entities are charged with providing access, cooperation, or support for Beijing's "intelligence-gathering activities," a term that is purposefully undefined in the law.[374]

Reportedly, the actual implementation of these laws is "messy in practice."[375] As Chinese companies have an interest in guarding their own intellectual property and global reputation, they sometimes publicly resist. One example is when Alibaba refused to turn over credit information to the People's Bank of China.[376] The concern is that such resistance, feigned or real, is required at all.

HUMAN RIGHTS VIOLATIONS

Just as the ASDA hit the chopping block in Congress, in what might be an impeccably timed coincidence, the Department of Commerce's Bureau of Industry and

Security (BIS) blacklisted DJI. This action was not based on cybersecurity or national security concerns, but rather on the company's human rights violations.

Specifically, in December 2020, the BIS added DJI to the economic blacklist or Entity List. This is part of the Export Administration Regulations that control the flow of the U.S. items, technology, and source code to individuals, organizations, and companies by requiring additional licensure to export, reexport, or transfer (in-country) when a listed entity is a party to the transaction.[377] All of these terms are nuanced, yet broad enough to preclude even basic interactions with listed entities, absent a special license. The challenge for both U.S. companies and DJI is that there is a presumption of denial for these license applications.

The standard for inclusion on the Entity List is "reasonable cause to believe, based on specific and articulable facts, that the entities have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States."[378] The official rationale for placing DJI on this list was the company's alleged "[enabling of] wide-scale human rights abuses within China through abusive genetic collection and analysis or high-technology surveillance, and/or [facilitating] the export of items by China that aid repressive regimes around the world, contrary to U.S. foreign policy interests."[379] DJI reportedly supplied drones to the Chinese government so that it could monitor detention camps throughout Xinjiang province.[380] Notably, Huawei had previously been placed on the Entity List.[381] License application reviews took more than six months and any approvals granted are not transparent.

While DJI's inclusion on the blacklist will remain a stumbling block to exchanges of items, technology, and source code, it does not constitute a prohibition on buying or using DJI drones in the short-term.

NATIONAL SECURITY CONCERNS

As members of Congress were introducing the ASDA of 2021, the Executive was putting pen to paper as well. Just two days prior to the end of his administration, on January 18, 2021, President Donald Trump issued Executive Order on *Protecting The United States From Certain Unmanned Aircraft Systems (UAS)* to "prevent the use of taxpayer dollars to procure UAS that present unacceptable risks and are manufactured by, or contain software or critical electronic components from, foreign adversaries, and to encourage the use of domestically produced UAS."[382]

The executive order requires federal agencies, within 60 days, to review their "authority to cease" procuring, funding, or contracting the "covered UAS" of foreign adversaries. And it defined foreign adversaries as China, North Korea, Iran, Russia, and any other foreign nation, foreign area, or foreign non-government entity that the Secretary of Commerce determines engages, "in long-term patterns or serious instances of conduct significantly adverse to the national or economic security of the United States."[383]

THE FUTURE

With a new administration at the helm, the question is whether or not we should expect a truce in the tech war with China. Given President Biden's plan to "Ensuring the Future is Made in All of America by All of American's Workers," perhaps a softer approach is unlikely.[384] Here are some questions that may be answered in 2021:

- Will the 117th Congress pass the newest iteration of the ASDA?
- Will federal drone policy bans and grant requirements dissipate, remain steady, or further proliferate?
- Will federal drone acquisition funding no longer be available for Chinese made drones?
- Will the five Blue sUAS companies step up production so as to overcome the Chinese drone giant before the commercial drone industry collapses upon itself?
- Will DJI remain on the economic blacklist?
- If so, will the downstream supply chain impacts topple the Chinese drone giant's market supremacy?

All of this remains to be seen. In the meantime, for the average drone user, it's business as usual. For the companies on the front lines of the global commercial drone ecosystem, not so much.

[349]"Interior Announces 2017 Drone Mission Report | U.S. Department of the Interior." 2018. U.S. Department of the Interior. February 20, 2018. https://www.doi.gov/pressreleases/interior-announces-2017-drone-mission-report.
[350]2011, Dennis O'Brien, USDA | Sep 30,. 2011. "USDA May Use Drones to Monitor Vast Western Rangeland | Farm Progress." Farm Progress. Farm Progress. September 30, 2011. http://www.farmprogress.com/government/usda-may-use-drones-monitor-vast-western-rangeland.
[351]"Unmanned Aerial Systems - Federal Highway Administration." n.d. Federal Highway Administration. http://www.fhwa.dot.gov/uas/.
[352]"Unmanned Aerial Systems | Homeland Security." 2018. Department of Homeland Security. January 17, 2018. http://www.dhs.gov/science-and-technology/unmanned-aerial-systems.
[353]1,756,885 drones are currently registered, consisting of 514,982 commercial users and 1,238,411 recreational, "UAS by the Numbers," FAA website, December 15, 2020, https://www.faa.gov/uas/resources/by_the_numbers/. But see FAA Aerospace Forecast Fiscal Years 2019-2039, which projected more than 800,000 drones by 2023. https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2019-39_FAA_Aerospace_Forecast.pdf.
[354] ltd, Research and Markets. n.d. "The Drone Market Report 2020-2025 - Research and Markets." Research and Markets - Market Research Reports - Welcome. Accessed January 4, 2021. https://www.researchandmarkets.com/reports/5117908/the-drone-market-report-2020-2025?utm_source=BW&utm_medium=PressRelease&utm_code=74l2tl&utm_campaign=1416130+-+Drone+Market+to+Grow+from+%2422.5+Billion+in+2020+to+Over+%2442.8+Billion+by+2025%2c+at+a+CAGR+of+13.8%25&utm_exec=joca220prd.
[355]Intelligence, Business Insider. 2020. "Commercial UAV Market Analysis 2020: Size, Growth & Forecast - Business Insider." Business Insider. Business Insider. February 10, 2020. http://www.businessinsider.com/commercial-uav-market-analysis#:~:text=With%20its%20headquarters%20in%20Shenzhen,share%20of%20the%20drone%20market.
[356]"RESEARCH | DRONERESPONDERS." n.d. DRONERESPONDERS. http://www.droneresponders.org/research.
[357]"Memorandum House of Representatives, Committee on the Judiciary, to Ms. Katharine T. Sullivan
Principal Deputy Assistant Attorney General, Office of Justice Programs, U.S. Department of Justice," May 13, 2020, https://assets.documentcloud.org/documents/6889784/2020-05-13-HJC-GOP-to-DOJ-Re-DJI-Drones-1.pdf
[358]"US Army Calls for Units to Discontinue Use of DJI Equipment - SUAS News - The Business of Drones." SUAS News - The Business of Drones, https://www.facebook.com/suasnews, 4 Aug. 2017, https://www.suasnews.com/2017/08/us-army-calls-units-discontinue-use-dji-equipment/.
[359]Kesteloo, Haye. 2018. "Department of Defense Bans the Purchase of Commercial-over-the-Shelf UAS, Including DJI Drones Effective Immediately - DroneDJ." DroneDJ. https://www.facebook.com/dronedj. June 8, 2018. https://dronedj.com/2018/06/07/department-of-defense-bans-the-purchase-of-commercial-over-the-shelf-uas-including-dji-drones/.
[360]https://www.doi.gov/sites/doi.gov/files/elips/documents/signed-so-3379-uas-1.29.2020-508.pdf; Department of Justice (DoJ) 9-95.100 - POLICY ON THE USE OF UNMANNED AIRCRAFT SYSTEMS.
[361]https://www.fema.gov/authorized-equipment-list-item/03oe-07-suas.
[362]CISA "Industry Alert: Chinese Manufactured Unmanned Aircraft Systems," https://content.govdelivery.com/attachments/USDHS/2020/06/03/file_attachments/1465486/Industry%20Alert%20-%20Chinese%20Manufactured%20UAS%20%2820%20May%202019%29.pdf.
[363]"Memorandum on Presidential Determination Pursuant to Section 303 of the Defense Production Act of 1950, as Amended | The White House." n.d. The White House. https://facebook.com/whitehouse. Accessed January 4, 2021. https://www.whitehouse.gov/presidential-actions/memorandum-presidential-determination-pursuant-section-303-defense-production-act-1950-amended/.
[364]National Defense Authorization Act for Fiscal Year 2020 (S. 1790; NDAA 2020, Pub.L. 116-92), https://www.congress.gov/116/bills/s1790/BILLS-116s1790enr.pdf
[365]"DIU." n.d. DIU. https://www.diu.mil/autonomy-blue-suas. The five companies were: Altavian, Parrot, Skydio, Teal, and Vantage Robotics
[366](Retired), Dawn M.K. Zoldi (Colonel, USAF,. 2020. "DJI Is Blacklisted: Whopper or Nothing Burger? - Inside Unmanned Systems." Inside Unmanned Systems. December 21, 2020. https://insideunmannedsystems.com/dji-is-blacklisted-whopper-or-nothing-burger/. Congress ultimately did not include the ADSA in the final Fiscal Year 2021 National Defense Authorization Act.
[367]ARM2106 JS2, American Security Drone Act of 2021, https://www.rickscott.senate.gov/sites/default/files/2021-01/ASDA%20FINAL.pdf
[368]For additional information on the ADSA of 2021, *see* Zoldi, Dawn M., "The American Security Drone Act: The Sequel," Drone Life, February 8, 2021, https://dronelife.com/2021/02/08/the-american-drone-security-act-the-sequel/
[369]Mozur, Paul, Julian E. Barnes, and Aaron Krolik. 2020. "Popular Chinese-Made Drone Is Found to Have Security Weakness - The New York Times." The New York Times - Breaking News, US News, World News and Videos. July 23, 2020. https://www.nytimes.com/2020/07/23/us/politics/dji-drones-security-vulnerability.html.
[370]"Is the Clock TikToking on Chinese Drones - American University Washington College of Law." n.d. American University Washington College of Law. https://www.wcl.american.edu/impact/initiatives-programs/techlaw/events/is-the-clock-tiktoking-on-chinese-drones/.
[371]*Ibid.* "Analyzing Data Use by the DJI Mimo App - River Loop Security." n.d. Home - River Loop Security. https://www.riverloopsecurity.com/blog/2020/05/dji_mimo/?fbclid=IwAR3pQZLAuHTvsGw2EOKSLNmgfTM_BEK--gwzT-54HPEBy44rmqHkN13Lh-0.
[372]"Risk Assessment: Detailed Report and Mitigation Plan Updated with Additional Testing and Analysis," https://www.precisionhawk.com/hubfs/Retest_DJI%20Cybersecurity%20Risk%20Assessment%20Final%20Report_03.31.2020%20Executive%20Summary%20(1).pdf
[373]"*Beijing's New National Intelligence Law: From Defense to Offense - Lawfare.*" 2017. Lawfare. July 20, 2017. https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.
[374]*Ibid.*
[375]NetChoice. 2020a. "Risk, Rhetoric and Reality: A Frank Conversation About Drone Data Security." YouTube. June 12, 2020. https://www.youtube.com/watch?v=TV0xLf7bl2E.
[376]*Ibid.*
[377]"Statement from Secretary Ross on The Department's 77 Additions to the Entity List for Human Rights Abuses, Militarization of the South China Sea and U.S. Trade Secret Theft | U.S. Department of Commerce." n.d. U.S. Department of Commerce. Accessed January 4, 2021. https://www.commerce.gov/news/press-releases/2020/12/statement-secretary-ross-departments-77-additions-entity-list-human.
[378]"15 CFR § 744.11 - License Requirements That Apply to Entities Acting Contrary to the National Security or Foreign Policy Interests of the United States. | CFR | US Law | LII / Legal Information Institute." n.d. LII / Legal Information Institute. https://www.law.cornell.edu/cfr/text/15/744.11. See Paragraphs (b)(1) through (5) of § 744.11.
[379]Federal Register / Vol. 85, No. 246 / Tuesday, December 22, 2020 / Rules and Regulations, https://www.govinfo.gov/content/pkg/FR-2020-12-22/pdf/2020-28031.pdf.
[380]"Bloomberg - DJI Won the Drone Wars, and Now It's Paying the Price" n.d. Bloomberg - DJI Won the Drone Wars, and Now It's Paying the Price. https://www.bloomberg.com/news/features/2020-03-26/dji-s-drone-supremacy-comes-at-a-price.
[381]Federal Register / Vol. 85, No. 97 / Tuesday, May 19, 2020 / Rules and Regulations, https://www.govinfo.gov/content/pkg/FR-2020-05-19/pdf/2020-10856.pdf.
[382]Executive Order 13981 of January 18, 2021, *Protecting the United States From Certain Unmanned Aircraft Systems*, 86 FR 6821, pages 6821-6823, https://www.federalregister.gov/documents/2021/01/22/2021-01646/protecting-the-united-states-from-certain-unmanned-aircraft-systems
[383]*Ibid.* For more detailed coverage, *see* Zoldi, Dawn M.K., "Show Me the Money! Adversary Country Drones To Be Replaced?" Drone Life, January 21, 2021, https://dronelife.com/2021/01/21/the-latest-executive-order-on-drones-the-ban-on-chinese-and-covered-country-uas-expanded/
[384] "The Biden Plan to Ensure the Future Is 'Made in All of America' by All of America's Workers | Joe Biden for President: Official Campaign Website." n.d. Joe Biden for President: Official Campaign Website. https://www.facebook.com/joebiden. https://joebiden.com/made-in-america/. See also Hass, Ryan, Ryan McElveen, and Robert D. Williams. 2020. "The Future of US Policy toward China." Brookings. Brookings. November 17, 2020. https://www.brookings.edu/multi-chapter-report/the-future-of-us-policy-toward-china/.

Dawn M.K. Zoldi (Colonel, United States Air Force, Retired) is an Adjunct Professor at the Colorado State University-Pueblo, Chief Executive Officer/Founder of P3 Tech Consulting LLC, a licensed attorney, and 25-year Air Force veteran and 3-year federal civil servant. She is an internationally recognized expert on unmanned aircraft system law and policy, recipient of the Woman to Watch in UAS (Leadership) Award 2019, and a columnist for both *Inside Unmanned Systems* and *Inside GNSS magazines*.