Prepared Statement of Harry Wingo
Faculty, College of Information and Cyberspace,
National Defense University

U.S. Senate
Committee on Commerce, Science and Transportation
Subcommittee on Security
"Drone Security: Enhancing Innovation and Mitigating Supply Chain Risks"
June 18, 2019

Chairman Sullivan, Ranking Member Markey and members of the Subcommittee, thank you for the opportunity to address the security of unmanned aircraft systems (UAS, or drones). I am humbled to have the chance to assist your efforts to build a prosperous and secure Nation. Fully integrating UAS into the National Airspace System (NAS) can create new jobs and enhance the quality of life for all Americans. This promise depends, however, on the security of UAS, including understanding and managing risks to drone supply chains.

As faculty at the Nation's cyber war college, the National Defense University's College of Information and Cyberspace, I educate national security leaders about strategic risk. The views I express today are my own; I am not speaking for the U.S. Department of Defense. My personal and academic perspective reflects over 25 years focused on law and policy issues concerning networked technologies, including roles at Google, where I helped the CEO, CISO and other leaders to engage Congress and the White House in the wake of the "Operation Aurora" cyber attacks; at the Federal Communications Commission, where I focused on broadband, spectrum and network security issues; and, for this Committee, as counsel to the great Senator Ted Stevens, when he served as Chair. My views also reflect my over six years of active duty service as a Navy SEAL officer, and my ownership of three small drones.

Accelerating the integration of UAS into commerce must be done with a focus on supply chain security. Also key, however, is a special kind of supply chain risk: The U.S. is over-reliant on the Chinese drone monopoly embodied in SZ DJI Technology Co., Ltd., doing business as DJI.

While advances in commercial drone technology are many, and encouraging, I respectfully invite the Subcommittee to examine the widening gap between China and the United States with respect to the market share of small drone (less than 55 lbs.) platform manufacturers like DJI.

Small drones are no small matter.

In 2016, the White House estimated that UAS could spur up to $82 billion in economic growth by 2025 and generate 100,000 jobs.[1] The potential for drones to benefit commerce has captured the interest of many companies and countries around the world. In the race to UAS dominance, however, China has taken a commanding lead in recent years.

DJI's market share may exceed 70 percent globally, and 80 percent in the U.S. While hobby drone market share is different than commercial market share, by any standard, China's leading drone company is dominating the UAS space. DJI employs 14,000 people, and is based out of Shenzhen.[2] Meanwhile, Western drone companies like Parrot SA, a French company, lag far behind. Others struggle to gain market share, remain relegated to specific niches, have shut their doors, or have shifted away from the drone platform market. One UAS innovator, Chris Anderson, CEO of U.S.-based 3D Robotics, has pivoted from a platform strategy to one of providing the software and analytics for UAS.[3]

While it is important to consider the security of all drones in commerce, the global dominance of China's small drone platform manufacturer, DJI, warrants a closer look with respect to its outsized impact on drone security, but also on the long term viability of U.S. companies as alternatives here and around the globe. This second aspect of supply chain risk management is of a special, critical nature: It presents a National risk, similar to that highlighted by President Trump in calling out the risk of using 5G equipment from Huawei (another Chinese company) in U.S. telecommunications networks. Unique risks arise from DJI's being based in, and operated from, China -- a peer competitor to the United States.[4]

The Rising Stakes of Drone Supply Chain Risk Management.

The FAA has noted that drones are the fastest growing component in aviation, with more than 350,000 UAS doing things that would be difficult or dangerous for human beings to do.[5] Drones are digital infrastructure, and will play a key role in allowing the safe and secure integration of *unmanned* aviation operations, including flights over people, night operations and beyond visual line of sight operations. A safe and efficient UAS Traffic Management (UTM) system means that drone security extends beyond just the individual drones themselves, but to the connected systems that will include detect-and-avoid capabilities and permit reliable and secure data links

---

[1] McKevitt, J. (2017, March 23). *FAA: Drones will fill the skies in 2021*. Supply Chain Dive. Retrieved from https://www.supplychaindive.com/news/FAA-commercial-drone-use-delivery-logistics/438710/.
[2] Berlinger, J. (2019, January 21). Chinese drone maker DJI uncovers fraud that could cost it $150 million. CNN Business. https://www.cnn.com/2019/01/21/tech/dji-fraud-investigation-china-intl/index.html.
[3] *See, e.g.,* Perlman, A. (2016, December 12). 3D Robotics' Cautionary Tale: Losing The Hardware Game To China and Pivoting To Software for Survival. UAV Coach. https://uavcoach.com/3d-robotics-pivots-to-software-for-survival/.
[4] U.S. Department of Defense. (2018). Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
[5] Federal Aviation Administration. (2019, April 30). Fact Sheet–The UAS Integration Pilot Program and UAS Traffic Management Pilot Program. https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=23574.

between Part 107 pilots and unmanned aircraft. Autonomous drone operations, like land-bound driverless cars and trucks, demand "baking in" privacy and security from the design phase.

A future-oriented, interconnected aviation network that relies on emerging technology like artificial intelligence (AI) and 5G networks, will revolutionize commerce. The range of use cases are highlighted by the FAA's ten drone innovation projects in Fairbanks, Alaska; Reno, Nevada; San Diego, California; North Dakota; Kansas; Durant, Oklahoma, with the Choctaw Nation of Oklahoma; Memphis, Tennessee; Lee County, Florida; North Carolina; and Herndon, Virginia. The projects include emergency management, agricultural support and infrastructure inspections.

Supply chain threats vary for UAS, and range from counterfeit parts to "back doors" installed to enable remote control of drones or otherwise disrupt UAS operations. Physical supply chain threats are perhaps overshadowed by software supply chain threats, which have increased as drones routinely connect to off-shore clouds of foreign companies. Companies routinely reassure customers about security, but the provision of firmware updates and the data flows from platforms back to offshore cloud-computing storage facilities can increase risk to UAS operations. Even if UAS were delivered to customers in "pristine" condition, the subsequent back and forth of image processing and analytics data flows, along with software and firmware updates, opens a "front door" to risk. Images collected in the U.S. for storage in China, and subject to AI and machine learning, can be demanded by Chinese authorities without the knowledge of U.S. customers. How would a U.S. customer know such a request was made?

"Great Power" Competition and Supply Chain Risk. Beyond the supply chain security risks that exist for the entire industry, there is a special class of risk concerning China's dominance of the U.S. drone market. Unlike other potential threat actors, China poses the most serious potential threat to U.S. drone security--that of a peer competitor that clearly intends to dominate the general space in which drones reside: Global Supremacy in Artificial Intelligence.[6]

In the context of National risk posed by over-reliance on Chinese drones, I respectfully call the Subcommittee's attention to what I call the "Three Ds" of strategic drone supply chain risk:

1. **Data Flows**. Reliance on broadband connections to offshore clouds gives China unprecedented information about U.S. commerce (and more).
2. **Dual Use**. China is an important and valued trading partner, but U.S. leaders are mindful of the (hopefully avoidable) potential for U.S.-China conflict, beyond competition, where UAS and other "Industry 4.0" technology would provide military advantage.
3. **Dependency**. Next-generation drone commerce in the U.S. is increasingly reliant on a Chinese drone platform monopoly, a factor that could hinder innovation and economic security.

[6] *See, e.g.,* Allen, G.C. (2019, February 6). Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security. The Center for a New American Security. https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

Data Flows. The information risk from data flowing to China's autocratic government should concern more than U.S. government customers. The Pentagon in recent years has shifted from risk mitigation to risk avoidance when it comes to Chinese drones. The Pentagon ordered the U.S. military to stop using DJI drones a few years ago, and the Department of Homeland Security has issued warnings to their use in areas that impact National Critical Functions.[7] More recently, the President issued a memorandum finding that "the domestic production capability for small unmanned aerial systems is essential to national defense."[8]

Despite these precautions, the less risk-averse commercial sectors are embracing Chinese drones, as are State and Local governments who are choosing to purchase DJI platforms, and to take advantage of the company's very capable analytics tools and services.[9] While sharing information from individual users, or even the data from specific companies or government units may seem inconsequential, DJI is compelled by Chinese law to provide information to the Chinese government. DJI's prowess in applying cutting edge data science to the growing deluge of data flowing into its cloud compute and storage assets is always available to the Chinese government. Making this U.S. information available to China must be considered in the context of that country's official position on achieving dominance in areas of disruptive technology like AI and Machine Learning.

Dual Use. While it is important to acknowledge that DJI has created technically compelling technology and services, they continue to do so with the support of the Chinese government and in the context of great power competition between the U.S. and China in areas that relate to national security as much as they do to commerce.

History teaches that economic and national security are closely linked. The recently celebrated Allied victory on the beaches of Normandy, and ultimately victory in the World War II, turned on technological power cultivated first in the field of commercial innovation. The modest beginnings of Henry Ford's Model T bloomed into U.S. dominance of the automotive market, which allowed our Nation pivot to building machines of war. U.S. innovation in electronics and communications technologies like telephones, radio and television, eventually supported military radar and the Allied breakthrough at Bletchley Park, where the private sector, academics and the national

---

[7] Sobczak, B. (2019, May 21). Feds to energy companies: Beware drone made in China. E&E News. https://www.eenews.net/stories/1060369689.

[8] President Donald J. Trump. (2019, June 10). Memorandum on Presidential Determination Pursuant to Section 303 of the Defense Production Act of 1950, as amended. https://www.whitehouse.gov/presidential-actions/memorandum-presidential-determination-pursuant-section-303-defense-production-act-1950-amended/.

[9] *See, e.g.* Reagan, J. (2018, October 31). Propeller Partners with DJI to Bolster Drone Analytics and Mapping. Drone Life. https://dronelife.com/2018/10/31/propeller-partners-with-dji-to-bolster-drone-analytics-and-mapping/; DJI. (2015, November 11). Commercial Drone Data Opening Up New Opportunities for Industrial Applications. https://www.dji.com/newsroom/news/blog-commercial-drone-data-opening-up-new-opportunities-for-industrial-applications.

security community united to defeat the Nazis' Enigma machine. Commercial success led to military success.

As a counsel for Google years ago, I had the honor to work with Vint Cerf, who while at DARPA co-created TCP/IP, a technology that enabled the Internet. That open protocol built on packet switching, a networking technology designed to make resilient our Nation's nuclear strike command and control capabilities. Today, China is aggressively dedicating national resources to building 5G networks able to increase Internet of Things (IoT) connections by 10 to 100 times that of current 4G networks, all with an eye towards winning the race to overmatch with respect to AI-enabled capabilities in UAS and other robotics technology. While that advantage can be applied to commerce, it also enhances China's military power.

Dependency. The U.S. has struggled to stem the tide when it comes to growing or even maintaining its manufacturing capability with respect to UAS platforms. There are many reasons for this, and the details might possibly take up an entire hearing. What matters now is taking a hard look at why and to what extent our Nation is relying on Chinese drone infrastructure.

The technical capabilities and rapidly evolving features of DJI drones have led even first-tier U.S. public safety teams like the New York Police Department to turn to China for UAS platforms. These choices are being made despite the Pentagon's ban on military use of DJI, perhaps as a result of the law enforcement community facing limited funding, a shortage of cybersecurity professionals able to assess the risk, or simply a willingness to accept a different level of risk than the U.S. military. Nonetheless, the different positions with respect to DJI that is being taken by the Nation's first responders highlights the shortage of alternatives to Chinese drones.

The United States is poised to leverage advances like the FAA's UTM system and Remote ID for UAS, but the Congress should explore deeply whether the benefits that will accrue from this might be diminished by the trailing market share of U.S. companies in the platform market for UAS. This harsh market reality may loom in related areas like 5G infrastructure, or even in the AI systems for self-driving cars or indoor robotics to be used in smart factories, hospitals, hotels and homes. While China over the past 20 years has played an important role in global commerce by augmenting the supply chain of U.S. companies, the glaring gap between U.S. and Chinese companies like DJI in the UAS platform market should be a wake up call.

Recommendation: Balance Risk Through Enhanced USA-Drone Incentives.

I respectfully suggest the following potential areas for further inquiry, oversight or legislation:

Incentives for Drones as "Digital infrastructure". Drones and UAS are digital infrastructure. Just as President Eisenhower's Interstate Highway Initiative had long-reaching benefits, an investment in the next-generation aviation infrastructure that UTM represents warrants investment tailored to create incentives for the private sector. While funding concrete and steel

for infrastructure projects matter, it is important to envision the "drone highways" of the future and make sure that we craft the right policies to remove legal and policy barriers to innovation by U.S. companies, from startups to existing industry leaders like Amazon, FedEx, UPS, Boeing or Lockheed. Another company to consider engaging is Uber, who is working with the Army Research Lab and the University of Texas at Austin to provide "UAS on demand" services.[10]

USA Assembly. The recent attention to Huawei in the context of 5G infrastructure and a U.S.-China "trade war" has led many to ask whether we could sever all ties to China when it comes to high-tech manufacturing for things like 5G equipment, or in this case, UAS platforms. The reality is that short of armed conflict with China, it is unlikely that a radical, across the board decoupling of our micro-electronics supply chains with China would be possible (or beneficial). The Chinese are far ahead of the U.S. on chip assembly, even if we retain an advantage on chip foundries like Intel.[11] It is worth exploring whether and how it might be possible to cultivate realistic alternatives to Chinese assembly of the smart components within UAS. It is possible that advances in automation and AI-enabled smart factories might help in this effort. The President's recent memorandum declaring small UAS essential to national defense highlights a potential area for leveraging related efforts within the U.S. government to grow our domestic UAS production capacity.

Abruptly disentangling our micro-electronics supply chain completely from China would be difficult, and (short of outright armed conflict with China) likely counter-productive. That said, we should identify and cultivate alternative manufacturing partners, including particularly those in the Western Hemisphere, Europe and Africa, and in coordination with our "Five Eye" (FVEY) partners (The United Kingdom, Canada, Australia, and New Zealand) and NATO countries. With respect to NATO countries, France is of particular interest on UAS since the Paris-based company Parrot SA is a distant but capable competitor to DJI in the UAS platform market. Also noteworthy in the NATO context is the Swiss company Flyability, whose indoor-drones are being used to inspect U.S. nuclear power facilities. On the homefront, an innovative leader in AI-enabled drone operations is Shield AI, which has a lidar-enabled drone capable of flying autonomously through buildings. Based out of San Diego, Shield AI has 100 employees and is an example of platform innovation in the small drone space industry.

Open source. The Subcommittee might also explore the role that open source initiatives like the DroneCode Project might play in providing more transparency, particularly if U.S. companies

[10] Miller, S. (2018, August 14). Army Research Lab teams up with Uber. https://defensesystems.com/articles/2018/08/15/uber-arl-ut-nasa.aspx. (These would be above the 55 lb. limit for "small UAS" in the FAA's 14 C.F.R. Part 107 regulations, of course.).
[11] Wang, B. (2019, February 23). China's Semiconductor Catchup is Critical to Future Technology Competition. Next Big Future. https://www.nextbigfuture.com/2019/02/semiconductor-race-and-parity-is-key-to-global-technological-competition.html.

continue to purchase Chinese platforms. Currently, DJI adheres to a proprietary model that acts to help lock-in its market dominance.[12]

While the best result would be a growing and competitive U.S. market in UAS platforms, incentives to encourage the growth of an open ecosystem to counter DJI's proprietary system may help. The limitations of this approach likely include the fact that open protocols work better when championed by a large player in the market. Consider the role that Google played in driving the success of Android phones. Whether open-source models like DroneCode can help to boost the market share of U.S. drone manufacturers is something worth examining.

Link "USA Drone" Incentives to AI Initiatives. President Trump's Executive Order on Maintaining Leadership in Artificial Intelligence, issued earlier this year, is a reminder of the high stakes in the AI race between the U.S. and China.[13] It is worth reviewing ways that the Subcommittee might find common ground with other National efforts related to AI. Integrating UAS into the NAS safely and securely is an effort that implicates AI and Machine Learning, and finding ways to leverage related efforts -- like accelerating the use of autonomous vehicles on our nation's streets and highways -- may help to speed the National use of drones in commerce.

Understanding smart cities is one challenge facing the integration of UAS into the NAS. I have personally researched a different area, but one that concerns the use of AI and UAS: Using indoor drones to help save lives during an active shooting.[14] This scholarship is an example of the work that I and my colleagues do on behalf of the Nation, at NDU's the College of Information and Cyberspace.

Conclusion. The alarming lead taken by China in this increasingly important area of interstate commerce demands purposeful, strategic action to level set U.S. drone manufacturing with our peer competitor. The United States is poised to reap the benefits of a next-generation aviation system that relies more on autonomous systems connected by 5G networks. This transition may be threatened, however, by continued dependence on Chinese UAS platforms. The future of American commerce is at stake.

I look forward to answering any questions you may have, and to further discussing this or related matters with the Subcommittee. Again, thank you for the opportunity to testify.

---

[12] *See, e.g.,* DJI. (2018, October 31). DJI Expands Drone Ecosystem With New Hardware, Software and Partnerships To Help Enterprises Gain Aerial Productivity: AirWorks 2018 Bolsters The DJI Platform For Businesses, Governments, And Others Ready To Do Their Work Better With Professional Drones. *https://www.dji.com/newsroom/news/dji-expands-drone-ecosystem*.

[13] White House. (2019, February 11). Executive Order on Maintaining Leadership in Artificial Intelligence. https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

[14] Wingo, H. (2018). Set Your Drones to Stun: Using Cyber-Secure Quadcopters to Disrupt Active Shooters. Journal of Information Warfare, Vol. 17, Iss. 2, p.54-64. https://search.proquest.com/openview/1ac335453924ced1aca49794f419d958/1?pq-orgsite=gscholar&cbl=2046421.