PUBLIC COMMENT: FOUNDATION FOR DEFENSE OF DEMOCRACIES

DEPARTMENT OF COMMERCE

Securing the Information and Communications Technology and Services Supply Chain

Unmanned Aircraft Systems: [Docket No. BIS-2024-0058]

AUTHORS

RADM (Ret.) Mark Montgomery
Senior Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Craig Singleton
Senior Director of the China Program at the Foundation for Defense of Democracies

Johanna Yang
Research and Editorial Associate for the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Jack Burnham
Research Analyst for the China Program at the Foundation for Defense of Democracies

Washington, DC
March 4, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Department of Commerce
Bureau of Industry and Security
Docket No. [BIS-2024-0058]

Public Comment on Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems

Overview of the UAS Threat from Foreign Adversaries (The People's Republic of China)

As part of its bid to supplant the United States as the world's leading power, the People's Republic of China has pursued dominance within a great number of emerging technologies, including the unmanned aerial systems (UAS) sector. China seeks to gain leverage over the United States and its allies and partners via America's reliance on Chinese supply chains, simultaneously heightening the Chinese Communist Party's (CCP) capacity to undermine U.S. national and economic security.

These developments have not only hampered the domestic U.S. drone industry but also given Beijing unfettered access to sensitive information about U.S. military installations and critical infrastructure. Chinese UAS technology and surveillance is paired with stringent national security laws that require even nominally civilian Chinese firms to share their data with CCP authorities. As such, China has gained both the capacity to map U.S. critical infrastructure and a blueprint for targeted cyberattacks and cyber-physical espionage. These risks are further heightened by the integration of internet-connected components, including software and hardware, into leading Chinese UAS models, allowing Beijing further access into U.S. networks via seemingly harmless patching and/or firmware updates.

Marking an escalation in its rivalry with the United States, Beijing has intensified its efforts to monitor and infiltrate U.S. critical infrastructure. In a campaign nicknamed "Volt Typhoon," PRC-linked hackers gained malicious access into U.S. transportation systems, water systems, communication networks, and energy networks, which could subsequently be used during a future crisis to disrupt or degrade U.S. military mobility and economic productivity. This was effectively an effort to conduct operational preparation of the battlefield.

This campaign is coupled with other efforts by PRC-affiliated hackers to compromise communications infrastructure. A campaign nicknamed "Salt Typhoon" infiltrated U.S. domestic telecommunications and internet infrastructure, allowing the PRC to access communications between senior American government officials, U.S. citizens' metadata, and secure Justice Department communications, among other assets. Another campaign, dubbed "Flax Typhoon" compromised communications and other technical systems linking the United States to East Asia.

These attacks could undermine Washington's ability to mobilize its military forces and provide Beijing with the ability to disrupt American society by endangering the nation's water and food supply, among other critical resources. Incursions into U.S. military and critical infrastructure can only be further enabled by Chinese UAS dominance.

The consequences of improper regulation of the UAS industry could entail losing U.S. intellectual property to Chinese companies and further exposing American assets to sabotage. The below will provide further detail into the threat posed by PRC drone technology dominance.

Evaluation of Risk Posed by Chinese Involvement in U.S. UAS ICTS Supply Chain

China has deeply penetrated the American UAS information and communications technology and services (ICTS) supply chains and has repeatedly demonstrated its willingness to weaponize its dominance within these supply chains to achieve its economic and geopolitical objectives.

Chinese Penetration into U.S. UAS ICTS Industry

China has sought to develop its UAS sector through a combination of state-directed investments and private sector growth. Having identified UAS technology as a key sector in its "Made in China 2025" campaign, Beijing has directed substantial investment towards its domestic UAS industry, namely by building out supply chains, nurturing national champions, and modifying regulatory barriers. This strategy is intended to develop a new engine for economic growth in the form of a "low altitude" economy by developing technologies with potential military applications and strengthening the capacity of the country's science and technology sector to compete globally.

China's role in the American UAS ICTS supply chain is significant and covers a range of secondary and tertiary inputs. Da-Jiang Innovations (DJI), a UAS manufacturer based in Shenzhen, is the undisputed leader within the American UAS supply chain, having captured nearly 90 percent of the consumer market and 75 percent of the industrial market. Other Chinese firms, such as Autel Robotics, also based in Shenzhen, have captured roughly 15 percent of the total U.S. market. Both producers sell to a range of U.S. based clients, including hobbyists, commercial ventures, and first responders, and are preferred due to their low cost, high quality, broad versatility, and ease of use.

Driven by a combination of regional economic clustering and state support, these firms rely on Chinese-based supply chains for sourcing ICTS components. While DJI once primarily relied on "off the shelf" components — many of which were sourced from the United States to guarantee price competitiveness — the company has steadily pivoted toward domestic suppliers,

supporting a growing ecosystem of interconnected firms. These secondary firms have subsequently become key global suppliers of UAS ICTS, including flight controllers, gyroscopes, and flight software, further integrating China into the U.S. UAS supply chain.

This strategy is also cemented by China's investments in related industries, including battery systems, semiconductors, and artificial intelligence, all of which offer spill-over benefits to UAS production. As part of its efforts to achieve technological self-sufficiency, the CCP has invested billions in industrial subsidies to strengthen key strategic industries seen as foundational for securing economic and military power: the "legacy" semiconductor sector, advanced battery technology, and versatile AI systems for autonomous vehicles.

Chinese Supply Chain Dominance Poses Significant Risks to U.S. National Security

Having stated its desire to supplant the United States as the leading global power, China has several available avenues to disrupt, co-opt, and weaponize its integral role within the UAS ICTS supply chain. These include conducting espionage, sabotaging U.S. critical and military infrastructure, undermining American commerce, and harming U.S. foreign and security policy.

Under China's National Intelligence Law of 2017, along with subsequent legislation such as the Data Security Law of 2021, private Chinese firms and citizens are compelled to cooperate with the CCP on matters deemed essential to national security. These laws nearly guarantee that data collected on U.S. individuals and entities by firms under Chinese jurisdiction will be accessed by state intelligence and security agencies, opening the door for broad-range espionage campaigns. Chinese law reflects the CCP's capacity and willingness to compel private firms to introduce covert entry points and deliberately placed loopholes within key software and hardware systems, compounding the vulnerabilities already introduced by Chinese UAS dominance.

As UAS assets are used to monitor and carry out a range of functions across U.S. critical infrastructure, agriculture, and commercial sectors, the security of this supply chain is paramount. These concerns are amplified by the potential cascading impact of an adversary's intrusions into UAS ICTS, particularly within critical sectors of the U.S. economy. DJI is the primary supplier of agricultural UAS, particularly crop sprayers, and interruptions within this supply chain may lead to lower yields, higher food prices, and substantial ripple effects within global commodity markets. Farming communities across the United States also use Chinese drones to survey land and livestock, collecting vast amounts of agricultural data. This data can be weaponized, giving China leverage over critical food production, resources, and supplies. With this access, China has the capability to unleash biological warfare against crops and livestock — a crisis America again cannot afford to bear.

Given the role of UAS systems in servicing a range of critical infrastructure, including public utilities, communications, and transportation, China has both the capacity and the incentive to utilize UAS ICTS to conduct espionage campaigns against the United States. The depth of this integration produces a broad range of additional risks, including reconnaissance, supply chain disruptions, hacking, and data theft. Improvements in both the quality and affordability of UAS sensor technology, much of which is produced within China, have rendered UAS platforms increasingly valuable sources of information, further increasing Beijing's incentive to compromise the ICTS supply chain.

Even more concerningly, these assets often interact with elements of the U.S. military, operating close to bases and other sensitive facilities. American emergency response personnel, including police, fire, and search and rescue, also utilize this technology. Chinese UAS surveillance of U.S. facilities is a significant espionage advantage, one the United States cannot afford to cede.

These risks extend to American commerce, as the CCP has steadily undercut the U.S. UAS industry by directing millions in state subsidies towards domestic manufacturers, along with key upstream suppliers of other UAS technology. By creating national champions such as DJI, these investments have allowed Chinese UAS ICTS suppliers to offer substantial discounts by pricing their technology well below the cost of production. These practices are illegal under anti-dumping statutes, and not only undermine the cost-competitiveness of the U.S. UAS industry but also hinder the development of a domestic alternative to PRC-dominated supply chains. China has also utilized this strategy in other ICTS components such as semiconductors, allegedly subsidizing its domestic industry to undermine U.S. reshoring efforts.

Chinese Supply Chain Dominance Aids Other Adversarial Campaigns

The PRC has also managed to leverage its state-backed UAS ICTS advantage to aid Russia in its illegal war against Ukraine. Beijing has supplied critical ICTS components needed for Russia's domestic defense production. China allegedly reinforces Russian offensive capabilities by manufacturing the loitering munition Garpiya-3 in the Xinjiang region, and advances development of the Reaper-style attack drone, the REM 1. China's supply and manufacturing resources have given Moscow a pathway to both evade Western sanctions and gain access to innovative military equipment, providing a lifeline to its war economy.

In contrast, China has cut off Ukraine's access to key ICTS components, including flight controllers, radio modules, and navigation cameras, due to its concern that Kyiv will use such imports in its defensive efforts. These asymmetrical restrictions highlight Beijing's willingness to use its relative dominance within the global UAS ICTS supply chain to support U.S. adversaries, particularly within the context of a military crisis that directly harms U.S. national security.

China also uses this leverage to block American UAS firms from supplying state clients in Taiwan. Skydio, a DJI competitor, is the largest U.S. UAS manufacturer and sells UAS systems to Taiwan's National Fire Agency. In response, China introduced sanctions against the firm, forcing it to restrict its sales due to a lack of PRC-supplied battery components. Defending the measure, the Global Times, an English-language Chinese propaganda outlet, claimed that Skydio could escape sanctions by "proactively remov[ing] itself from the US government's list of suppliers 'arming Taiwan' and cease using unfair means to suppress Chinese companies and disrupt market order," directly linking the firm's support for Taiwan to Beijing's actions.

Conclusion

China's unfair trade and manufacturing practices and exploitative espionage laws, compounded by its willingness to exercise the power therein, introduce an unacceptable national security threat to the United States. The Department of Commerce's proposed rule is critical to protecting U.S. interests and securing the U.S. UAS ICTS supply chain. Given China's repeated intrusions into military and critical infrastructure, as well as its dominance of the global drone supply chain, the federal government should advance the provisions outlined in this rule to protect U.S. assets from espionage and sabotage by foreign adversaries.

Thank you for considering our comments, and we look forward to seeing how our input is incorporated into the final rule.

RADM (Ret.) Mark Montgomery is the senior director at FDD's Center on Cyber and Technology Innovation, and a senior fellow at FDD. He also directs CSC 2.0, an initiative that works to implement the recommendations of the congressionally mandated Cyberspace Solarium Commission, where he served as executive director. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

Craig Singleton is a senior fellow at FDD, where he also serves as senior director of FDD's China Program. He previously spent more than a decade as a senior U.S. diplomat, completing multiple overseas assignments in the Middle East, Latin America, and East Asia. While stationed in Washington, DC, Craig focused on developing policies aimed at confronting China's malign influence activities and North Korea's nuclear weapons program.

Johanna (Jo) Yang is a research and editorial associate at FDD's Center on Cyber and Technology Innovation.

Jack Burnham is a research analyst at FDD's China Program.