

29 July 2026

IW PERSPECTIVES



Cultivating Vulnerability: The Irregular Warfare Campaign Against American Farms and America's Economy

By Dr. John Ringquist

Dr. John Ringquist is an instructor at the Command and General Staff College and a retired U.S. Army Lieutenant Colonel. His background in biology and past work with food science fuel his interest in supply chain study and protection. He is a prolific writer in professional and peer-reviewed publications.

China is engaging in tactics just short of war, unconstrained by any formal declaration of hostilities as it seeks weaknesses to exploit in the United States Farm Surveillance Program and Homeland Defense initiatives. The U.S. agricultural supply chain is under attack from global competitors seeking to degrade America's ability to feed its populace and export products. Special academic relationships between U.S. and Chinese [universities](#), and scientific expert [exchanges](#) are being abused by Chinese scientists with links to

The views expressed in these articles are those solely of the authors and do not reflect the policy or views of the Irregular Warfare Center, Department of War, or the U.S. Government.

the Chinese military and associated intelligence programs. Chinese researchers in the U.S. have been implicated in smuggling pathogens and potential biological material. Further, U.S. agribusinesses are vulnerable to cyberattacks that threaten to crash food production and transport. [Food production warfare](#) is part of [asymmetric warfare](#) as much as cyber incursions or espionage. Competitors willing to wage long campaigns can probe supply chains for weaknesses, strike industrial control processes, and introduce bioagents into our food system that degrade its viability and consumer confidence. China's playbook includes biological and cyber tools that it is already employing to undermine the United States and gain advantage in world markets.

Americans take for granted that we will be able to weather natural disasters and that the domestic food supply system will adjust for unseasonal weather impacts on our crops. The fact is that our food supply chain has always been vulnerable and attacks have been a potential threat since before the Cold War. Even during the mid-2010s Global War on Terror, Al-Qaeda planned to target the United States agriculture sector in order to induce domestic conditions that would force the United States to leave [Afghanistan](#).

In response to the potential for foreign attacks against agriculture, the Department of Homeland Security implemented measures designed to protect U.S. farms and the food supply chain. Although oriented toward early detection and quarantine of modified organisms and threats to livestock, the measures are also economic in nature. The 2025 [National Farm Security Action Plan](#) introduced a series of measures to protect national security by defeating foreign attempts to infiltrate biological pathogens into the national supply chain. Further, the plan restricts foreign ownership of farmland by Russia, China, Iran, and North Korea. [Additional measures](#) include agricultural supply chain resilience enhancement, tougher screening against pathogen entry at customs inspection points, animal biosafety enhancements, and protection of agricultural research and ideas.

China is likely to favor indirect methods to affect American agriculture. The 1999 document "[Unre-](#)

[stricted Warfare](#)" espouses a "no limits" approach. Although "Unrestricted Warfare" is not strategy, its advocacy for competition across all domains and at all times by whatever means possible renders most agreements and treaties secondary to national ambition. China is building a national science capability that will make biological asymmetric warfare possible and may already be [developing agents](#).

China's national defense writings emphasize the importance of biotechnology in its national defense strategy. Beginning with the 2010 publication of [War for Biological Dominance](#) and elaborated upon further in [2022 in Science of Military Strategy](#), Chinese military thought embraces an approach to [biology and biotechnology](#) that implies that biological warfare will be a part of [China's future plans](#). Additional documents including 2015's declaration of biotechnology as a new "strategic height," reinforced by 2017's biology as a "new domain of warfare," emphasize China's intentions. [Biology](#) is an offensive tool in the competition paradigm and senior People's Liberation Army leaders have noted that genetic engineering of biological agents will make them "more toxic, more contagious, and more [resistant](#)." However, in asymmetric warfare, biological agents are more likely to be employed gradually and with a systematic approach to achieving goals without crossing into actions that amount to a declaration of war. One example of China's incremental approach to test the biosensor and screening effectiveness of the United States was the mass mailing of millions of random [seed packets](#) from addresses originating in China. The end result could have been the mass introduction of [biohazards](#) or biological agents into the U.S. through seemingly random and innocuous mail from China. China defeated customs checkpoints by using commercial international mail.

A more deliberate stage of biological sabotage against U.S. food crops is occurring through academic exchange programs. [Researchers from the China](#) have proven themselves to be Trojan Horses in the system. Scientists from Chinese academic institutions come to the United States to conduct scientific research ostensibly for

the good of all. However, these researchers are responsible for reporting their research to the Chinese government under the [Military-Civil-Fusion Law](#). The same researchers often fail to declare their links to Chinese military units and think tanks. The relationship between the People's Liberation Army, academia, and its Academy of Military Medical Sciences mixes academic with state security obligations. Further, many scientists in academia and industry are People's Liberation Army officers and benefit from the China's national funding for scientific enterprises, specifically biotechnology and information [technology](#). The opaque relationship between scientists and the People's Liberation Army blurs the alleged Chinese biological pathogens research and development program, including genetically altered and [ethnically focused bioweapons](#). However, the Chinese government claims that it is in full compliance with the [Biological Weapons Convention](#) despite recent discoveries at a [point of entry](#) into the United States. In 2025, the Federal Bureau of Investigation charged two scientists, Yunqing Jian and Zunyong Liu, with conspiracy and smuggling after the Chinese Communist Party linked-pair were caught with samples of [Fusarium graminearum fungi](#) in their possession. *Fusarium graminearum* is a fungus responsible for billions of dollars in economic losses worldwide each year. Despite the pair's claims that the organism was for [research](#), *Fusarium graminearum* fungus has no peaceful purpose; import permits would have been refused. However, as a biological pathogen the fungus could be introduced in the wild, which would be a [violation](#) of the Biological Weapons Convention, especially when the likelihood of the fungi being [genetically modified](#) is considered. The danger inherent in genetically engineered fungus is any specific modification to do harm and the likelihood of enhanced mycotoxins, the ability to destroy plant protections, and any enhanced potential for human illness.

The pair have additional links to China that make their role in the United States and their research questionable. Jian is linked to Chinese defense authorities through Zhejiang University; Liu is involved in the Chinese Communist Party's "Hundred Talents Program." Both hold academic link-

ages to institutions in [China](#) that point to greater involvement in potential biological warfare programs, especially Liu's involvement with the People's Liberation Army at [Zhejiang University](#). Although their presence at the university was not well screened, it was also not unusual. The U.S. and China have long conducted an exchange of academics and researchers, but Chinese researchers have allegedly conducted extensive [thefts of Intellectual Property](#) from U.S. companies and universities, especially mRNA data, agricultural trade secrets, and pharmaceutical data from joint United States-China companies.

The academic institution where they claimed to be conducting research, the University of Michigan, has experienced other security incidents involving Chinese students that point to either espionage or clandestine surveillance. In 2024, five students were charged with conducting surveillance on a United States military [installation](#). The students were part of a joint exchange program with Shanghai Jiao Tong University in Shanghai, China, which was revealed to have extensive ties with the [People's Liberation Army](#).

The Federal Bureau of Investigation arrested another Chinese national on June 9, 2025 for smuggling [roundworm-related growth medium and plasmids](#) into the United States. The researcher, Chengxuan Han, a Chinese doctoral student at the College of Life Science and Technology at the Huazhong University of Science and Technology (HUST) in Wuhan, China, and a student at the University of Michigan also sent an additional four shipments of roundworms to the [university](#). Although news articles did not specify what type of roundworms were being smuggled, if they were nematodes, their economic damage to U.S. agriculture could have been high once a population was established. [Nematodes](#) are especially damaging to plant roots and can weaken them against fungal infections. Nematode damage can exceed 60 percent yield loss in a crop, and globally cause an estimated loss of \$157 billion a year. Han's attendance at the Huazhong University of Science and Technology (HUST) also links her to People's Liberation Army. [HUST](#) is co-administered by the State Administration of Science, Technology and Industry for National Defense (SASTIND),

the government agency responsible for equipping and researching for the People's Liberation Army. Three days before her arrival in the United States, Han wiped the contents of her electronic [device](#). Han's behavior and the smuggling violations point to China using academic connections to infiltrate organisms and develop surveillance necessary to commence biological warfare in the U.S.

The potential connection between at least three Chinese scholars (likely more) smuggling biological agents, the People's Liberation Army, and a pattern of disregarding permits appears deliberate and systematic. In addition, the lack of respect for scientific protocols, encrypted smuggling plans on What's App provide support to accusations of clandestine biological warfare research on US soil, against US targets. Han's smuggling roundworms and Jian and Liu's *Fusarium graminearum* samples pair well as a one-two biological attack against agricultural targets where worms weaken plants and the fungus spreads as a result. The potential threat from [bioengineered synthetic organisms](#) heightens the need for systems capable of detecting synthetic organisms. The possibility of a genetically modified outbreak of *Fusarium graminearum* fungi against the US wheat, barley and [corn crops](#) would have outsize impacts compared to the top three world grain producers because the US lacks a national [grain reserve](#) unlike China, Russia, and India. Chinese efforts to attack US agriculture go beyond the lab and into the area of technological and economic warfare.

The technological threat to the US agriculture comes from a three-part combination of cyberattacks against autonomous food distribution and packing systems; attacks against farm control systems and infrastructure; and the potential deployment of [Artificial Intelligence-designed novel biological agents](#) undetectable by current surveillance methods. As with the fungus strain that was smuggled into the United States, a genetically engineered, artificial intelligence-designed biological pathogen could wreak havoc in the U.S. monoculture against [genetically modified crops](#). U.S. agricultural sector components from the field to the factory and beyond are under threat for hostile cyber actors. Further, the threat that malignant artificial intelligence (AI) poses to agriculture is

significant, not only for the potential that it poses for attacks against sector components, but also for the informational disruption that an AI-enabled attacker could inflict on the reputation of the American food safety system. As AI enables enhanced [bio surveillance](#), sensors and analytics, it can also be used against the food system through models that identify the best time and conditions for maximum harm by pathogens and degraded detection capabilities. AI can also be used to reduce confidence in food networks by disseminating disinformation about food reliability and [false outbreak data](#). AI could also obscure real outbreaks and the results of surveillance.

The explosive expansion of AI-operated [autonomous tractors](#) in the agricultural sector makes them an obvious target for cyberattack. The loss of productivity that a cyberattack could create amongst the computer-driven tractors would be economically catastrophic with ripple effects across the agricultural supply chain. Some companies have reported attacks on their logistics and data through smart items linked through the Internet of Things, and the Federal Bureau of Investigation warns that agriculture cooperatives are susceptible to ransomware attacks during the [planting and harvesting season](#).

Attack timing would be the difference between an inconvenience and a crop loss for want of smart farm equipment shut down by cyberattacks. Ransomware attacks are also striking United States companies with increasing regularity. Meat processing and canning multinational companies have been attacked by Russian and criminal groups, and the delays imposed by those attacks show how information could be captured and denied to companies resulting in [supply chain delays](#). There is a wider potential for employment of ransomware and cyberattacks from Chinese state-sponsored cyber threat actors against logistics, power, water, and waste systems that affect agriculture directly or indirectly. The Chinese cyber actors demonstrated their ability to deeply imbed viruses like [Salt Typhoon](#) within computer systems. Imbedding and executing a cyberattack that delays the transfer of food, delivery of critical resources like fertilizer or water, or misrouting of agricultural sector resources could result in huge losses. If

exports cannot leave ports because of inoperable cranes or can't deliver products because recipients lack working bulk storage, losses would be high, as would be frustration.

Another area in which Chinese elements could possibly inflict damage against the United States agricultural sector is through more legal means: the ownership of United States farmland through shell corporations and majority company shares. China-based companies have gained majority ownership in multiple U.S. agricultural sector core businesses and production sectors. The China Policy Initiative labels it a “national security threat” due to Chinese company ownership of food production, agricultural research companies and their intellectual proprietary products. Chinese state-owned enterprises which once faced sanctions for their history of attempted industrial espionage have gained access to [special strains of seeds](#) through their company takeovers. These seeds are taken back to China, studied, replicated, and then sold by Chinese companies while the same are restricted in the United States. The loss of control over export products, exposure to corrupt practices, and indirect control of agricultural output through indirect Chinese Communist Party influence is a threat to agricultural sector viability. Farms that rely on a global supply chain for parts, fertilizer, and chemicals that [cannot be sourced in the U.S.](#) are forced to navigate Chinese export restrictions and [sanctions](#). Undercutting and weakening United States food security and the long-term health of the agricultural sector is one of the China's goals; China drafts food security laws as protective measures for its [domestic market](#) while ignoring or breaking those of the United States. China also gains soft power influ-

ence through [agricultural innovation stolen from the United States](#).

China's overall strategy for competition and disruption of U.S. economic systems includes smuggled plant pathogens, AI and cyber threats, physical dangers from supply chain contamination and market manipulation. The U.S. military is affected by the potential for asymmetrical warfare against the agricultural sector. Agricultural exports help fund the Department of War, and if crops are attacked or the systems that distribute food is disrupted, the U.S. military will have a role in the security of food sources and distribution. Most U.S. grocery stores have less than a three-day supply of food on the shelves due to [just in time logistics](#). Any significant impacts on trucking companies will also create [food shortages](#).

The threat against the U.S. agricultural sector and its exports is complex and the attacks being waged against it come in a variety of forms. Legacy programs and measures are increasingly being circumvented or ignored by the Chinese. The potential for a multi-sectorial attack on U.S. foodstuff production, transportation, and export is rising with a new generation of potential cyber and AI-driven threats. The added influence of trade barriers, intellectual propriety theft, and corruption threaten effective governance and coerce damaging concessions to a China that does not observe the laws or processes of other nations. The dangerous confluence of People's Liberation Army and Chinese Communist Party-linked academics, companies, and diplomacy point to a concerted effort to gain economic dominance in agricultural sectors vital to United States national security.