# Made In China: Strategic Risks to the U.S. Transportation Industry

NMFTA National Motor Freight Traffic Association, Inc. | CYBER


## Co-Author

Artie Crawford, CISSP, CISM
**NMFTA**



## Co-Author

Ben Wilkens, CISSP, CCSP, CISM
**NMFTA**

**Made in China: Strategic Risks to the U.S. Transportation Industry**

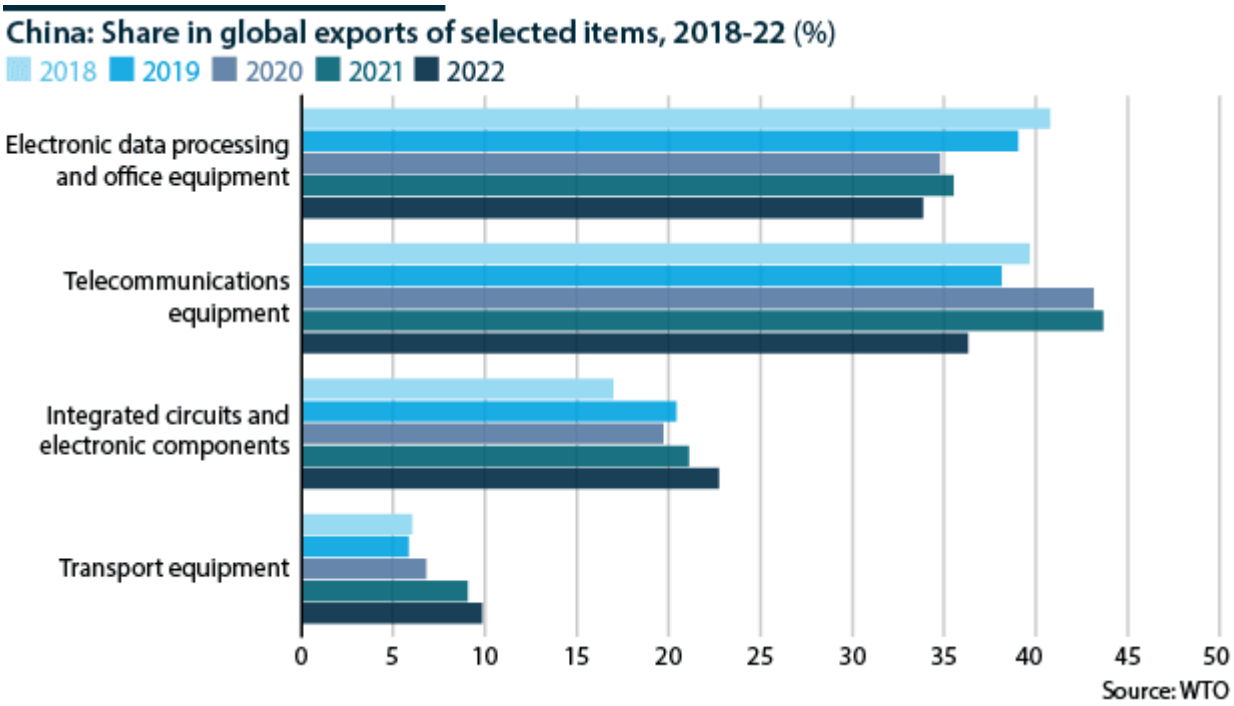
The rapid growth of Chinese technological dominance is reshaping global supply chains, national security policies, and the future of critical infrastructure. Between 2018 and 2022, China nearly doubled its share of global transport equipment exports and gained substantial control in sectors including shipping, telecommunications, computer hardware, and vehicle components.

One of the most significant findings for transportation was disclosed during an investigation led by the United States (U.S.) House Committee on Homeland Security in 2024. This investigation determined that there was covert communications hardware embedded in Chinese-made cranes deployed in U.S. ports which allowed for covert communications and data exfiltration to China. These findings are explored in detail in NMFTA's 2024 whitepaper: *Navigating the Impact of Chinese Infrastructure on U.S. Ports and the Supply Chain*.

For the U.S. trucking industry—central to national commerce and economic resilience—this trend has introduced both operational dependency and systemic risk.

The issue extends far beyond cost efficiency or competitive pricing. Hardware and devices manufactured by Chinese companies are increasingly connected, data-generating, and embedded in everyday operations. These components, many of which are produced by firms with ties to the Chinese government or military, present opportunities for espionage, supply chain disruption, and data exfiltration.

This whitepaper examines how Chinese strategy, technological reach, and regulatory control combine to create real and rising threats to transportation firms operating in the U.S.

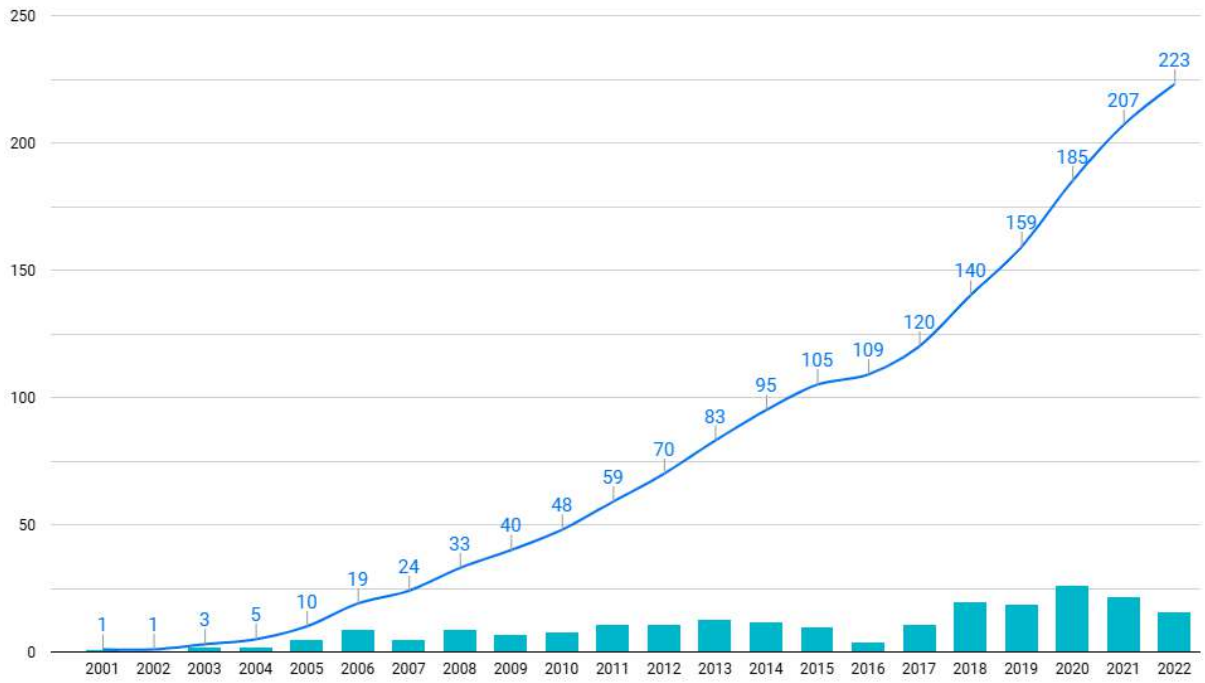



***Above:*** *Chart showing Chinese share of global exports in certain technology market. (Source)*

China's industrial policy—most notably outlined in its *Made in China 2025* plan—identifies 10 strategic sectors for global leadership, including transportation, aerospace, advanced materials, and energy. Achieving dominance in these sectors is not viewed as an end in itself but as a means to a broader political and military advantage.

This policy framework is backed by long-standing espionage and cyber campaigns. In 2020, former Federal Bureau of Investigation (FBI) Director Christopher Wray noted that the agency was initiating a counterintelligence case relating to China every 10 hours, while he stated that China "aimed to 'ransack' the intellectual property of Western companies." U.S. authorities documented at least 224 Chinese espionage incidents between 2001 and 2022, many of which targeted logistics, defense, and energy infrastructure. The FBI estimates annual economic losses from such activity exceed $600 billion. Crucially, Chinese law mandates that domestic companies provide the Chinese government (including intelligence agencies) access to systems, data, and infrastructure—even if the information originates overseas.

Taken together, these realities mean that Chinese-manufactured hardware often operates as a potential conduit for unauthorized surveillance, data theft, or disruption—especially when installed in critical supply chain systems.




***Above:*** *Total number of espionage cases linked to China by year, 2001–2022. (Source)*

The Chinese government has a long history of sponsoring advanced persistent threat (APTs) (including cyber-specific military units) who engage in direct action against U.S.-based critical infrastructure and networks.

- Salt Typhoon, one of the most well-known and prolific APTs from China, was reported in October 2024 to have conducted a widespread campaign targeting U.S. telecommunications infrastructure that began as early as 2019. The initial discovery indicated that AT&T, Verizon, T-Mobile, and Lumen Technologies were targeted as part of the campaign, a list that later expanded to also include Spectrum, Consolidated Communications, and Windstream. The campaign progressed by exploiting multiple privilege escalation vulnerabilities in Cisco-made Internet of Things (IoT) network devices such as routers, compromising over 1,000 devices globally over the course of the campaign. The objective of the campaign, while still under investigation, may have been to collect signals intelligence or to create a mechanism to disrupt telecommunication systems in the event of a geopolitical incident.

- Volt Typhoon another highly active APT sponsored by the Chinese state, was identified in August 2024 as being behind a series of attacks utilizing a vulnerability tracked as CVE-2024-39717 due to links to the group's known tactics, techniques and procedures. Volt Typhoon is a Chinese state-backed hacking group that is assessed to be mostly politically motivated, engaging in cyber espionage for the

Chinese government. Volt Typhoon usually operates by hijacking Small Office/Home Office (SOHO) routers and Virtual Private Network (VPNs) to launch attacks at target companies and organizations. The group uses these compromised routers and devices to feed malicious traffic into legitimate traffic to mask their entry and remain undetected.

- Evasive Panda, another active but lesser known APT, was implicated in February 2025 in a new network device attack campaign that utilizes a new SSH backdoor vulnerability. The attack format has been dubbed "ELF/Sshdinjector.A!tr" and is made up of a collection of malware injects designed to attack and hijack the Secure Shell (SSH)daemon on network appliances. Evasive Panda has been known to use similar techniques in related attacks since November 2024. The threat actor is known to deploy on a targeted device several binaries that act as a backdoor into the system.
- Raptor Train, a Chinese botnet was observed in September 2024 targeting critical infrastructure in the U.S. and was seized by the FBI. Since 2020, Raptor Train has targeted military, government, education, and telecommunications infrastructure IoT devices mainly in the U.S. The FBI connected the botnet to Flax Typhoon, another Chinese state-backed hacking group, and further identified that the botnet was operated through the Chinese IT company, Integrity Technology Group. In the time it was active, Raptor Train infected over 260,000 devices and at maximum infected 60,000 devices at one time.

The hardware risks facing trucking companies can be grouped into four interrelated technology domains. Each of these has been shown to contain vulnerabilities or active threat campaigns with links to Chinese state-backed actors.

TP-Link is a major manufacturer of routers and IoT hardware used widely in small and mid-sized enterprises. As of 2024, TP-Link held an estimated 65% U.S. market share in this category. In recent congressional and agency investigations, TP-Link has been singled out due to its product vulnerabilities and its legal obligation to cooperate with Chinese state intelligence services. While TP-Link represents SOHO routers and switches, these types of exploits have not been confined to the SOHO market as evidenced by attacks on Cisco enterprise-grade networking hardware.

Chinese APT groups—including Camaro Dragon and Salt Typhoon—have exploited TP-Link devices in known cyber campaigns. These attacks involved firmware implants, malware deployment, and remote access exploits. Although no formal backdoor has been

discovered in TP-Link's devices, the combination of remote access features, account-based management portals, and a history of compromise poses considerable risk.

A compromised router placed in a trucking depot, terminal, or dispatch office could be used as an access point into broader network environments, enabling attackers to move laterally into fleet management, logistics, or financial systems.

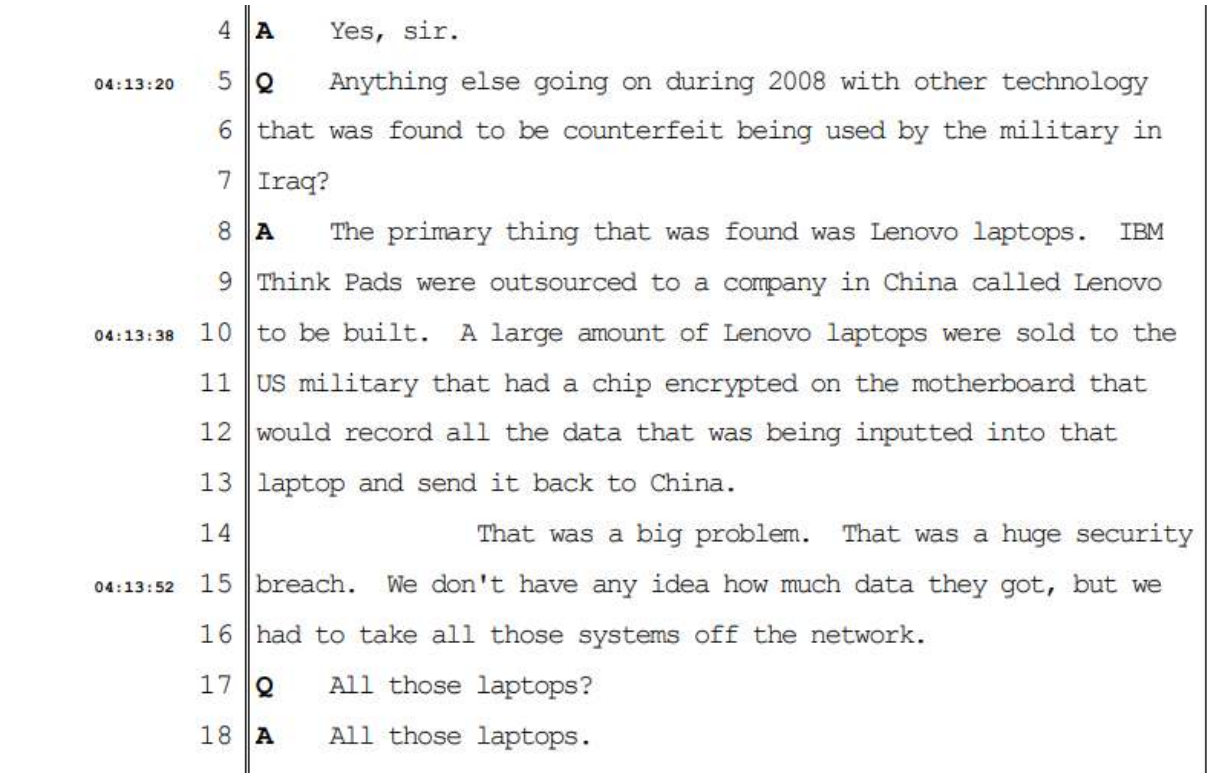
***A compromised router placed in a trucking depot, terminal, or dispatch office could be used as an access point into broader network environments, enabling attackers to move laterally into fleet management, logistics, or financial systems***

The integrity of computer hardware used in logistics operations has also been challenged by years of supply chain infiltration efforts. In 2018, Bloomberg reported that Chinese subcontractors for Supermicro embedded surveillance chips in server motherboards used by over 30 U.S. companies, including Amazon and Apple. Though denied by the affected firms, subsequent reviews by federal agencies have kept this issue under scrutiny.


***Above:*** *Graphic showing how Supermicro inserted surveillance tools into its computer chips. (Source)*

Earlier incidents support the plausibility of hardware-based threats. In 2010, Lenovo

laptops used by the U.S. military were found to be transmitting input data back to Chinese servers. These discoveries led to bans on Lenovo products in sensitive environments as early as 2006.



A Yes, sir.

04:13:20 Q Anything else going on during 2008 with other technology that was found to be counterfeit being used by the military in Iraq?

A The primary thing that was found was Lenovo laptops. IBM Think Pads were outsourced to a company in China called Lenovo

04:13:38 to be built. A large amount of Lenovo laptops were sold to the US military that had a chip encrypted on the motherboard that would record all the data that was being inputted into that laptop and send it back to China.

That was a big problem. That was a huge security

04:13:52 breach. We don't have any idea how much data they got, but we had to take all those systems off the network.

Q All those laptops?

A All those laptops.

***Above:*** *Excerpt from court testimony revealing backdoor communication devices embedded in Lenovo computers. (Source)*

While modern IT environments prioritize software-based defenses, these cases show that hardware-level compromise can enable undetectable surveillance or sabotage, with long-term consequences for organizations reliant on untrusted infrastructure.

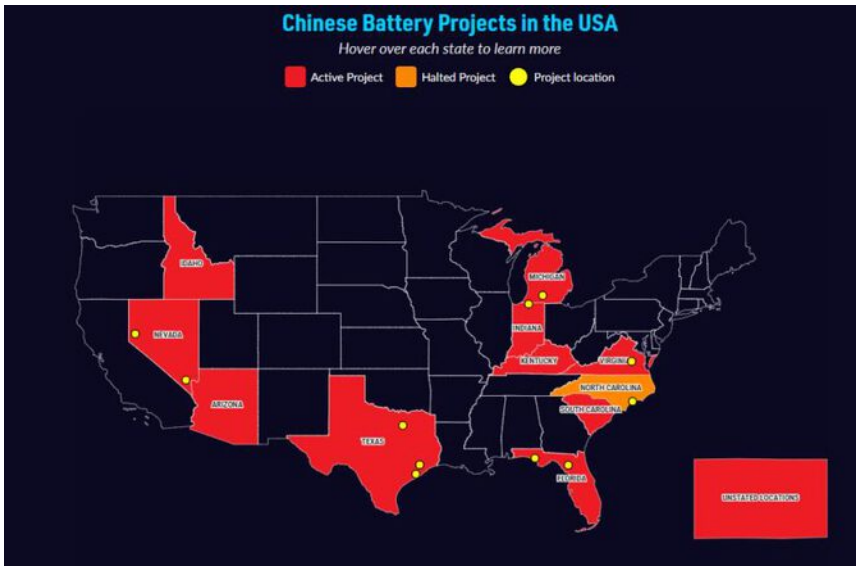
Video surveillance technologies, while essential to facility security, introduce additional vectors for cyber compromise and espionage. In 2022, the Federal Communications Commission (FCC) formally banned equipment from companies including ZTE, Huawei, Hikvision, and Dahua—two of China's largest producers of security cameras—when used in public safety, government, or critical infrastructure settings.
Despite these restrictions, such devices remain available in the commercial market and are often deployed in warehouses, vehicle cabs, and logistics facilities.

In 2024, the FBI reported that Hikvision and Dahua cameras were actively targeted by the remote access trojan (RAT) dubbed "HiatusRAT," which exploited known vulnerabilities to gain remote administrative access and control systems.

In its most basic form, a compromised video system could allow access to video and audio content which could reveal cargo contents, security processes, or company-specific logistics activity. These exposures are particularly relevant for trucking companies transporting high-value or time-sensitive goods. Compromised video systems could also serve as an initial entry point for wider network compromise, particularly in flat networks or networks with weak segmentation controls.

Contemporary Amperex Technology Co. Ltd. (CATL), based in China, is the world's largest supplier of lithium-ion Electric Vehicle (EV) batteries. It provides battery systems to manufacturers including Tesla, Ford, BMW, and Hyundai. In January 2025, the U.S. Department of Defense added CATL to its list of Chinese military companies, citing concerns over national security and critical infrastructure exposure.

In recent years, CATL has promoted the concept of the "electric intelligent vehicle," involving enhanced connectivity between batteries and cloud-based management platforms. These battery management systems (BMS), if compromised or misused, could be leveraged to extract geolocation data, performance diagnostics, and operational behaviors across an entire fleet.




***Above:*** *Map of facilities and plants where CATL products and technologies are in use. (Source)*

The threat is compounded by China's control over raw materials. Controlling over 90% of rare earth magnets and nearly the entire global supply of heavy rare earth metals, China dominates battery supply chains from resource extraction to final deployment.

The trucking industry sits at the intersection of critical infrastructure and commercial operations. As such, it presents an attractive target for espionage and influence campaigns aimed at disrupting supply chains or extracting strategic intelligence.

From an operational standpoint, vulnerable hardware introduces several risks:

- **Loss of proprietary or competitive data**: Telematics, routing information, performance metrics, and driver behavior data can be exfiltrated silently and aggregated to create a comprehensive picture of company operations.
- **Increased risk of cyber intrusion**: Hardware exploited by state-sponsored actors may offer attackers a durable presence within enterprise systems, bypassing traditional detection mechanisms.
- **Cascading supply chain disruption**: A compromise at one logistics provider can ripple through upstream and downstream partners, affecting customers, suppliers, and broader markets.
- **Regulatory and liability exposure**: Federal restrictions on certain technologies are expanding. Continued use of restricted hardware may lead to compliance violations or legal exposure.

For small and mid-sized fleets specifically, the appeal of affordable, commercially available Chinese hardware often outweighs security considerations. Yet these firms face the same strategic risks as large carriers—and may have fewer resources to respond to breaches or hardware recalls.

The risks posed by Chinese-made technologies are strategic in nature, systemic in scope, and particularly relevant for transportation and logistics companies embedded in the national supply chain. These are not isolated device issues but symptoms of a broader security model—one that exploits economic dependence and regulatory gaps to advance foreign state interests.

For the trucking industry, security cannot be separated from hardware. Every connected device is a potential node in a global intelligence campaign. Leadership must address this risk directly through updated procurement policies and strategies that include county-of-origin risk as a weighted factor in vendor selection, supply chain oversight, and a more holistic understanding of how adversarial technologies impact day-to-day operations.

Resilience begins not at the firewall, but at the point of purchase.