CHINESE TECHNOLOGY INFLUENCE IN U.S. SEAPORTS

THE MITRE CORPORATION

RESILIENT TRANSPORTATION & LOGISTICS

Defining the Problem

The proliferation of Chinese technology throughout U.S. seaports presents economic, transportation, and national security risks. A deeper understanding of these risks is required to inform decision making on how to address them as well as potential threats.

This paper proposes four notional courses of action on how to address risks posed by Chinese technology in U.S. seaports, summarizes findings that have been captured in this domain, and identifies actions for further discovery to capture and quantify the level of risk.

American seaports play a significant role in the U.S. and world economy. In 2018, $2.2 trillion in freight moved through U.S. ports, which in turn supported 30.7 million jobs and generated $378.1 billion in tax revenue for federal, state, and local authorities.[1] The American Association of Port Authorities reports that 15,000 jobs are created for every additional $1 billion in exports shipped out of U.S. seaports.[2] According to the U.S. Department of Transportation (USDOT), the nation's ports handled 41 percent (over $1.8 trillion) of U.S. international trade by value in 2021.[3] Today, over $6 billion in cargo is handled every week by U.S. ports, with an annual economic activity value of $5.4 trillion.[4]

Seaports also play a vital role in national defense. Several U.S. commercial seaports have been designated as Strategic Seaports by the Department of Defense (DOD). Strategic Seaports are intended for use in military deployments because of their large staging areas, connection to rail infrastructure, and ability to load non-containerized cargo. Strategic Seaports are expected to make facilities available to the military with as little as 48 hours' notice, and for extended periods of time, if necessary.

THIS PAPER PROPOSES FOUR NOTIONAL COURSES OF ACTION ON HOW TO ADDRESS RISKS POSED BY CHINESE TECHNOLOGY IN U.S. SEAPORTS, SUMMARIZES FINDINGS THAT HAVE BEEN CAPTURED IN THIS DOMAIN, AND IDENTIFIES ACTIONS FOR FURTHER DISCOVERY TO CAPTURE AND QUANTIFY THE LEVEL OF RISK.

There is growing concern about Chinese influence in U.S. seaports. The Chinese government has made a concerted effort to expand its influence into seaports around the world. Chinese companies own or operate terminals in 100 ports in 60 countries. China is also a major player in port technology, including cranes (Shanghai Zhenhua Heavy Industries Company Limited, or ZPMC) and logistics management systems (National Transportation and Logistics Public Information Platform, or LOGINK). ZPMC has a 70 percent global market share in container cranes. ZPMC cranes constitute 80 percent of cranes in U.S. ports, and they are present in 10 of the Strategic Seaports. Global adoption of LOGINK presents economic and national security risks to the U.S. Through LOGINK, the Chinese government has significant visibility into shipping and supply chains, providing opportunities to spot vulnerabilities and track shipments of U.S. military cargo on commercial freight.[5]

"WE ARE PARTICULARLY CONCERNED ABOUT TECHNOLOGY EMPLOYED BY CHINESE-MANUFACTURED CRANES OPERATING IN U.S. PORTS, WHICH SIGNIFICANTLY INCREASES THE CYBERSECURITY RISK TO BUSINESS OPERATIONS SYSTEMS AND TERMINAL INDUSTRIAL CONTROL SYSTEMS."

The federal government, particularly Congress, has expressed concern on the topic of Chinese influence in ports. A November 2022 bicameral letter to the President urged action "to halt the spread of LOGINK, a Chinese Communist Party (CCP) controlled digital platform for maritime data-sharing," and a subsequent letter in April 2023 from the House Committee on Homeland Security to the Secretary of Homeland Security expressed concern "about existing vulnerabilities at our nation's maritime ports. We are particularly concerned about technology employed by Chinese-manufactured cranes operating in U.S. ports, which significantly increases the cybersecurity risk to business operations systems and terminal industrial control systems."[6] In May 2023, the House Subcommittee on Transportation and Maritime Security held a hearing titled "Evaluating High-Risk Security Vulnerabilities at our Nation's Ports."[7]

Recent legislation addresses Chinese influence in ports. Section 3529 of the National Defense Authorization Act for Fiscal Year 2023, Study of Cybersecurity and National Security Threats Posed by Foreign Manufactured Cranes at United States Ports, commissions a study by the Maritime Administrator, in consultation with the Secretary of Homeland Security, the Secretary of Defense, and the Director of the Cybersecurity & Infrastructure Security Agency to "assess whether there are cybersecurity or national security threats posed by foreign manufactured cranes at United States ports." In March 2023, Rep. Michelle Steel (R-CA) and Sen. Tom Cotton (R-AR) introduced draft legislation in the Securing Maritime Data from Communist China Act of 2023, which calls for the ban of "the free, Chinese state-owned logistics platform LOGINK from being used by U.S. military or commercial interests at ports at home or abroad." Included in the proposed legislation:

- Ban all DOD usage and DOD contracts with entities using or sharing data with the platform.
- Require the President to prohibit entities in the United States from using or sharing data with LOGINK.
- Require the administration to report on the threat of LOGINK, including a report on U.S. port bans.
- Work with international partners to stop its use and prevent its inclusion in any economic/trade package.

Background on ZPMC Cranes and LOGINK

The topic of Chinese influence in U.S. seaports is expansive, but the two areas that capture the most attention, in both the press and the federal government, are Chinese-manufactured cranes (specifically ZPMC) and the logistics management system LOGINK.

ZPMC Cranes

Several news sources have published articles on the potential risks associated with ship-to-shore cranes made by the Chinese manufacturer ZPMC.[8,9] The specific concern highlighted is that the cranes contain sensors that can track

the details of containers that could potentially allow China to capture information about materiel being shipped in or out of the country, particularly in support of U.S. military operations. In September 2021, news reports indicated that FBI counterintelligence agents searched a ZPMC crane delivery vessel, Zhen Hua 24, in Baltimore harbor.[8] The vessel was delivering four new cranes to Ports America Chesapeake Bay. According to the report, "The agents were said by informed sources to have uncovered intelligence-gathering equipment on the ship during the search."

National Transportation and Logistics Public Information Platform

LOGINK is a logistics management system that facilitates the exchange of documents and data and provides information related to cargo location and price quotes from freight carriers. In April 2022, the International Port Community Systems Association partnered with LOGINK to develop the Network of Trusted Networks that would give China access to data and information across 70 ports and 10 airports and set data standards for the Association of Southeast Asian Nations region. LOGINK has global reach and, even with a potential U.S. prohibition, has presence in several countries. Any effort to adopt alternatives to LOGINK will require a coordinated effort with multiple nations.

Initial Analytic Findings

MITRE has developed several analytical products regarding Chinese influence in ports, with a focus on technical analysis of seaport systems.

Threat-informed cyber resiliency analysis of crane operations

In 2020, a research effort was conducted that examined the cyber resilience of crane operations with a focus on foreign-manufactured cranes. The analysis leveraged MITRE's understanding of adversarial cyber behavior to identify feasible cyberattack scenarios that could remotely access and disrupt crane operations. These scenarios were used to identify key risks and propose mitigations to improve the security and resilience of the cranes. The key findings of this analysis were:

- The crane manufacturer has broad access and the opportunity to add or manipulate components throughout a crane's manufacturing, shipment, and onsite commissioning process.
- There is a need to better control and monitor access to the cranes (e.g., network segmentation, file transfer, remote access).
- Ports need to be better prepared to recover and reconstitute key crane control systems, including through the availability of spares and backups.

Business and economic analysis of Shanghai Zhenhua Heavy Industries Company

An analysis of ZPMC's global footprint, corporate partnerships, and operational locations was conducted. The analysis also included a deeper assessment of ZPMC's presence in the U.S. and Latin America. The key findings of this analysis were:

- ZPMC uses its lack of corporate structure transparency and its access to the People's Republic of China to underbid contracts, control the flow of marketing information, and shuffle employees across the region and across multiple port projects.
- ZPMC is a vital player in China's Belt and Road Initiative (BRI) and has likely leveraged its cranes and technology in all BRI ports and many U.S. ports, posing a risk of market dominance and counter-intelligence concerns.
- ZPMC presents national security concerns due to its relationship with parent company China Communications Construction Company, partnership with Huawei, and potential technology vulnerabilities built into cranes that could allow unauthorized access.

Identifying and Analyzing Courses of Action

Given the potential risk posed by the spread of Chinese technology in U.S. seaports, there is a need for data-driven decision making in adopting courses of action (COAs). To shape the decision space and develop solutions, four notional COAs are presented.

COA 0

Let Chinese influence continue without restriction. This COA allows market forces to drive capability investment in U.S. seaports. This is the status quo COA option.

COA 1

Ensure Chinese technology is trusted and secure. This COA assumes that seaports will continue to use ZPMC cranes and LOGINK as a logistics management system but requires exploration, assessment, and monitoring of U.S. risk. In parallel, risk mitigation measures would be funded and implemented. A program could be established to oversee the analysis and identification of risks, and to oversee the implementation of mitigation measures.

COA 2

Stop further proliferation of Chinese technology in U.S. seaports. This COA institutes a ban on not only ZPMC cranes and use of LOGINK, but also other Chinese technologies that pose similar risks. For Chinese technology that is currently in use, exploration, assessment, and monitoring of U.S. risk would still be required. Identified risks would need to be mitigated.

COA 3

Remove Chinese technology from all U.S. seaports.

As the U.S. seeks to reduce Chinese influence in seaports, there is a need for mission-driven analysis to assess risks and inform decisions. The table below provides a current state.

COURSE OF ACTION	INITIAL ANALYTIC FINDINGS	ADDITIONAL ANALYSIS NEEDED TO INFORM DECISIONS
COA 0 Let Chinese influence continue without restriction.	▪ Chinese technology will likely continue to proliferate in the U.S. ▪ ZPMC presence in U.S. seaports has been identified, including in critical Strategic Seaports.	▪ Assess the risk of proliferation of Chinese technology at U.S. seaports (how many seaports, breadth and depth of technology deployment).
COA 1 Ensure Chinese technology is trusted and secure.	▪ MITRE's cyber vulnerability analysis of foreign-manufactured cranes has not directly identified specific threats; however, there is an opportunity to explore this area further. There are several potential vulnerability areas that have been highlighted, including manufacturing, transportation, and installation of cranes in U.S. seaports.	▪ Conduct a comprehensive risk assessment of ZPMC cranes and LOGINK (capture true vulnerabilities of cranes, vulnerability of U.S. data in LOGINK). ▪ Develop mitigation measures to address principal risks. Engage with alternative manufacturers and suppliers of cranes and related equipment from various countries to reduce dependency on Chinese manufacturers. Support the implementation of trade policies that promote fair competition and prevent market dominance by a single foreign supplier. ▪ Deploy demonstrable capability to prove mitigation approaches. Invest in R&D to develop new technologies and improve existing ones in the crane and port equipment industry. ▪ Provide constant risk monitoring and assessment. Develop a platform to continuously monitor and assess supply chain risks related to the reliance on Chinese technology and develop contingency plans to address potential disruptions.

COURSE OF ACTION	INITIAL ANALYTIC FINDINGS	ADDITIONAL ANALYSIS NEEDED TO INFORM DECISIONS
COA 2 Stop further proliferation of Chinese technology in U.S. seaports.	▪ Alternative solutions for cranes and logistics management systems have been identified. Initial analysis of these alternatives shows they provide comparable capability to Chinese counterparts.	▪ Identify viable non-Chinese crane and logistics management systems solutions. Are there alternative suppliers available from other countries or regions? What steps has the U.S. taken to diversify the supply chain and reduce reliance on Chinese technology at U.S. seaports? Are there other suppliers or technologies that could serve as alternatives in case of disruption? Support investment in the modernization and expansion of port infrastructure to accommodate a diverse range of crane systems from various suppliers. ▪ Assess opportunities to create incentives for adoption of non-Chinese technology solutions. Are there any existing or potential trade restrictions, tariffs, or sanctions that could impact the import of non-Chinese technology? Are there any additional costs, such as transportation, tariffs, or maintenance, that could impact the total cost of ownership? Encourage and support domestic manufacturing of cranes and related equipment through incentives, grants, and tax breaks. ▪ Address the broader implications of adopting non-Chinese solutions, including the global impact. What are the potential geopolitical risks and trade tensions between the U.S. and China on this issue? How could these impact our supply chain?
COA 3 Remove Chinese technology from all U.S. seaports.	▪ There are several commercial alternatives for cranes and logistics management systems from non-Chinese suppliers that have positioned their products to be trusted alternatives. Initial analysis of these alternatives shows they provide comparable capability to Chinese counterparts.	▪ Assess the cost and implications of removing all Chinese technology at U.S. seaports. ▪ Same considerations as COA 2.

Based on the current state, MITRE recommends the near-term parallel execution of several specific additional analyses to directly inform decision making and COA determination:

- **Deeper analysis of Chinese presence in U.S. seaports:** There is an opportunity to develop a comprehensive baseline to understand the footprint, dependencies, supply chains, risks, and threats associated with Chinese-built cranes. This foundational baseline will provide a deeper understanding of the size and scope of Chinese presence and will serve to inform course of action decision making. This baseline will also allow for a prioritized methodology and strategy for developing risk mitigation measures. Specific areas of analysis include: develop a complete inventory of ZPMC cranes in U.S. and international seaports, identify other Chinese equipment installed in seaports, and capture future U.S. seaport investment in Chinese equipment.
- **Cyber vulnerability analysis of ZPMC cranes:** Although there is no concrete evidence that ZPMC cranes can be exploited, this issue requires further assessment. Part of this effort should include fostering partnerships with ports to: identify and implement risk mitigation measures; identify and address components of the cranes that have a dependency on Chinese products and components; minimize opportunities for China to remotely communicate or access the cranes; and ensure the resilience of crane operations, including having adequate spares and sufficient best practices for crane restoration.
- **Analysis of trusted alternatives to LOGINK:** There is a need to conduct an analysis of alternatives to LOGINK, examining how comparable capability can be achieved, ensuring the trustworthiness of alternative solutions, and identifying the international user community that would need to be included in adopting an alternative.

Conclusion

Chinese technology influence in U.S. seaports is a recognized concern of the U.S. government, with proposed legislation designed to counter this influence and several initiatives designed to better understand the risk and develop alternatives. DOD, DHS, and USDOT have initiatives to assess risk, spread awareness throughout the maritime community, and pursue non-Chinese technology alternatives.

Most published efforts are focused on highlighting the risk without accompanying releasable risk assessments and funded efforts to incentivize and develop alternatives. This paper highlights three specific focus areas – broader technology risk assessment, cyber vulnerability of ZPMC cranes, and LOGINK.

Using these focus areas as starting point, there are several courses of action presented that identify initial analytic findings and present additional areas of analysis that can inform decision making at all levels of the U.S. government and maritime commercial entities.

References

1. American Society of Civil Engineers, 2021 Report Card for America's Infrastructure, Port Infrastructure | ASCE's 2021 Infrastructure Report Card
2. American Association of Port Authorities, Exports, Jobs and Economic Growth, https://www.aapa-ports.org/unifying/landing.aspx?ItemNumber=21705&navItemNumber=20808
3. 2023 Port Performance Freight Statistics Program: Annual Report to Congress
4. America's Air, Sea, and Land Ports Require Investment to be Globally Competitive, Wilson Center, March 2, 2023, https://www.wilsoncenter.org/article/americas-air-sea-and-land-ports-require-investment-be-globally-competitive
5. U.S.-China Economic and Security Review Commission, LOGINK: Risks from China's Promotion of a Global Logistics Management Platform, LOGINK: Risks from China's Promotion of a Global Logistics Management Platform | U.S.-CHINA | ECONOMIC and SECURITY REVIEW COMMISSION (uscc.gov)
6. United States House Committee on Homeland Security. Letter to Secretary Alejandro Mayorkas on Existing Vulnerabilities at Nation's Maritime Ports Due to Chinese-Made Cranes. April 3, 2023.
7. Testimony was provided by Eric Goldstein, Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency (CISA); John "Neal" Latta, Assistant Administrator for Enrollment Services and Vetting Programs, Transportation Security Administration (TSA); and Rear Admiral Wayne R. Arguin, Jr., Assistant Commandant for Prevention Policy, United States Coast Guard.
8. Inside the Ring: Biden goes easy on China at U.N., The Washington Times, September 21, 2021, Inside the Ring: Biden goes easy on China at U.N. - Washington Times
9. Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools, The Wall Street Journal, March 5, 2023, Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools - WSJ

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

For more information, contact:
resilienttransport@mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®