MARITIME ADMINISTRATION

STUDY OF CYBERSECURITY AND NATIONAL SECURITY THREATS POTENTIALLY POSED BY FOREIGN MANUFACTURED CRANES AT UNITED STATES PORTS

Section 3529 of the 2023 National Defense Authorization Act directed the Maritime Administrator, in consultation with the Secretary of Homeland Security, the Secretary of Defense, and the Director of the Cybersecurity and Infrastructure Security Agency, to conduct a study to assess whether there are cybersecurity or national security threats posed by foreign manufactured cranes at United States ports.

The U.S. Department of Transportation's Maritime Administration (MARAD) has hosted a series of classified and unclassified information gathering discussions involving Federal representatives of the Departments of Defense, Homeland Security (including the U.S. Coast Guard and the Cybersecurity and Infrastructure Security Agency), State, and Commerce, as well as the Federal Bureau of Investigation and other members of the Intelligence Community on the potential cybersecurity and national security threats potentially posed by foreign manufactured cranes in U.S. ports. MARAD also led discussions with several maritime industry stakeholders and allied foreign maritime security agencies on this subject. MARAD notes President Biden's Executive Order (EO) of February 21, 2024, (EO 14116), *Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States.* This EO will bolster the security of U.S. ports by expanding the U.S. Coast Guard's authority to regulate maritime cybersecurity. Subsequently, the U.S. Coast Guard issued U.S. Coast Guard Maritime Security Directive 105-4 titled *Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies.*

ZPMC (Shanghai Zhenhua Heavy Industries Company Limited) maintains the largest share, by sales revenue, of the ship-to-shore crane market worldwide. By design, these cranes may, depending on their individual configurations, be controlled, serviced, and programmed from remote locations, and those features potentially leave them open to exploitation. The company provides products and services to approximately 300 harbors in 103 countries. Since at least 2007, they have maintained an estimated 70 to 80 percent of the global port crane market and an estimated 70 percent of the world's post-Panamax container crane market. ZPMC entered the U.S. market in 1994 and currently has an estimated 209 cranes of all types operating in at least 23 ports. As such, this study is focused on ZPMC cranes. ZPMC has the following U.S. subsidiaries: ZPMC North American in Long Beach, CA and its subsidiary, ZPMC USA in Colts Neck Township, NJ.

MARAD lacks both the legal authorities and organic expertise to conduct on-site technical assessments of the potential threats posed by foreign manufactured cranes. This study, therefore, relies heavily on analysis that has been published by other agencies and the results of recent physical assessments of foreign manufactured cranes at U.S. ports executed by the U.S. Coast Guard and shared with MARAD.

To date, U.S. Coast Guard teams have conducted threat 'hunts' and vulnerability assessments on over 92 ZPMC cranes at U.S. ports. These missions included ports both within and outside the continental U.S., as well as several strategic seaports within the U.S. National Port Readiness Network, and near critical economic centers. The Coast Guard found that throughout the Marine Transportation System (MTS), technical implementation of crane cybersecurity measures varies between ports due to differences in operational technology (OT) and other infrastructure. These Coast Guard engagements did not identify unique vulnerabilities or exploitations specific to foreign STS cranes. Instead, they found that potential vulnerabilities present in foreign cranes reflect weaknesses present across other OT systems and implementations including terminal operating systems, positioning systems, and automated cargo tracking equipment. Most notably, many MTS OT systems remain exposed to cyberattack due to poor cyber hygiene (e.g., poor password policies, lack of network segmentation, unpatched systems, and exposed services). Previous Coast Guard engagements determined that, although foreign cranes represent a potential vulnerability, these risks were not determined to substantially outweigh concerns from other OT exposure. Encouraging improved OT cyber hygiene throughout the MTS would help eliminate risks to both foreign cranes and broader port infrastructure.

U.S. Maritime Advisory 2024-002 (*Foreign Adversarial Technological, Physical, and Cyber Influence – Worldwide*), which is available at https://www.maritime.dot.gov/msci-advisories, provides references and recommendations addressing foreign manufactured port cranes and other maritime port infrastructure concerns. In addition, the U.S. Coast Guard has shared with MARAD that they are working on additional messaging and direct engagement with crane owners/operators to address potential vulnerabilities, mitigations, and security controls focused on the following:

- Network Segmentation
- Software Updates
- Vulnerability Scanning
- Network Monitoring
- Privileged Account Management
- Recovery

Conclusion

In reviewing all available U.S. government reports on this subject and during each of the information gathering discussions that MARAD participated in over the course of this study, all participants were repeatedly asked if anyone was aware of any case of a foreign manufactured crane at a U.S. port being actively exploited. The answer was consistently "no." It is clear, however, that as with any other critical complex cyber-physical systems, foreign manufactured port cranes should be assessed for potential cybersecurity or other national security threats, they should be actively monitored whenever possible, and that interagency collaboration on this issue should continue.