The Maritime Executive
INTELLECTUAL CAPITAL FOR LEADERS

Report: Time to Invest in Cybersecurity for U.S. Sealift Forces

iStock

Published Mar 31, 2025 7:13 PM by **The Maritime Executive**

A panel of senior cyber experts has called for more investment in maritime cybersecurity in order to ensure American military mobility in wartime. Most cyber analyses focus on the economic and commercial impact of cyber meddling, but this study is squarely focused on defense - specifically on defense against China, America's most sophisticated adversary in the cyber domain.

In its 2024 report, the U.S. intelligence community predicted that China could use "aggressive cyber operations against U.S. critical infrastructure and military assets" and attempt to "interfere with the deployment of U.S. forces." China's hackers have also proven themselves capable of penetrating utilities, videocameras, routers and the deep infrastructure of American telecom companies - giving Beijing a birds-eye view of American logistics, including military logistics.

"The nation can no longer afford to waste time debating the immediacy of the threat. Washington must identify and resource solutions now," wrote Annie Fixler, RADM Mark Montgomery (USN, ret'd) and Rory lane for the Cybersecurity Solarium Commission (CSC 2.0).

The threats affect all modes of transport - rail, road, air and maritime. Sealift may be the most important link in the chain, as it carries 90 percent of the cargo when America goes to war overseas. It is also vulnerable, as U.S. sealift capacity is already strained, reliant on aging tonnage and uncertain mariner availability. "The nation's lack of excess sealift capacity means that the U.S. military's ability to mobilize forces could be severely degraded by any cyber or physical incident," the panel warned.

The authors singled out known vulnerabilities in Chinese port equipment, including unexploited security vulnerabilities in cranes built by ZPMC; likely logistics spying activity in China's free-to-use

LOGINK container tracking platform; and low performance of a Chinese-made cargo inspection device that is marketed for detecting nuclear materials.

The Biden administration gave the Coast Guard more authority to directly regulate port and maritime cybersecurity, and USCG captains of the port are following up with stakeholders. However, "the Coast Guard has no funding specifically designated for work with the private sector to improve the cyber resiliency of America’s port infrastructure," the panel warned. It remains to be seen if the Trump administration will prioritize cyber vulnerabilities in its next budget.