Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity

By William Loomis, Virpratap Vikram Singh, Dr. Gary C. Kessler, and Dr. Xavier Bellekens

The Maritime Transportation Sector (MTS) is critically important to the United States:

- The global economy depends on the efficient operation of the maritime transportation sector (MTS). No global supply chain is independent of the maritime transportation sector, and most are existentially dependent.
- The critical role that the MTS plays goes beyond manufacturing supply chains; ships and offshore sites, refinement, and shipping are integral to the health of vital global energy systems.
- The United States' maritime infrastructure is key to the United States' ability to project and sustain power abroad.

Yet, recent history shows that the MTS is increasingly vulnerable to cyber threats. Like other critical infrastructure sectors, drive for operational efficiency and profit have lead to intense investments in new technology and remote capabilities across the MTS. This spread of technology has led to a shift toward an even more complex systems environment. As users and operators continue to stack new technology on top of existing legacy systems, the MTS is confronted with a familiar problem; complexity begets insecurity. This focus on layering on new technology to increase operational efficiency and the diversification and differentiation of systems and players in the MTS has created a wide and diverse attack surface – and a corresponding recent 400% increase in cyberattacks targeting maritime systems and a 900% increase in attacks targeting maritime and maritime energy OT technologies.

To address this problem, the Atlantic Council, in partnership with Idaho National Lab, has developed a strategic engagement plan and report on maritime and global energy cybersecurity predicated on key points of leverage in the MTS. Two points in this analysis underpin the report's recommendations

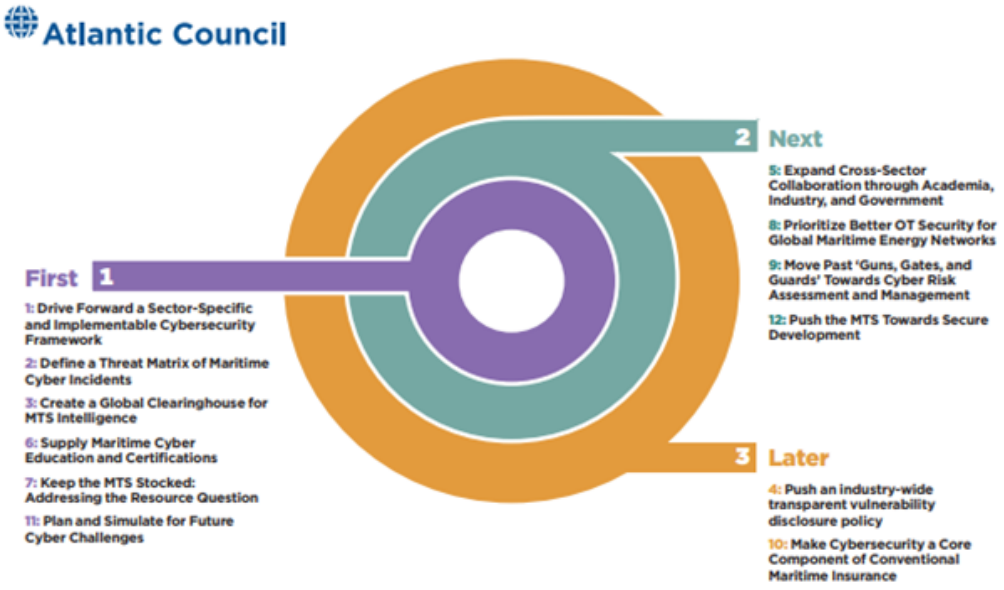
First, it is imperative to recognize that the MTS is not monolithic. Instead, it is a "system of systems" composed of ships and ports, but also shipping lines, refineries, ship builders, intermodal transport operators, maritime administrators, and more. Influencing the MTS toward better cybersecurity outcomes must approach these systems as modular parts of an important while. This approach should be reflected in every action taken to secure the MTS and frames the substance and recommendations of the report.

Second, the MTS and particularly energy providers and transport, is critically reliant on a differentiated but interconnected set of international players spread throughout the public and private sectors. A single port may house operators from hundreds of different companies, including numerous third-party contractors. All these actors must take steps in some coordination to better secure their system (the port). One lagging entity can undermine a host of

neighboring successes. The report identifies important players and relationships and discusses their interactive roles in greater detail.

The US government took an important first step in December 2020 with the release of the National Maritime Cybersecurity Plan (NMCP). The plan aims to “buy down the potential catastrophic risks to national security and economic prosperity caused by MTS operators’ increasing reliance on IT and OT, while still promoting maritime commerce efficiency and reliability.” However, like any strategic plan, it lacks tactical specificity on implementing the goals to actualize these principles and deliver a coherent strategy and demands increased focus on critical MTS applications like the global energy system.

To drive better cybersecurity outcomes and more effectively mitigate risk in the MTS and global energy networks, this report builds on existing processes and programs like the DoE CyTRICS program to broaden and deepen risk management tools and cybersecurity efforts across the MTS. This report lays out twelve recommendations in three groups to increase systemic cybersecurity in the MTS with allies and partners. To better understand their prioritization, the recommendations have been broken into three categories - **first**, **next**, and **later** - to sort recommendations based on the maturity of the point of leverage they are built on and the corresponding actors tasked with their implementation.



The Cyber Statecraft Initiative

The Cyber Statecraft Initiative works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

Learn more at: www.atlanticcouncil.org/cyberstatecraft/