Testimony of

Dr. Gary C. Kessler
Non-Resident Senior Fellow
Atlantic Council

Before the
United States House of Representatives
Committee on Transportation and Infrastructure

The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure

04 November 2021

Chairman DeFazio, Ranking Member Graves, and members and staff of the committee – thank you for the invitation to provide testimony to the committee. I am a Non-Resident Senior Fellow at the Atlantic Council and one of the authors of the Council's report, *Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity*.[1] I have spent my professional career since the 1970s in the information technology and information security fields, am a retired professor of cybersecurity, and the co-author of a book on maritime cybersecurity.[2] I am also a Principal Consultant at Fathom5 working on cyber issues related to maritime operational technology (OT) testbeds, am a visiting faculty member at the U.S. Coast Guard Academy, and hold a national office in the U.S. Coast Guard Auxiliary's Cybersecurity Division.

United States Dependence Upon Maritime Transportation

Most people in the United States do not think of our country as a maritime nation. They view our nation's waterways as a venue for recreation or a vacation get-away, a source of food, or the home of 12 million recreational boats and pleasure craft. Our citizens, in large part, neither know about nor appreciate our reliance upon the maritime transportation system for our very way of life.

Our report addresses that dependence in some very tangible ways – the maritime transportation system (MTS) contributes $5.4 trillion to the U.S. economy, representing about

[1] Loomis, W., Singh, V.V., Kessler, G.C., & Bellekens, X. (2021, October). *RAISING THE COLORS: Signaling for Cooperation on Maritime Cybersecurity*. Cyber Statecraft Initiative, Scowcroft Center for Strategy and Security, Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2021/10/Raising-the-colors-Signaling-for-cooperation-on-maritime-cybersecurity.pdf

[2] Kessler, G.C. and Shepard, S.D. (2020, September). *Maritime Cybersecurity: A Guide for Leaders and Managers*. Amazon Kindle Direct Publishing, http://www.maritimecybersecuritybook.com

25% of our country's gross domestic product, as well as 30 million jobs.[3] Roughly 80% of global trade and nearly two-thirds of the world's total petroleum and other liquid energy supply is carried by ship. In the U.S., approximately 90% of our imports/exports are by ship, emphasizing the point that no global supply chain is independent of maritime transport, and most, in fact, are existentially dependent upon it.

Consider the disruption to the global supply chain caused when the cargo ship EVER GIVEN was stuck in the Suez Canal in March of this year, costing the global trading community nearly $9 billion each day. Although the blockage only lasted for six days, the 20,000-container vessel did not leave the Canal area for nearly four months pending a dispute with the Suez Canal Authority.[4] Much closer to home, consider the current disruption to the U.S. supply chain due to the backlog at the Ports of Long Beach and Los Angeles, the entry way for nearly 40% of U.S. imports. There are myriad causes for the backlog but the bottom-line impact is higher costs, delays in getting goods to market, and global disruption of many product supply chains.[5]

In addition, the ability to move military personnel and matériel – a capability known as *sealift* – combined with the global presence of U.S. Navy warships and U.S. Coast Guard cutters are the basis of U.S. military power projection around the world. These latter capabilities have

[3] United States Coast Guard (USCG). (2021, August). *Cyber Strategic Outlook: The United States Coast Guard's Vision To Protect and Operate in Cyberspace*. https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf

[4] Chellel, K., Campbell, M., & Ha, K.O. (2021, June 24). Six Days in Suez: The Inside Story of the Ship That Broke Global Trade. *Bloomberg Businessweek*. https://www.bloomberg.com/news/features/2021-06-24/how-the-billion-dollar-ever-given-cargo-ship-got-stuck-in-the-suez-canal

[5] Caplan, J. (2021, October 14). Port of Long Beach Director Warns Cargo Backlog is 'National Crisis.' *Breitbart*. https://www.breitbart.com/politics/2021/10/14/port-of-long-beach-director-warns-cargo-backlog-is-national-crisis/; Meeks, A., Isidore, C., & Yurkevich, V. (2021, October 19). North America's Biggest Container Port Faces Record Backlog. *CNN Business*. https://www.cnn.com/2021/10/18/business/container-port-record-backlog/

served the nation in time of war, provided a capability to protect shipping routes, and acted as a deterrence to ensure peace.[6]

The MTS is not Monolithic

While we often talk about the MTS as if it was a single, monolithic entity, it is actually a system of systems, representing ships, ports, shipping lines, inland waterways, and intermodal transfers.[7] All of these systems operate independently, yet are co-dependent and inextricably intertwined. The life cycle of a ship, for example, intersects with the lifecycle of a port and is only a part of the life cycle of a shipping line. The life cycle of people and cargo within the MTS intersect with a ship's voyage and transit through ports, intermodal transfers, and inland waterways. The cybersecurity threats to the MTS are similar to threats everywhere else in information space, but are unique to our industry and way of life.

Ports are one of the primary focus points of our report. Intellectual property (IP) theft related to port operations and construction can yield very valuable information to competitors and adversaries, alike. The deliberate installation of a Stuxnet-type of vulnerability[8] – i.e., software that can attack and destroy hardware – into a vessel or vessel component during construction could provide the basis for a ransomware or other cyber attack years later.

[6] Harris, S., & Fasching, Sr., J. (2020, May 21). Sealift: The Foundation of U.S. Military Power Projection. *LMI blog*. https://www.lmi.org/blog/sealift-foundation-us-military-power-projection; Masters, J. (2019, August 19). Sea Power: The U.S. Navy and Foreign Policy. *Council on Foreign Relations*. https://www.cfr.org/backgrounder/sea-power-us-navy-and-foreign-policy; Schuler, M. (2021, October 21). New USTRANSCOM Commander is 'Laser-Focused' on Buying Secondhand Ships to Boost Military's Surge Sealift. *gCaptain*. https://gcaptain.com/new-ustranscom-commander-is-laser-focused-on-buying-secondhand-ships-to-boost-militarys-surge-sealift/

[7] Kessler & Shepard, 2020; Mansouri, M., Gorod, A., Wakeman, T.H., & Sauser, B. (2009). A Systems Approach to Governance in Maritime Transportation System of Systems. *Proceedings of the IEEE International Conference on System of Systems Engineering (SoSE)*. Albuquerque, NM.

[8] Kushner, D. (2013, February 26). The Real Story of Stuxnet. *IEEE Spectrum*. https://spectrum.ieee.org/the-real-story-of-stuxnet

The adage, "If you've seen one port, you've seen one port"[9] is well-known in the maritime industry. All ports are unique in terms of their ownership and management, the mix of civilian and military vessels and operations, the interconnection of information and communication technology (ICT) systems by port operators and tenants, personnel management, intermodal connections, volume of traffic, cargo, passengers, etc. While all ports have the same general functions, each is unique.[10]

Ships, another focus point of the report, are floating networks. There are multiple operational networks onboard a vessel, including passenger/entertainment networks, navigation systems, satellite communications, ballast control, engineering control, propulsion and steering, cargo management, and more. Global Positioning System (GPS) and Automatic Identification System (AIS) communications are essential to positioning, navigation, timing, and situational awareness, and are both susceptible to jamming and spoofing.

Shipping lines are a business like any other business; they just happen to own and operate ships. Thus, they have the same potential information security vulnerabilities that any business does, from finance and logistics to communications and cargo/passenger management. There is a significant amount of third-party software and systems employed by shipping lines, so the business is not even in charge of all of their own computers and networks.

[9] Keefe, J. (2019, March 6). Port Security: If You've Seen One Port, You've Seen One Port. *Maritime Logistics Professional*. https://www.maritimeprofessional.com/news/port-security-seen-port-seen-343481

[10] Polemi, N. (2018). *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*. Amsterdam: Elsevier.

Remember the havoc in companies and governmental agencies around the world with the attack on SolarWinds less than a year ago.[11]

Intermodal transfers are where the MTS touch every other form of transportation, including trucking, rail, and aviation. Even if the port, ship, and shipping line have outstanding security, a cyberfraud or cyberattack might still be perpetuated via a compromised trading partner.

People are often the largest security attack vector, both in physical space and cyberspace. People are our passengers, our workers, our adversaries, our clients, and our colleagues. We need to vet the people that are engaged in any way with the MTS, obviously at different levels of access to information and systems. Cyberattacks on the personnel or passport control systems, for example, can render the ordinary security checks worthless, not to mention the enormous amount of personally identifiable information (PII) and financial information in the personnel and passenger databases.

Cyber security in the maritime sector is a very broad endeavor. Regulation and administrative controls apply very differently to each of the sector's sub-systems.

Technology Advances in the MTS

Technology in the MTS and cyber attacks go to the heart of why we at the Atlantic Council issued our report. The beginning of the modern computer age dates back only about 75 years. Modern digital communications technologies date back to the 1960s. The beginning of the global Internet started slowly just more than 50 years ago but, once commercialized a mere 30

[11] Herr, T., Loomis, W., Schroeder, E., Scott, S., Handler, S., & Zuo, T. (2021, March). *Broken Trust: Lessons from Sunburst*. Cyber Statecraft Initiative, Scowcroft Center for Strategy and Security, Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2021/03/BROKEN-TRUST.pdf

years ago, was adopted more rapidly than any other technology in human history – at least up until that time.[12]

The acceleration of change affecting information and computing technologies is now almost beyond comprehension and includes advances in processors, sensors, embedded computers, OT, cyber-physical systems. *Digitization* – the conversion of all forms of information into a binary format – has provided the ability to store, process, analyze, and integrate all sorts of information. This has led to the huge data sets commonly known as *big data*, providing significant advances in machine learning and artificial intelligence (AI).

Indeed, digitization of information and full integration of many data streams has led to *digitalization*, the transformation that offers an incredibly broad understanding of systems that heretofore was impossible.[13] As an example, the concept of a *smart ship* allows the master of a vessel to be aware of almost every aspect about the state of the vessel, from the speed, course, bearing, water temperature, and salinity level to the stress on the hull, instantaneous fuel consumption, cargo container status, and power generation levels. Smart ports, the Internet of Things, the Ocean of Things,[14] increased automation in maritime systems, and fully autonomous vessels are a direct result of this transformation within our knowledge base and AI

[12] Kleinrock, L. (2010, August). An Early History of the Internet. *IEEE Communications Magazine*, *48*(8), 26-36. https://www.lk.cs.ucla.edu/data/files/Kleinrock/An%20Early%20History%20Of%20The%20Internet.pdf

[13] Sanchez-Gonzalez, P.-L., Díaz-Gutiérrez, D., Leo, T.J., & Núñez-Rivas, L.R. (2019, February 22). Toward Digitalization of Maritime Transport? *Sensors*, *19*(4), 926. https://doi.org/10.3390/s19040926; United Nations Conference on Trade and Development (UNCTAD). (2019, June). Digitalization in Maritime Transport: Ensuring Opportunities for Development. *Policy Brief No. 75*. https://unctad.org/system/files/official-document/presspb2019d4_en.pdf

[14] See the Defense Advanced Research Projects Agency OoT Web page at https://oceanofthings.darpa.mil/

software. Taken all together, the combination of advanced ICT and smart systems is driving Industry 4.0, or what is recognized as the fourth industrial revolution.[15]

The drivers for this rapidly increasing level of intelligence include safety and efficiency in operation. The majority of maritime accidents are caused by human error, often due to fatigue; automated systems can respond more quickly to unexpected events and a smart ship is better able to anticipate events. In addition, more complete knowledge of the state of the vessel can allow the officers to provide more efficient operation and routing, which can lead to a lowering of operation and fuel costs.[16]

These data-driven systems, however, offer a larger cyberattack surface than ever before. Computer attacks that were almost unheard of 30 years ago are commonplace today; ships that barely had a computer onboard 25 years ago are now susceptible to cyberattack even in the middle of the ocean. There has been a significant uptick in cyberattacks targeting the MTS since 2019,[17] including more than a dozen ransomware attacks since early 2020. Cybersecurity has risen to become a significant threat to the smooth operation within the maritime sector.

Additional Thoughts and Considerations

The cyberthreat landscape to the MTS raises the question about the role of government in helping improve the state of maritime cybersecurity. The government's response to a

[15] Marr, B. (2018, September 2). What is Industry 4.0? Here's a Super Easy Explanation for Anyone. *Forbes*. https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/; Reni, A., Hidayat, S., Bhawika, G.W., Ratnawati, E, & Nguyen, P.T. (2020, February 20). Maritime Technology and the Industrial Revolution. *Journal of Environmental Treatment Techniques*, *8*(1), 210-213.

[16] Kosowatz, J. (2019, September 2). Sailing Towards Autonomy: Future of Self-Driving Cargo Ships. *The American Society of Mechanical Engineers*. https://www.asme.org/topics-resources/content/sailing-toward-autonomy-future-of-self-driving-cargo-ships

[17] Maritime Cyber Attacks Increase by 900% in Three Years. (2020, July 29). *Vanguard*. https://www.vanguardngr.com/2020/07/maritime-cyber-attacks-increase-by-900-in-three-years/; Report: Maritime Cyberattacks Up by 400 Percent. (2020, June 4). *The Maritime Executive*. https://maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent

physical attack is very different than that of a cyber attack. If a foreign country were to fire a missile at a private company within the U.S., for example, the government would take the lead to track down the source and, undoubtedly, respond militarily. Conversely, when foreign entities launch cyberattacks against American companies, the government response is essentially that the target is on their own.[18]

The MTS represents a concentration of cyber risk. In this context, risk is a function of system vulnerabilities, exploits that can take advantage of these vulnerabilities, and threat actors willing to use these exploits to cause harm. The *Vulnerabilities Trump Threats* maxim says that a cyberdefender needs to concentrate on vulnerabilities in their systems because these are internal and manageable, rather than focusing on threats because those are external and largely unknown.[19]

One example of a significant vulnerability to the MTS are the systems used for positioning, navigation, and timing (PNT), and situational awareness at sea. The primary source for PNT in maritime – in fact, the primary timing source for all U.S. critical infrastructures – is the Global Positioning System (GPS). GPS has been a victim of jamming (i.e., blocking of the signal) and spoofing (i.e., sending false timing and location information) for some years.[20] The Automatic Identification System (AIS) is used for maritime situational awareness. AIS

[18] Why Do We Call it Cyber CRIME? Gary Warner at TEDxBirmingham 2014. (2014, March 1). https://www.youtube.com/watch?v=MPMr5jPwA7I

[19] Johnston, R.G. (2020, July). Security Maxims. *Right Brain Sekurity*. http://rbsekurity.com/Papers /Johnston_Security_Maxims.pdf

[20] Balduzzi, M., Wilhoit, K., & Pasta, A. (2014, December). A Security Evaluation of AIS. Trend Micro Research Paper. https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf; Center for Advanced Defense Studies (C4ADS). (2019). *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria*. https://www.c4reports.org/aboveusonlystars; U.S. Coast Guard (USCG). (2021, April 22). Worldwide Navigational Warnings Service. Marine Safety Information Bulletin (MSIB 05-21). https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2021/MSIB_21-05_WorldwideNavigationalWarningsService.pdf

information will be incorrect when bogus GPS information has been received by a ship or an attacker can insert false information into the system. Although it is of some value to know the Threat Actors that might employ GPS or AIS spoofing, it is more important to fix or augment the systems to be more resistant to the attacks in the first place. This is an important role for government to play.

Unfortunately, regulators, administrators, and managers usually respond to threats rather than vulnerabilities. New laws and funding sources do not appear merely because a new vulnerability is discovered but rather once a new threat is identified. This is a mindset that needs to be re-examined.

We need the federal government to take a more active role in the cyberdefense not only of the MTS, but of transportation as a whole. Industry self-inspection has been cited as partial causes for the Boeing 737 Max[21] and EL FARO[22] disasters. While neither of those were cybersecurity incidents, both speak to the reduced involvement in the inspection and compliance process by responsible government agencies. This is not a question of big government versus small government, but a close examination of the issues in order to determine the appropriate level of government. In general, the level of an agency's authority should match the level of its responsibility. The USCG has the regulatory responsibility to

[21] Schwellenbach, N. & Stodder, E. (2019, March 28). How the FAA Ceded Aviation Safety Oversight to Boeing. *Project on Government Oversight (POGO)*. https://www.pogo.org/analysis/2019/03/how-the-faa-ceded-aviation-safety-oversight-to-boeing/; U.S. Department of Transportation. (2015, October 15). *FAA Lacks an Effective Staffing Model and Risk-Based Oversight Process for Organization Designation Authorization*. Office of the Inspector General, Audit Report No. AV-2016-001. https://www.oig.dot.gov/sites/default/files /FAA%20Oversight%20of%20ODA%20Final%20Report%5E10-15-15.pdf

[22] National Transportation Safety Board. (2017,December 12). Sinking of US Cargo Vessel SS *El Faro* – Atlantic Ocean, Northeast of Acklins and Crooked Island, Bahamas, October 1, 2015. NTSB Marine Accident Report (MAR)-17/01, PB2018-100342, Notation 57238. https://www.nhc.noaa.gov/pdf/ElFaro-NTSB-full.pdf; United State Government Accountability Office (GAO). (2020, April). *VESSEL SAFETY: The Coast Guard Conducts Recurrent Inspections and Has Issued Guidance to Address Emergency Preparedness*. Report to Congressional Committees, GAO-20-459. https://www.gao.gov/assets/710/705785.pdf

protect the MTS from all forms of threat, in both real space and cyberspace. They must be provided with the necessary resources to carry out this vital mission.

Another critical defensive tactic is related to intelligence sharing. Cyber-related incidents, reports, and analysis must not only be freely shared amongst all of the government regulatory agencies, but between all MTS stakeholders that wish to participate. The maritime entities most at risk are the small shipping lines, ports, cargo handlers, and manufacturers that do not have the financial assets to have a large information security team or join one of the industry information sharing organizations. A central maritime security information sharing center – such as Singapore's Information Fusion Centre[23] – would go a long way to assisting the MTS in protecting itself against new and emerging threats in both real space and cyberspace.[24]

Maritime regulators also need to prepare better reporting requirements about cyber-related events for information flow to the Department of Homeland Security (DHS), the Cyber and Infrastructure Security Agency (CISA), and/or USCG, as well as a central location for such reporting, and clearinghouse and reporting distribution center for the industry.

Additionally, we have to recognize cybersecurity as a safety issue in the maritime environment. The maritime industry prides itself on it focus – and relatively strong record – on safety. But cyber safe environments require excellent cybersecurity hygiene on the part of the users and that requires regular training for all members of the MTS.[25]

[23] https://www.ifc.org.sg

[24] U.S. Coast Guard. (2021, August). *CYBER STRATEGIC OUTLOOK: The United States Coast Guard's Vision To Protect and Operate in Cyberspace*. https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf; U.S. Department of Homeland Security (DHS). (2016, October). *Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community*. https://www.cisa.gov /sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf

[25] Canepa, M., Ballini, FD. Dalaklis, D., & Vakili, S. (2021, March). Assessing the Effectiveness of Cybersecurity Training and Raising Awareness Within the Maritime Domain. In *Proceedings of the* 15th *International Technology,*

Finally, the designers and builders of maritime systems that depend upon any ICT or OT equipment need to have a mindset of *security by design*. All too often, systems are protected by layering security on during implementation rather than designing security into every device. Indeed, a vessel network composed of a collection of secure devices might itself not be secure; the network must be designed with security in mind.

Conclusion

The United States is very much a maritime nation where our food security, energy security, economic security, homeland security, and national security are dependent upon the seas. The maritime transportation sector is broad, diverse, and global so that, while international cooperation is essential, central management is impossible. Cyber vulnerabilities are as plentiful in the maritime sector as in the non-maritime world and provide unique threats to the industry. Both the commercial maritime industry and our military maritime interests demand our proactive response to this ongoing threat.[26]

The *National Maritime Cybersecurity Plan* was a clarion call about a significant threat facing this country. Our report, *Raising the Colors*, was a first step at trying to provide a tactical approach to addressing that threat. We have to continue pushing forward to address this critical issue.

Education and Development (INTED) Conference. http://dx.doi.org/10.21125/inted.2021.0726; Tam, K., & Jones, K. (2019). Factors Affecting Cyber Risk in Maritime. In *Proceedings of 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Oxford, UK, 2019, 1-8. https://www.researchgate.net/profile/Kimberly-Tam/publication/334051022_Factors_Affecting_Cyber_Risk_in_Maritime/links/5e60e9cb299bf182deea63a6/Factors-Affecting-Cyber-Risk-in-Maritime.pdf

[26] Demchak, C.C., and Thomas, M.L. (2021, October 15). Can't Sail Away from Cyber Attacks: 'Sea-Hacking' from Land. *War on the Rocks*. https://warontherocks.com/2021/10/cant-sail-away-from-cyber-attacks-sea-hacking-from-land/; Zorri, D.M., & Kessler, G.C. (2021, September 8). Cyber Threats and Choke Points: How Adversaries are Leveraging Maritime Cyber Vulnerabilities for Advantage in Irregular Warfare. *Modern War Institute at West Point*. https://mwi.usma.edu/cyber-threats-and-choke-points-how-adversaries-are-leveraging-maritime-cyber-vulnerabilities-for-advantage-in-irregular-warfare/

Thank you again for the opportunity to provide testimony and information for the committee. I look forward to your questions and further discussion.