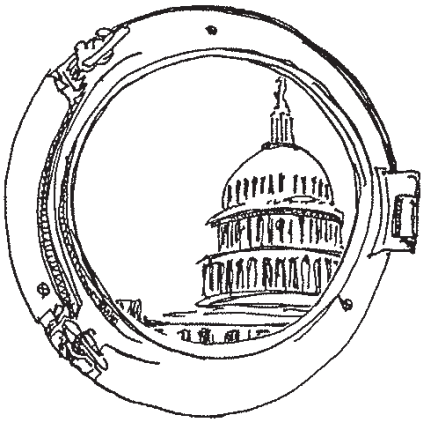
WINDOW ON WASHINGTON



CYBER SETS SAIL

By Bryant E. Gardner

Automated container tracking and crane systems go haywire in a major U.S. Port, shutting down operations for weeks and wreaking havoc on supply chains across the country. Computer assisted navigation and propulsion systems on a supertanker go dark causing the vessel to break up on the East Coast just before high summer season. An offshore rig's stabilization system fails causing her to tilt at a dangerous angle, shut down production, and potentially discharge large amounts of crude oil. Container tracking and gate appointments are masked and manipulated to smuggle drugs or a dirty bomb through ports undetected. Each of these is an all-too possible scenario resulting from cyber attacks on the maritime sector—and several have happened already.

Cybersecurity is a hot issue in Washington. According to the latest National Intelligence Estimate, the next terrorist attack on U.S. infrastructure is just as likely to be a cyber attack as a conventional terrorist attack, but many sectors of the economy are poorly prepared.[1] Although the Defense Department ("DOD") has been acutely aware of cyber warfare issues for quite some time (how long, only they know) and the Nuclear Regulatory Commission has evolved a regulatory framework following 9/11, there is very little awareness and even less preparedness for cyber attacks upon maritime infrastructure. In the wake of a handful of high priority incidents, such as the Stuxnet worm breach of Iran's nuclear program, and a parade of data breaches against, *inter alia*, Home Depot, Target, and Sony Pictures, other communities are also tuning in, among them the maritime regulators. In February 2013, President Obama issued an Executive Order[2] and companion Presidential Policy Directive[3] calling for improved critical infrastructure cybersecurity across all of Government and emphasizing a cooperative approach with industry. Toward that end, the Executive Order called for the National Institute of Standards and Technology ("NIST") to lead the development of a cybersecurity framework.

The development of a maritime cybersecurity regime is in its infancy. One of the first analyses came in November 2011, when the European Network and

[1] Commander Joseph Kramek, U.S. Coast Guard, Federal Executive Fellow, *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*, Brookings Ctr. for 21st Century Sec. & Intelligence (July 2013).

[2] Exec. Order No. 13,636, 78 CFR 11739 (Feb. 12, 2013).

[3] *Critical Infrastructure Security and Resilience*, Presidential Policy Directive-21 (Feb. 12, 2013).

Information Security Agency ("ENISA") issued its "Analysis of Cyber Security Aspects in the Maritime Sector," which found low to non-existent awareness of cybersecurity issues in the European maritime sector incongruous with the importance of the sector to social wellbeing in member states.[4] Specifically, it concluded that the sector was "particularly vulnerable to cyber attacks, which could result in severe maritime disruptions," due to the lack of risk awareness and rapid transition to adopt new technologies without commensurate adoption of security measures. For example, the agency found significant industry exposure to attacks on Information Communication and Technology used throughout the industry for navigation, propulsion, freight management, traffic control, etc. In particular, the report flagged the port sector, which has become increasingly privatized, outsourcing core competencies to international vendors typically developing the information technology outside European member states. ENISA recommended a short-term goal primarily aimed at getting maritime stakeholders aware of the cyber risks they face, and the development of a holistic maritime cyber strategy over the mid-term, to be ultimately crystallized into a regulatory framework in coordination with the International Maritime Organization ("IMO") over the long-term, building off the existing physical security apparatus.

Then, in July 2013, Commander Kramek, U.S.C.G. (now Captain), issued a report examining U.S. port cybersecurity while working with the Brookings Institution in 2013.[5] The Kramek report offered a very sobering assessment of the soft underbelly presented by ports which supply a nation of zero-inventory, just-in-time delivery systems that would grind to a halt in the event of a major attack upon highly automated port critical infrastructure. Consistent with the ENISA analysis of European ports several years earlier, Kramek found a low to non-existent awareness of cybersecurity challenges at U.S. ports and a lack of cybersecurity culture in ports, despite the fact that they are heavily reliant upon digital solutions which are most often networked.[6] He also noted the lack of cybersecurity standards for U.S. ports, and the dearth of U.S. Coast Guard authority to regulate cybersecurity in port facilities or in any other area of maritime critical infrastructure, posing a legal challenge to executive action by the service. In conclusion, Kramek recommended that (i) Congress pass legislation providing the Coast Guard authority to enforce cybersecurity standards for maritime critical infrastructure consistent with existing physical security standards; (ii) the Coast Guard ensure a functional information sharing network is in place permitting government, port owners and operators, and other industry stakeholders to exchange cyber threat information; and (iii) port owners and operators conduct cyber vulnerability assessments and prepare response plans.

Around the same time in 2013, Senator Jay Rockefeller (D-WV), Chairman of the U.S. Senate Committee on Commerce, Science, and Transportation called upon the U.S. Government Accountability Office ("GAO") to prepare a report examining cybersecurity measures in U.S. ports. In June 2014, GAO released its report, tellingly titled "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity."[7] GAO found that the Department of Homeland Security ("DHS"), which includes the Coast Guard, has focused upon physical security threats, mostly to the exclusion of cyber threats, and has yet to conduct an assessment of vulnerabilities and potential consequences of a cyber attack—let alone planning for prevention and recovery. However, GAO reported that DHS officials advised that future security plans would be required to include cybersecurity measures. GAO recommended that the Coast Guard assess cyber security risks, use the assessment to inform maritime security guidance, and determine whether to re-establish maritime sector information coordinating counsel among government and industry stakeholders. GAO further recommended that FEMA

---

[4] European Network and Information Security Agency, *Analysis of Cyber Security Aspects in the Maritime Sector* (Heraklion, Greece: November 2011). *See also* Commonwealth of Australia, Office of the Inspector of Transport Security, *Offshore Oil and Gas Resources Sector Security Inquiry* (2012) (finding that cyber attack is probably the most serious threat to offshore oil and gas facilities and land-based production).

[5] Commander Joseph Kramek, U.S. Coast Guard, Federal Executive Fellow, *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities* (July 2013).

[6] The Kramek report did, however, observe that some of the larger ports such as Long Beach and Houston have substantial in-house information technology operations with awareness of cyber threats. However, even in these cases he found a lack of cybersecurity training, vulnerability assessments, or written response plans and guidelines.

[7] U.S. Gov't Accountability Office, *Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity*, GAO-14-459 (June 2014).

reexamine its grant structure to encompass and incentivize cybersecurity.

On December 18, 2014, the U.S. Coast Guard published in the Federal Register a notice of public meeting and request for comments to receive stakeholder views on the identification and mitigation of vulnerabilities to cyber-dependent systems in the maritime sector in order to formulate governing policy to address such vulnerabilities.[8] Importantly, the notice marks the Coast Guard's realization that "cyber-related vulnerabilities could contribute to a Transportation Security Incident" under Coast Guard regulations implementing the Maritime Transportation Security Act ("MTSA"), bridging concerns earlier raised by Commander Kramek that the agency lacked the authority to address cyber matters.[9] The notice specifically requests comments regarding potential cyber weaknesses, current procedures and standards used to identify vulnerabilities, cybersecurity programs now used by industry that the agency should recognize, the state of cybersecurity training, the value of manual backups or other non-technical approaches to address cybersecurity vulnerabilities, the continued use of the Coast Guard's bespoke "Alternative Security Programs"[10] in the cyber arena, and the extent to which classification societies and protection and indemnity clubs or other insurers recognize cybersecurity practices in the maritime sector.[11]

Commenters identified numerous maritime systems vulnerable to cyber attacks, including Automatic Identification Systems, Global Positioning Systems, Electronic Chart Display and Information Systems, Global Maritime Distress and Safety Systems, Ship Security Alert Systems, Load and Stability Programs, onboard servers including email, and Safety Management Systems, among others. However, several stakeholders declined to disclose in the public docket details regarding vulnerabilities and defenses, with concern of undermining their existing security regime. Several industry stakeholders opined upon the need for greater information sharing, movement beyond best risk practices toward an overall improvement in risk assessment and management for marine software applications, and upon the need for greater focus on cybersecurity in marine training programs for both vessel and facility personnel. Additionally, commenters emphasized the need to ensure coordination with other Federal and state actors in order to prevent the development, implementation, and enforcement of duplicative, contrary, or unnecessary mandates on the industry. Lastly, commenters from the marine underwriting community indicated that they currently do not offer cyber coverage because the risk of a systemic loss across many platforms is uninsurable, and in any event cyber attack coverage would be premature since many of the insured do not even know how often they are hit by cyber attacks or the extent to which their systems present risk to themselves and the insurers.

The Coast Guard conducted its first maritime cybersecurity meeting at the U.S. Department of Transportation on January 15, 2015.[12] Immediately clear during the meeting was the Coast Guard's interest in a collaborative approach, both with industry and with other partner agencies specialist on cybersecurity, notably the NIST which was empowered to set the framework by the President's Executive Order, and the DHS Cybersecurity Division. The Coast Guard confirmed that, from its point of view, the triggering jurisdictional issue is whether the cyber threat rises to the level of a MTSA Transportation Security Incident, and further confirmed that the agency is moving away from a "guns, gates, and guards" only approach to focus upon cybersecurity in maritime security plans. Importantly, Coast Guard leadership made clear that they have not yet determined where they are on the spectrum of regulation for cyber, and that it remains an open question as to whether cybersecurity regulations on par with the existing physical security regulations will be promulgated, or whether a more collaborative, voluntary approach is more

---

[8] U.S. Coast Guard, Depart. of Homeland Sec., Notice with Request for Comments, *Guidance on Cybersecurity Standards*, 79 Fed. Reg. 75,574 (Dec. 18, 2014) (subsequently corrected at 79 Fed. Reg. 78,883 (Dec. 31, 2014)). Comments are available at http://www.regulations.gov, Docket No. USCG-2014-1020.

[9] *Id.* (citing 33 CFR § 101.105). *See also* U.S. Coast Guard, Guidance on Maritime Cybersecurity Standards, Notice of Public Meeting and Request for Comments, 79 Fed. Reg. 73,896 (Dec. 12, 2014).

[10] Alternative Security Program means "a third-party or industry organization developed standard that the Commandant [of the Coast Guard] has determined provides an equivalent level of security to that established by [33 CFR Chapter I, Subchapter H]." 33 CFR § 101.105.

[11] Comments were due April 15, 2015, after this article went to print.

[12] The meeting is available on YouTube at https://www.youtube.com/watch?v=rzOVc1ZOuvY&feature=youtube.

appropriate. Moreover, they acknowledged the old saying that "if you've seen one port, you've seen one port" because of the widely varying arrangements of ownership and operation at U.S. ports, and suggested that expansion of the Alternative Security Program to cyber matters may be the best way to individually tailor requirements.

Also during the meeting, maritime industry stakeholders raised a host of concerns with the Coast Guard's foray into cybersecurity. Of particular concern was that the Coast Guard not impose a rigid "one size fits all" set of regulations or requirements onto ports which have evolved in very different directions, with vastly different resources, and with vastly different risks in respect of cyber threats. In keeping with similar concerns expressed by the American Association of Port Authorities, a spokesperson for the American Waterways Operators opined that any effort must be "scalable and risk-based." Moreover, commenters across the spectrum were in agreement with respect to the need to expand port security grants to include cybersecurity matters, and further suggested that stakeholder matching requirements for grants be suspended in order to better incentivize cybersecurity measures.

In closing, the Coast Guard addressed questions about timeline and industry incentives to move forward at this time. Rear Admiral Paul Thomas, Assistant Commandant for Prevention Policy, observed that the Coast Guard recently conducted an analysis that revealed 88% of the cost of Coast Guard regulations arises out of two requirements: The Oil Pollution Act of 1990 and MTSA—each of which followed a national tragedy. Therefore, he concluded, the cost of waiting could be high: "Wait to fail, then Congress will fix it as expensively as possible," Thomas said. "If we wait until we fail, that opportunity [to collaborate on cyber standards and policies] goes away."[13]

The Coast Guard's maritime cyber security initiative is still in its formative stages, but the service should be applauded for forging ahead consistent with the President's directives. The effort is challenged by the rapidly evolving and increasingly sophisticated cyber threat, which must be balanced against the desire to ensure a thoughtful, measured process permitting balanced and widespread stakeholder input. Industry participants should pay close attention to the effort to ensure that their unique concerns are proactively addressed up front before government policy is set, because once that ship has sailed it's a big effort to turn it around.

*****

Bryant E. Gardner is a Partner at Winston & Strawn, LLP, Washington, D.C. B.A., summa cum laude 1996, Tulane University of Louisiana; J.D. cum laude 2000, Tulane Law School.

[13] *Coast Guard officials emphasize flexibility, sound economics in cyber policy*, Inside Cybersecurity (Jan. 20, 2015).