CCICADA
Command, Control, and Interoperability Center for Advanced Data Analysis

DIMACS
Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center

Maritime Cyber Security Symposium hosted by CCICADA at Rutgers University

[March, 2015] On March 2-3, 2015 CCICADA, the homeland security center of excellence based at DIMACS, hosted a Maritime Cybersecurity Learning Seminar and Symposium at Rutgers University. The organizers believe it to be the first event dedicated to articulating the cybersecurity challenges and threats to the maritime transportation system. The symposium was jointly organized and sponsored by CCICADA and the American Military University, with additional sponsorship from the Centre for Combined Joint Operations from the Sea, a NATO center based in Norfolk. It brought roughly 150 participants to Rutgers and reached over 200 more who participated remotely. Vice Admiral Chuck Michel, the Deputy Commandant of the Coast Guard, highlighted the importance of the event by unveiling the Coast Guard's new cyber security strategy in its first public preview, and he invited attendees to help ensure that they "get it right."

Vice Admiral Chuck Michel of the US Coast Guard delivered the morning keynote presentation at the Symposium.

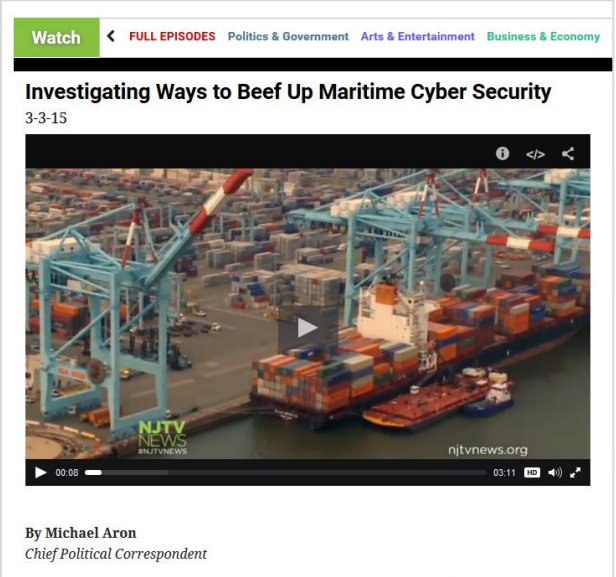
U.S. ports handle more than $1.3 trillion in cargo every year and are vital to the nation's economy, and like other critical infrastructures, maritime transportation must be protected against both physical and cyber threats. Increasingly, port and vessel operations are controlled by networks, which symposium speakers identified as attractive targets for exploitation and potentially crippling sources of vulnerability. Coast Guard Rear Admiral Marshall Lytle opened the event by describing modern ports and vessels as entirely networked and largely automated. Networks are at the heart of navigation, radar, and engine systems on vessels—he said that "virtually nothing" happens on a modern container ship without networks. Likewise for port operations—cranes move via GPS allowing unloading of a cargo ship to be almost completely autonomous.

US Coast Guard Rear Admiral Marshall Lytle's talk opened the Learning Seminar

While the cyber exploits in the maritime domain sound familiar—denial-of-service attacks, phishing, Trojan horses, viruses, and worms—the potential scenarios sound both larger than life and entirely plausible. Reliance on GPS for navigation both at sea and in ports poses a more domain-specific threat. Rear Admiral Lytle offered an example of a trucker who used a GPS jamming device to prevent his employer from tracking him, but in so doing, he unwittingly interrupted cargo operations every time he made a pickup at the port. Another example concerned the Electronic Chart Display and Information System (ECDIS), a computer-based navigation system that augments and largely supplants paper navigation charts. ECDIS integrates a variety of real-time information and serves as an automated decision aid, continuously determining a ship's position in relation to land, charted

objects, navigation aids, and unseen hazards. It includes electronic navigational charts and integrates position information from GPS and other navigational sensors. Rear Admiral Lytle noted that ECDIS is not a "closed environment," and malicious corruption of chart data or other navigational information could lead to the grounding or diverting of enormous vessels.

Other speakers at the event represented a wide range of expertise in the maritime and cybersecurity domains. Among them were: Dr. Phyllis Schneck, Deputy Under-Secretary for Cybersecurity and Communications at the Department of Homeland Security (DHS), who described the National Cybersecurity and Communications Integration Center and building capabilities for automated machine-to-machine communication to block cyber threats in real time; Christopher Rodriguez, Director of New Jersey's Office of Homeland Security and Preparedness, who was featured with Vice Admiral Michel in a related report by Michael Aron of NJTV News; and Stephen Caldwell, Former Director of Maritime and Supply Chain Security at the U.S. Government Accountability Office, who compared the findings of reports on maritime cybersecurity from agencies in Europe, Australia, and the U.S., including a 2014 GAO report that he led. Among the common themes in the reports and in the Symposium presentations was the low level of cybersecurity awareness in the maritime domain and the critical need to increase it.



A major goal of this first symposium on the topic was to raise awareness by bringing maritime cybersecurity to the attention of a wider audience. In his opening remarks, CCICADA Director Fred Roberts noted that outcomes from the event will include a post-symposium book and recording of presentations that he hopes can be used for educational purposes in future courses.

To learn more about the Symposium, the CCICADA website includes more detailed articles on Vice Admiral Michel's remarks, the Symposium in general, and on discussions related to cybersecurity education.

Related Links:

- CCICADA: http://www.ccicada.org/
- Maritime Cybersecurity Learning Seminar and Symposium: http://www.ccicada.org/2014/12/08/maritime-cyber-security-learning-seminar-and-symposium-at-ccicada-at-rutgers-university-march-2-3-2015/
- American Military University: http://www.amu.apus.edu/index.html
- Centre for Combined Joint Operations from the Sea: http://www.cjoscoe.org/home.html
- Report by Michael Aron: http://www.njtvonline.org/news/video/investigating-ways-to-beef-up-maritime-cyber-security/
- National Cybersecurity and Communications Integration Center: http://www.dhs.gov/about-national-cybersecurity-communications-integration-center
- 2014 GAO report: http://www.gao.gov/products/GAO-14-459