Congress seen as failing to prioritize maritime cyber risks

March 27, 2019 John Gallagher

The United States Coast Guard (USCG) routinely responds to cybersecurity breaches on ships at the same time lawmakers are failing to devote the attention and resources needed to help lessen the threat, according to government officials.

“The problems are very severe,” said John Garamendi, a Democratic congressman from California, speaking on a panel on “Securing Maritime Commerce” at the Brookings Institution in Washington, D.C. this week.

The spoofing of GPS devices is particularly prevalent, he said. “If we were in a ship in the Black Sea near Sochi (Russia), the navigational equipment on that ship would tell the captain that he is in the middle of Sochi Airport. We should assume that spoofing could occur in the U.S., and ships that are totally dependent on GPS will find this is a problem.”

The USCG warned in October and November of 2018 that “significant” GPS interference continues to be reported by vessels operating in the eastern Mediterranean Sea, concentrated near Port Said, Egypt; the Suez Canal; and near Jeddah Port, Saudi Arabia. “This interference is resulting in lost or otherwise altered GPS signals affecting bridge navigation, GPS-based timing and communications equipment,” the agency stated at the time.

“We’ve become digitally addictive,” Daniel Abel, the USCG’s Deputy Commandant for Operations, said during the panel discussion.

“As it stands now, we get reports from shippers and ships saying, ‘I’ve had a cyber breach and I’m inbounding to your port.’ Our intelligence center can tell us how many ships from that shipping line are due in other U.S. ports, and we work with the company” to assess the level of the threat, he said. “Cyber is a great enabler, but it’s also a great vulnerability.”

Attacks can leave transportation companies financially vulnerable as well. In reporting its fiscal 2019 third quarter on March 19, FedEx (NYSE: FDX) acknowledged that the June 2017 “NotPetya” cyberattack as a factor in its struggles to integrate Dutch delivery firm TNT Express.

The NotPetya malware also attacked container line operator Maersk, affecting five of its APM Terminal facilities in the U.S., causing significant delays in processing cargo containers.

As on-road vehicles continue to morph into “computers on wheels” their cyber vulnerability risks increase as well. And in aviation, U.S. Department of Transportation Inspector General Calvin Scovel testified before Congress on March 27 that his office will soon begin a review of the Federal Aviation Administration’s role in the Aviation Cybersecurity Initiative, in the wake of the 737 MAX 8 investigation.

Todd Semonite, Commanding General of the U.S. Army Corps of Engineers (USACE), is responsible for operation of the locks and dams on the country’s inland waterways system, and worries that federal funding to address cyber vulnerability in the maritime sector is not reflective of the risk levels. The Trump Administration’s 2020 budget proposal cut funding for the USACE by one-third.

“There’s an adage that priorities are those things that get resourced, and if this is a national security issue it has to be resourced adequately,” Semonite said during the panel discussion. “If you flatline the budget and your stuff’s getting older so that it’s even more expensive to maintain it, and add on top of that an additional requirement for a higher level of security, it shows how much stress there is.”

“We know that this is a major vulnerability across every part of our society,” Garamendi said. “Are we up to speed? No. Are we dealing with it? We’re moving ahead inadequately, in my estimation.”