Cybersecurity Sits at the Crux of Government, Industry, Commerce for Sea Services

The moderator of the May 7 panel discussion on cybersecurity at Sea-Air-Space, Navy Vice Adm. Matthew Kohler. Cyber defense is a top concern of all the sea services, panelists said. U.S. Navy/Mass Communication Specialist Seaman Apprentice Richard Rodgers

NATIONAL HARBOR, Md. – Citing recent high-profile comments by Chief of Naval Operations Adm. John M. Richardson and Marine Corps Commandant Gen. Robert B. Neller on cybersecurity's importance, panelists at a May 7 event at Sea-Air-Space agreed that it is a top issue for their services, regardless of external perceptions.

Coast Guard Rear Adm. David Dermanelian, assistant commandant for C4IT and commander of Coast Guard Cyber Command, said his branch is known for its drug interdictions and waterway management missions, but often perception does not equate that work with cybersecurity.

"All those missions are directly linked to the cyber domain," he said. "And I would posit that even within the Coast Guard, we're in contact with bad actors, or the enemy, every day. The Coast Guard's role is to defend our maritime transportation, our cyber domain."

Detailing how maritime commerce coming through U.S. waterways is valued at $5.4 trillion and supports 31 million Americans,

Dermanelian quantified the importance of cybersecurity for fellow panelist,
Maritime Administration Director of the Office of Maritime Security Cameron
Naron.

Naron said it’s critical MARAD has cyber systems, as well as resilient measures, in place should anything under their purview be
compromised. With MARAD sitting at the crux of defense, homeland security and
commerce, his office is focusing on working with all its stakeholders to
maintain security.

“Our role is really to make sure that industry’s needs, industry’s equities, are represented in federal policy formulations,” Naron
said.

Naron said commercial network monitoring and vulnerability remediation options are out there today, and there are also great government
solutions, and those resources need to be in the hands of industry, not only
because it’s good for business, but because it’s good for national security. MARAD
also must ensure the security of the Ready Reserve Fleet, and Naron stressed
that cyber concerns also extend to areas such as precision navigation and GPS
vulnerability.

Gregg Kendrick, Marine Corps Forces Cyberspace Command executive
director, addressed his service’s complex network of cybersecurity operations
and how that information is critical to the Marines’ return to

its roots.

“Just like the Coast Guard, we have a little of a unique mission as well. … The commandant and the chief of naval operations are exceedingly … bringing us out of the ground force and bringing us back to our naval heritage,” Kendrick said. That makes the fidelity of the information the Marines and Navy share when they go from sea and ashore critical so the services can make that gap as seamless as possible, he said.

Kendrick also addressed how the Marines are staffing up their cybersecurity teams, when industry hiring is so competitive. He said 40% of the Corps’ cyber mission force is civilian, stating that Neller wanted to use best business practices from people that work for companies like Google or other software developers to ensure the Marines had cutting-edge tactics.

The moderator, Navy Vice Adm. Matthew Kohler, deputy chief of naval operations for information warfare and director of naval intelligence, summed up the vastness of the challenge of keeping up with cybersecurity needs, and how it’s directly tied to the larger challenges the sea services face. “Technology is running at us at an unprecedented rate. … It’s not just the pace of the technology, it’s the race for how quickly we can adopt that technology … to how we fight and [it] gives us the ‘Great Power Competition’ that we find ourselves in today,” he said.