US Facing ‘Pearl Harbor Moment’ From Cyber Attacks, Vice Adm. Trussler Says



Vice Adm. Jeffrey Trussler says cyber attacks are something that now threaten every American. *NAVY LEAGUE / Lisa Nipp*

NATIONAL HARBOR, Md. — Vice Adm. Jeffrey Trussler, deputy chief of naval operations for information warfare and director of naval intelligence, said cybersecurity threats to the United States are such that “frankly, where we sit today in 2021, we ought to be having one of those Pearl Harbor moments without the Pearl Harbor.”

Trussler spoke on a panel at Sea-Air-Space 2021 panel on “Cyber Today’s Fight, Tomorrows Capabilities,” along with Rear Adm. Michael Ryan, commander of U.S. Coast Guard Cyber Command, Karen Van Dyke, director for positioning, navigation, and timing and spectrum management at the Department of Transportation, and Ryan Roberts, senior manager of cyber and strategic risk at Deloitte.

Trussler said cyber attacks — such as the one that disabled the Colonial Pipeline, affecting the flow of oil along the East Coast and Southeast — shows that the threat is no longer just about defense and security, but “you could be impacted personally from anywhere around the world, based on our dependency on technology … I’m worried that enough people aren’t hearing, wow, it’s a new world.”

Ryan said the Coast Guard is issuing an update to its Cyber Strategic Outlook and wants to embrace innovation on the cybersecurity front, which is where industry can help.

“We understand the value of partnerships, particularly with those in the room,” he said.

Van Dyke said from her point of view, a big fear is the jamming and spoofing of Global Positioning System signals.

“It’s a weak signal coming from space,” she said of GPS, and “it doesn’t take much power to jam GPS over a wide area.”

Jamming is a temporary threat, but spoofing can actually permanently disrupt communications, as a GPS user might lose access to their receiver for good.

“This is an increasing concern,” Van Dyke said, and DoT is working with the Department of Defense to counter these and other threats.

Roberts said automation will take on a larger role when responding to future cyber attacks, as eventually humans will be too slow.

If a major attack happens “and we convene a committee to decide what we’re going to do, we’ve already lost,” he said. “Over time, we’re going to have to remove that human in the loop and get to autonomous decision making.” It’s a scary thought, but “humans are not going to be able to respond quickly enough.”

Interagency cooperation is key to fighting cyber attacks, the panelists said. Trussler said he learned new things just by being on the panel, and said “Sea-Air-Space has done a really good job” in bringing together different viewpoints.

Ryan said the Coast Guard is already working with commercia shipping ports to assess their facilities so they can harden their infrastructure.

That’s a niche area for the service, he said, “but reflective of the fact this is a joint fight.”