Navy Infrastructure to Combat Cyber Threats Still a Work in Progress

U.S. Navy Rear Adm. Danelle Barrett during her May 8 cybersecurity presentation at Sea-Air-Space 2019. Lisa Nipp

NATIONAL HARBOR, Md. — Rear Adm. Danelle Barrett began her May 8 presentation at Sea-Air-Space 2019 with a cost comparison. A Gerald R. Ford-class aircraft carrier costs some $13 billion, she said. A troublemaker can build a capable hacking device that could disrupt systems on a Ford carrier and potentially every other U.S. Navy platform, for about $9.97.

Given that Navy computers rely on the same off-the-shelf providers as industry and the bad guys, Barrett described how she is doing what she can to ensure that data gets delivered safely and quickly to who needs it, without fear of being encumbered by attackers.

Navy ships have "about 50 different systems" funneling data to commanding officers, Barrett said, who in turn have a limited amount of random access memory "to figure out what to do with all that."

The Navy needs the right infrastructure, with machines capable of using artificial intelligence (AI) to sift through the stream of data and provide the most important facts.

As an example, Barrett cited the considerations the carrier Abraham Lincoln's commander and crew would face when planning a trip through the Straits of Hormuz.

"Things are tense with the Iranians. We want a safe transit," Barrett said.

Every key player on the Lincoln wants to know specifics relative to his or her own job, she said.

"The navigator needs to know, can I navigate safely through at [a given] course and speed. The chief engineer wants … data on problems I might have with the plant. The communications officer wants to make sure I don't drive out of my satellite footprint. The intel folks, those on tactical watch and battle watch, need it, too. The last time [a carrier] went through, about 20 nautical miles away, Iranian UAVs came over to harass the ship," Barrett said.

The Navy does not have this capability – to provide data and ensure security to the lowest possible element later – today, Barrett said. She also pointed out that mischief likely would not manifest itself as some bold and splashy operation.

Rather, "They would mess with the data just a little bit … just enough to make you make a

really bad calculation," Barrett said. "It's not going to be noticeable if it's coming from a very sophisticated adversary."

Barrett is spearheading a course that would have the right systems in place as quickly as possible. Stove-piping of approval for new systems, or delivery of data, will not work for her. The process will use "stuff that industry is doing, leveraging the exact same products," and will provide interoperability. The Navy must be able to get its hands on the next fastest thing, get it installed and have it functioning – before enemies upgrade their own capabilities.

"The environment to the left of the boom is going to get more complicated," she said.

Already, ships are inundated with data from scores of sensors in and under the surface and in the air, she said. Soon, thousands of such devices are going to be funneling such information. Managing the data, Barrett said, will require ensuring that its quality is as good as it can be. Commanders should be able to get what they need within, say, a two-hour window of their next major milestone.

"If I could do that today, I'd have a huge operational advantage," Barrett said. "It's a tall order. But we'll get there."