IN THE NEWS

Navy, Marines Bolster Cybersecurity Defenses

March 21, 2016 | *National Defense*

By: Yasmin Tadjdeh

Related Expert: Bryan Clark

Bryan Clark, a senior fellow at the Center for Strategic and Budgetary Assessments, a Washington, D.C.-based think tank, said CANES is "designed to consolidate a lot of the little networks that we have out in the fleet today into a smaller number of networks.

"A lot of the network investment that's being made by the different services is an attempt to reduce the amount of surface area that their networks have to the outside environment," he said.

Smaller networks can often be more vulnerable because they don't have the same level of protection that many of the bigger systems have, he said. Moving to larger networks also allows the services to adopt new forms of information protection, he added.

"In a bigger network I can start using cloud computing. I can start putting information into places where it's going to be harder to find it," he said. "If you go to the cloud … you can actually hide your valuable information among millions of bytes of non-important information."

Going forward, Clark said the Navy and Marine Corps would begin investing in automated systems that could immediately detect when an intruder penetrates a network.

"They want automated features in their software that detect an intrusion and then can immediately isolate that intrusion from other parts of the network and then use the access point that has been gained as a way to respond to the threat and in some ways go and hack the threat immediately," he said. By gaining access to a network, the hacker also makes himself vulnerable because he opened a portal into his own network.

While the government has made significant investments in cybersecurity, more can be done, Clark said.

"The government could spend even more on cybersecurity if you look at it from an infrastructure perspective," he said. "There's been a lot of aspirations in the government to shift to cloud computing to a greater degree and improve security … by protecting … [information] at the data level but it's going to be expensive for the government to do that with its military network just because of the cost of transitioning from all these legacy systems to new systems."…