CyberPro

January 29, 2009

Keeping Cyberspace Professionals Informed

Senior Leader Perspective

NSCI's Lindsay Trimble recently interviewed Vice Admiral H. Denby Starling II. Admiral Starling is commander of the Naval Network Warfare Command in Norfolk, Va. Naval Network Warfare Command (NETWARCOM) is a global command with more than 13,000 military and civilian professionals working to provide sustained information superiority to Navy, Joint and Coalition warfighters. In support of this mission, NETWARCOM delivers and operates a reliable, secure and battle-ready global Navy network, leads the development and integration of information operations capabilities, intelligence and space within the Fleet and for Joint Commanders.

NSCI: What is NETWARCOM's role in supporting Department of Defense cyberspace operations?

VICE ADMIRAL H. DENBY STARLING II: We have a broad spectrum of responsibilities. NETWARCOM's role is two-fold: we are an operational organization that supports all of the DoD organizations that execute any sort of cyberspace activity including the Joint Task Force and USSTRATCOM. We also provide those same services throughout our Naval fleet.

We are "the one-stop shop for cyberspace within the Navy." Our portfolio goes across a number of disciplines. On the operational side, we are responsible for all aspects of information operations, as well as computer network operations and electronic warfare. We act as the Navy's type commander for Fleet Intelligence, Information Operations, Network Operations, Signals Intelligence and Space. We're also the Navy's central operational authority for Cryptology, Information Operations, Information Technology, networks, Signals Intelligence and space in support of Naval forces afloat and ashore. NETWARCOM operates and maintains secure and interoperable Naval networks.

We have training and equipment operations as well, so when it comes to training people, equipping and budgeting, NETWARCOM takes responsibility for those too. Our team isn't responsible for purely networks; we are much broader in scale.

NSCI: There has recently been significant discussion regarding the DoD's organization for cyberspace. What is NETWARCOM's relationship to other DoD organizations supporting cyberspace operations?

STARLING: The DoD organization is at a stage of growth and maturation right now. USSTRATCOM is designated as the organization responsible for the defense of the global network for the military. I have a direct reporting relationship to USSTRATCOM for planning and support in computer operations and network operations. I also work directly for the Joint Task Force for Global Network Operations; we provide the same function for the Navy's side of the DoD network.

We have similar relationships with the National Security Agency, the Joint Functional Component Command for Network Warfare and the Defense Information Systems Agency. There are Navy personnel in those organizations and we work with them on training.

My boss is Admiral Jon Greenert at U.S. Fleet Forces Command. I'm an arm of the fleet, so it provides a great tie-in between fleet operations and cyberspace operations that take place on ships and the contributions the Navy makes to our nation. It really ties things together quite well. On the other side of the house, I have a reporting responsibility to the commander of U.S. Strategic Command and we work very closely with the Director of Naval Intelligence.

NSCI: From a NETWARCOM perspective, can you discuss a few of the key challenges regarding cyberspace operations?

STARLING: The biggest challenge is the scope of it. NETWARCOM has only been around for six years. It was set up in 2002 when our computer operations and what we now commonly refer to as ISR were converging. Back in 2002, the Navy combined all of its communication organizations as well as its computer network organizations into one organization – NETWARCOM. Three years later, we combined it with the Navy's security group, the Navy's cryptologic element. We're responsible for operating the network and defending the network. We think this organization is very powerful conceptually. It aligns with the recent change that has Joint Task Force for Global Network Operations working for the Joint Force Component Commander for Network Operations.

The scope of the challenge is huge. It covers every warfare area and impacts everything we do. If you're in DoD with a computer on your desk, you're a cyber warrior – even if you're not on the battlefield, but here in the U.S. You don't have the luxury of defining your battlespace geographically or the time and place you want to engage. You're in it everyday and your workforce is in it everyday.

We have a very large challenge out there to train our folks in cyberspace activities and how cyber activities support the typical things we think about the military doing, but also the rest of the network that does our day-to-day business. We have to secure the entire network. It's a huge challenge – both the training aspect and just getting your arms around the whole piece.

NSCI: What activities does NETWARCOM have underway to improve cyberspace capabilities?

STARLING: There is obviously a huge technology component to what we do. We are working closely with our resource sponsors in Washington, D.C., as well as with our Systems Commander to make sure that the technology we employ makes us ready to fight in this domain. We need the newest and the greatest. We also have to ensure that the network is technologically sealed everywhere. We have to have the best technology out there to defend against our enemies.

But technology means nothing without a quality workforce. We define the requirements for our future workforce to help the Navy recruit and retain what we need to operate in this domain. We also work to educate our current workforce so they don't do something that weakens our posture on the networks. We need to integrate these capabilities with how we operate.

DoD is on a voyage of discovery in the realm of cyberspace. We have to integrate Navy with the DoD; and other branches of the government outside of DoD to make sure the wholeness of the network is there. Figuring out where this is taking us is important to stay ahead of those who want to do us harm.

NSCI: What do you see as opportunities where industry and academia may be able to contribute to improving cyberspace?

STARLING: There is a laundry list of technologies that industry is developing that would contribute to the things we can do. Much of it centers around making our networks more secure and easier to operate. The network world is complex and when you look at what industry has done to simplify the operation of networks and computers, we need that inside the military. We had a habit for a number of years of having networks designed by engineers for engineers. Anything we can do that reduces our training burden gives us a great advantage. Those things that bring us simplicity in multiple domains in what is a complex environment would be very welcome.

In the Navy, we operate on the sea, under the sea, on the shore, in the air and space. We need solutions. It is helpful when the solutions can move back and forth from a ship, through a satellite or other medium. We don't have the luxury of running a huge landline; what's on the ship is what we've got. It has to be scalable so we can use it on a patrol craft or hand it to a special forces unit as well as running it on an aircraft carrier. You also have to remember that cyberwarfare is an inherently joint business, so I'm not interested in a Navy-only solution, but a solution that would work across the different branches of the military.

In cyberspace, industry and academia face many of the same challenges the military does. Everybody is interested in network defense – from banks to colleges to the military. Those things the industry develops for its own protection can be useful to us too. We need to find a way to partner with industry on things that meet all of our needs. I would suspect that there are many things being done in corporate America that would really benefit the military as well; we just have to discover it.

NSCI: What are some of your priorities in the area of cyber-warfare and/or computer network defense?

STARLING: There are really three. First, you've got to understand what the adversary is doing and be able to defend yourself against them. It will take a tremendous amount of effort because you have to have other ways of understanding what the threat is.

Second, we have to leverage the knowledge of putting ourselves in the position to take the advantage. Cyber warfare could be a stand-alone portion of the next war – a cyberwar that exists on its own, damaging economically, politically and even physically.

Third, we need to really have a trained and educated workforce that understands this stuff. It's challenging for the military because there are a limited number of these folks out there. Industry wants them, the government wants them and the military wants them. We need to retain the best and the brightest to do cyberspace work and enter cyberspace career fields. It's a high priority for all of us.

That's an excellent point about looking for the best and the brightest. I know that much of industry and government organizations are experiencing this same competitive atmosphere.

That's exactly right. If you've got an IT guy at NASA or in a corporate atmosphere, you care if they are capable of showing up to work on time and doing the job. You don't have to worry about them getting through a physical fitness test or being overseas deployable. There are extra challenges for military recruitment. We look closely at people's backgrounds and finding people that are qualified to be in the military makes it tougher than the average civilian company. We don't have the luxury of a huge budget in the military either. We do offer things you can't find anyplace else, though – we give people a chance to serve our nation, make a huge difference and do things you wouldn't have the opportunity to do anywhere else.

NSCI: Is there anything else you'd like to add?

STARLING: Thank you again for the opportunity to tell our story a little bit; what we're doing is not necessarily understood outside of the Navy. This is the side of business that we don't spend too much time publicly talking about, due to security aspects of the business.

The Navy has done some leading-edge things in cyberspace – and not just on the technical side of the house. The Navy Cyber Defense Operations Command (NCDOC) used to be the former Navy Computer Incident Response Team. The organization was upgraded to a command in January 2006 after its mission was expanded. We're the only service cyber defense organization that has attained the National Security Agency's highest certification for network defense. Our NCDOC was the first Computer Network Defense Service Provider in DoD to achieve this level of certification.

The Navy was also the first of the services to establish an enlisted rating that's designed specifically for computer network operations – the Cryptologic Technician Network rating established in 2004. We've been heading down a road now for the past three to five years to develop people to work specifically in network ops. The Navy has a strong educational capacity to train people to do this in all branches of the service. We train people in all the branches of the military in high-end computer network defense at the Center for Information Dominance at Corry Station in Pensacola, Fla.