CyberPro

May 5, 2011

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: DAVID J. "JACK" DORSETT, VADM, US NAVY

NSCI's Charles Winstead recently had the opportunity to interview Vice Admiral Jack Dorsett, Deputy Chief of Naval Operations for Information Dominance (N2/N6) and Director of Naval Intelligence (DNI). Vice Admiral Dorsett was born in Roanoke Rapids, N.C., and raised in Virginia. He graduated from Jacksonville University (Florida) in 1978. As a flag officer, he has served as: special assistant to the Director of Naval Intelligence; director of Intelligence (J2), United States Pacific Command; director for Intelligence (J2), U.S. Joint Staff; and is the 63rd Director of Naval Intelligence (N2), Chief of Naval Operations. On November 2, 2009, Dorsett assumed office as the first Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6). Dorsett is a naval intelligence officer, joint specialty officer, a specialist in Joint and Strategic Intelligence, and a qualified surface warfare officer. He possesses significant experience in National Security Affairs (Europe, Middle East, Asia) and in Strategic Planning. He graduated with distinction from the U.S. Naval War College and Armed Forces Staff College, and was awarded a Master's Degree from the Defense Intelligence College.

NSCI: It's been about 18 months since the CNO announced the creation of the Navy's Information Dominance Corps. Can you give us an update on how it is going and the priorities for the next 12 months?

Dorsett: We have achieved considerable momentum in the past 18 months. I'm very proud of the achievements of our professionals and the innovative approaches they are taking to advancing the Chief of Naval Operations' vision for the Navy. For those not familiar, the CNO has directed that the Navy pioneer, field and employ game-changing capabilities to ensure Information Dominance over adversaries and decision superiority for commanders, operational forces, and the nation.

I believe that if you look at the progress we have made in funding new information capabilities, you will quickly recognize that the Navy's Information Dominance team is working deliberately to ensure that "information becomes a main battery of the U.S. Navy." In particular, we have accelerated the funding and/or are actively testing and employing a variety of unmanned airborne systems, including STUAS, FIRE SCOUT VTUAV, BAMS-Demonstrator, BAMS, MRMUAS, UCAS-D, and UCLASS. We are experimenting with unmanned underwater vehicles, and we are recapitalizing Navy's electronic warfare systems (e.g., Surface Electronic Warfare Improvement Program, Ship's Signals Exploitation Equipment, and NextGen Jammer). In the cyber arena, we recommissioned the U.S. TENTH Fleet, established the Navy Cyber Forces type command, and have introduced new cyber curriculum at the U.S. Naval

Academy and Naval Postgraduate School, as well as at our Center for Information Dominance and the Center for Naval Intelligence.

Our priorities for the year ahead include:

1) Delivering Game-Changing Information Capabilities. We will be bold in identifying and resourcing programmatic solutions that advance our unmanned, electronic warfare, ISR, command and control, network, and space capabilities to deliver maximum warfighting effects.

2) Operationalizing Information Dominance. We will coordinate with the fleet and other stakeholders to ensure the development of concepts, strategies, doctrine, TTPs, experimentation, wargames, and training that advance our operational proficiency in the use of cyber, command and control, EW, ISR, space and other information capabilities.

3) Solidifying Information Dominance as a Main Battery. We will continue to build momentum by advancing Information Dominance concepts and reinforcing their strategic value throughout our Navy, the Armed Forces, the Congress, our industrial partners, and the U.S. population at large.

4) Promulgating the Information Dominance Strategy. We will leverage the existing Information Dominance Vision and publish a global Navy strategic network which assures command and control for our commanders and delivers information superiority for our warfighters in the future.

NSCI: Regarding the Information Dominance Corps (IDC), what would you consider the most significant successes of the previous 18 months?

Dorsett: Our most significant success is that members of this profession continue to serve in demanding assignments afloat and ashore. Today, over 1300 active and reserve IDC personnel are currently deployed on individual augmentation assignments in the Central Command area of operations. Our people are demonstrating their skills from Baghdad to Bagram, and from Kandahar to Kabul. Their individual successes are our successes.

I'm also proud of the rapid and highly successful implementation of professional qualifications and standards across the Information Dominance Corps. Quite significantly, the CNO directed the creation of the Information Dominance Warfare pin, recognizing the IDC as the Navy's fifth warfare community (Aviation Warfare, Submarine Warfare, Special Warfare, Surface Warfare and Information Dominance Warfare). In related activity, we established and held our first Corps-wide Command and Milestone Screening Board. We crafted Warfare Professional Qualification Standards and have implemented a professional qualification process. We also implemented a mandatory IDC Senior Leaders Symposium and IDC Mid-Career Course to advance our officers' professional knowledge and skills.

Finally, and perhaps most important, we vigorously communicated the CNO's vision and direction. We have done this through a series of communiqués, interviews, and road shows across the Navy. Our

objective was to reach out and explain this dramatic transformation of the Navy, and to capture the ideas and innovations present in the Fleet.

NSCI: I think originally the IDC included approximately 44,000 personnel. What do you think is the right number and where do the most significant shortages exist?

***Dorsett*:** Our current manpower strength is "about right" to meet the requirements of our operational commanders. We expect some growth in the cyber manpower component of our Corps, and perhaps a slight reduction in the manpower assigned to expeditionary functions as our nation draws down forces in Iraq, and then in Afghanistan. In short, I'd have to say we have about the right number of professionals, but need to increase the depth and breadth of the skills of the work force.

NSCI: As you know, there is a nationwide shortage when it comes to the cyber workforce. How is the Navy going about attracting and retaining cyber personnel?

***Dorsett*:** This is perhaps our greatest challenge, and one that all the Services face. Fortunately for the Navy, we already have a very sound professional cyber work force. Our professionals are formed from two primary communities (Information Warfare and Information Professionals). The Navy's Information Warfare (formerly, cryptologic) community (a part of the Information Dominance Corps) was formed from the cryptologists of the inter-war years. Those professionals earned their reputation during World War II and have maintained their world class status over the past several decades. Navy's Information Professional community is relatively young, but has matured rapidly, and forms the other cornerstone of our cyber professionals. While our future cyber force will be built largely on this foundation, we are also investigating and implementing innovative approaches to recruiting and retaining cyber professionals. For instance, we have implemented cyber education programs at the U.S. Naval Academy and the Naval Postgraduate School. We also are proud that Navy's Center for Information Dominance (Corry Station, Florida) provides the initial training for our cyber professionals, and is also used by other Services for their cyber training. Additionally, we are planning to establish reserve units in high technology locations (e.g., Silicon Valley) and are creating innovative approaches to hiring "civilian" reservists, who are experts in various cyber disciplines, and who can augment the Navy active duty work force.

NSCI: There's been some discussion in the press regarding computer network exploitation (CNE) and computer network attack (CNA). From your perspective, what is the relationship and is there a definitive way to say when the line is crossed from CNE to CNA?

***Dorsett*:** For the U.S., there is a clear distinction between CNE and CNA, which are governed by policy and authorities (Title 50 / Title 10). However, the same cannot be said of our potential adversaries, who are not limited by similar policies or governance. Cyber actors range from nation states to terrorists, criminals, and hackers. Their intent is not always clear and attribution even more difficult to discern. In many cases, cyber operations are deemed a means of information gathering. For some, it is another form of espionage. CNA is focused on causing effects (disrupt, deny, degrade, destroy) against systems, or the information residing on them, compared to CNE which is the exploitation of systems for intelligence purposes.

NSCI: What is the Navy doing to improve cybersecurity at the tactical edge (e.g., data links)?

Dorsett: Navy is improving cyber-security by implementing an improved Defense in Depth infrastructure that is aligned to the DoD Information Assurance Boundary Architecture. Navy's Computer Network Defense Service Provider, the Navy Cyber Defense Operations Command, shore and afloat networks, and data links at the tactical edge all deploy intrusion prevention and detection system sensor grids and firewalls to filter traffic, as well as provide threat analysis and incident response management.

As it relates to data links and telecommunication that serve our warfighters on the tactical edge, Navy planned, programmed, and funded modern cryptographic capabilities to protect classified information transiting over our tactical and strategic communications networks. This investment in modern cryptographic devices protects both network and link communications. Navy is scheduled to implement in ground, sea, and air platforms High Assurance Internet Protocol Encryptors (HAIPE) and Link Encryption Family (LEF) devices to protect strategic networks within a few years. Tactical networks are currently provisioned per OSD guidance. The HAIPE devices will provide critical network protection, while the Link Encryption Family (LEF) devices protect network information in-transit between major telecommunication nodes.

NSCI: What grade would you give the Navy's Cyber Situational Awareness, including its cyber assets, day-to-day readiness, and the threat?

Dorsett: We are good, but need to become much better. Since its establishment in January 2010, one of the highest priorities at U.S. TENTH Fleet has been the development of cyber situation awareness similar to the common operational picture we have for air, surface, and undersea. It is essential to maintain near real-time situational awareness of the status of our networks and communications in order to operate effectively in cyberspace. We must be able to identify, understand, and react to problems in the order of milliseconds.

The Navy is aggressively adapting to the radically changing cyberspace environment. Navy continues to build the capability to ensure the confidentiality, integrity, availability, and authenticity of data and information commensurate with warfighting mission needs. In February of this year, the Navy took the next step in the evolutionary process of Cyber warfighting by launching the Navy Cyber Defense Core (Cyber Core) at the U.S. TENTH Fleet Maritime Operations Center. Cyber Core is a decision support capability displaying timely and relevant information in an innovative manner using a combination of traditional reports and interactive visualizations. It supports role-based decision making by delivering customized dashboard views and improved internal/external reporting in a user friendly web-service environment. Cyber Core provides a one stop shop for the consumption of information based on data gathered, analyzed, and housed within the Navy's cyber defense systems.

NSCI: Can you tell us about the challenges and progress of integrating C2 of Navy maritime, air, and cyber capabilities? Will that happen at the Maritime Operations Center (MOC)?

***Dorsett*:** A. The global nature of cyber poses unique challenges and a primary mission for U.S. TENTH Fleet is to direct cyberspace operations for the Navy, assuring Navy's ability to command and control its operational forces in any environment. The integration of cyberspace operations with Fleet operations will occur at each of the numbered Fleet maritime operations centers, with U.S. TENTH Fleet taking the lead for global cyber command and control in coordination with U.S. Cyber Command and the other Service cyber components. U.S. TENTH Fleet continues to refine the data feeds and tools required to provide a cyberspace situational awareness, and the best means to share that information with the other numbered Fleets.

NSCI: Thank you very much for taking the time to visit with us. Is there anything else you'd like to add?

***Dorsett*:** These are quite exciting times. We have entered a new era, in which the old order is being supplanted by new structures, processes, and capabilities. This revolution in military affairs demands new thinking and a bit of risk taking. Your Navy is taking several bold, innovative steps to deliver capabilities that enable us to dominate across the information domain. Our Corps of information professionals is acquiring and increasing the depth of professional skills required to excel in this environment. Thank you for providing me this brief opportunity to share with you and your readers some of the initiatives the U.S. Navy is implementing in the cyber arena.