Underwritten Content

DEFENSESYSTEMS FCW TECHNICAL PARTNER: Booz | Allen | Hamilton

INFORMATION WARFARE EVOLVES WITH THE TIMES

THE NAVY TAKES AN ENTERPRISE-LEVEL VIEW TO DELIVER NEW TECHNOLOGIES AND DATA TO THE WARFIGHTER.

IN 1998, VICE ADMIRAL Arthur K. Cebrowski and John J. Garstka wrote a landmark article articulating a vision for network-centric warfare, in which tactical decision-making would be based on real-time access to information about the battlespace. That vision is now termed information warfare. It remains a driving force in the Navy and the Department of Defense (DOD) as a whole.

Information warfare has evolved as both the technology and the battlespace have evolved, according to senior Navy leaders and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) experts speaking at an event titled "Network-Centric Warfare: Next Steps toward Achieving the Vision," co-located with WEST 2016, the premier naval conference and exposition on the West Coast held at the San Diego Convention Center.

The basic goal—increasing the speed of command by delivering the right information to the warfighter at the right time and the right place—remains the same. Now the Navy is working in an increasingly complex maritime environment that demands more agility and challenges how the service both develops and defends its warfighting systems—all while driving toward an enterprise approach that integrates the many systems into a cohesive whole to ensure mission success.

CYBER GETS ITS DUE

Perhaps the most important change—one Cebrowski and Garstka could not have anticipated eighteen years ago—has been the emergence of cyberwarfare as a vital concern.

The concept of cyberwarfare has taken shape over time, said keynote speaker Rear Admiral David Lewis, commander of the Space and Naval Warfare Systems Command (SPAWAR), which delivers cyber warfighting capabilities from seabed to space. People bought "a little of this and that … stuff happened, but it wasn't a 'thing'," said Lewis.

That is no longer the case. The Navy has elevated cyber to a warfare domain, putting it on a level with its space, air, land and sea domains. This means it must be managed differently, with a focus on standards, improved acquisition, modernization and systems engineering.

SPAWAR recently unveiled its first set of department-wide cybersecurity standards, which will be incorporated into contracting language, evaluations and inspections. The command is also defining end-to-end systems engineering for C4I by mission thread, as well as defining systems interfaces.

"That's what's happening in this arena," said Lewis. "We are becoming rigorous. We are becoming warfighter-centric. We're on the A-Team now, we're one of the top listed domains for warfighting, and we need to behave differently as a consequence."

RETHINKING THE ENTERPRISE

The evolution of cyberwarfare is bringing in an evolution in how the Navy thinks about building and managing

networks and systems.

In a traditional environment, a network provides fixed connections between a defined set of systems. But such an approach limits the Navy's ability to respond to changes in the cyber landscape. The service wants to spend less time working out network connections and more time delivering new capabilities.

Essentially, network-centric warfare is the enterprise, said Greg Shaffer, assistant chief engineer, mission engineering, at SPAWAR, speaking during a panel discussion at the event.

"We need to stop thinking about building large monolithic, brittle systems," he said. "We need to really start thinking about building smaller apps and widgets that let me plug other apps and widgets together."

One step in that direction is providing developers with a common starting point. "We have to get to the place where we set up a development and integration environment where all the people are developing … and integrating against that same environment on a regular basis," said Bill Bonwit, Department Head for the Command and Control Department of the Space and Naval Warfare Systems Center Pacific.

In the long run, the DOD needs to shift from building fixed networks to creating an open digital ecosystem based on standard interfaces, said Greg Wenzel, executive vice president and lead of Digital Solutions/C4ISR within Booz Allen Hamilton's Strategic Innovation Group.

Otherwise, the DOD will have trouble keeping up with the constantly evolving battlespace. Wenzel pointed to Uber and its ability to disrupt the transportation industry by quickly assembling a new, easy to use application based on open and available interfaces that act together commonly referred to as application program interfaces (APIs). "Having an open digital ecosystem allowed this to happen," he said.

In the same way, the DOD needs to become as agile as the enemy. "We don't want to get 'out-Ubered' by asymmetric threats," he added.

A DATA-CENTRIC PERSPECTIVE

Still, despite everything that has changed since 1998, Navy leaders have not lost sight of the original goal: To deliver data when it's needed, where it's needed. Everything else should be just a means to that end.

The key? Start with the end in mind and work from there, said Capt. Robert Croxson, program manager in the Navy's Multifunctional Information Distribution System Program Office.

Decision-makers need to take a long-range view of how to build the enterprise so they can deliver the right data when it's needed, he said. For example, that might involve better algorithms, more computing power in the air and more predictive, rather than historical, analysis.

"When I'm in an aircraft and I'm being targeted, I need the data right then and there," said Croxson. "I don't need someone … showing full motion video sucking up the bandwidth. I have to have that data that I need at the right time."

Information warfare also requires a more agile procurement system—one that enables all of the military services to take advantage of new and emerging solutions for moving and displaying information.

"How do you more effectively acquire and get those apps into the fleet and into the hands of the sailors by being a fast follower?" said Steve Soules, executive vice president in Booz Allen's Defense & Intelligence business leading the firm's C4ISR cross-cut cohort initiative along with Navy/Marine Corps C4ISR. "You need an enterprise contract to go with the enterprise testing and acquisition processes."

Underwritten Content

DEFENSESYSTEMS FCW TECHNICAL PARTNER: Booz | Allen | Hamilton

SESSION HIGHLIGHTS

KEYNOTE

REAR ADMIRAL DAVID LEWIS, COMMANDER

Space and Naval Warfare Systems Command

"We are becoming rigorous. We are becoming warfighter centric. We're on the A-Team now. We're one of the top listed domains for warfighting and we need to behave differently as a consequence of this action."

TAKEAWAYS:

- C4I has provided the U.S. with an asymmetric advantage since before World War II, but that is changing with information warfare.
- Until recently information warfare has not been managed as a coherent, well-orchestrated domain, resulting in overburdened networks and communications channels and old equipment.
- Cybersecurity standards must be treated as an integral part of operations at every step in the system lifecycle.

PANEL DISCUSSION

BILL BONWIT

Department Head for the Command and Control (C2) Department of the Space and Naval Warfare (SPAWAR) Systems Center Pacific

"We have to get to the place where we set up a development and integration environment where all the people are developing … and integrating against that same environment on a very regular basis."

TAKEAWAYS:

- Being effective in network-centric warfare means being able to access the information needed and present it in a way that is useful and easy to understand by warfighters.
- We need to take advantage of new technology quickly and it must be easy to use. Engineers strive to reduce the complexity of systems for end users.
- DOD is moving to shared processors, and shared access to the same network and the same data.
- DOD must incentivize enterprise behavior. Don't duplicate services.

GREG SHAFFER

Assistant Chief Engineer, Mission, National Competency Lead ISR/IO

Space and Naval Warfare Systems Command

"We need to stop thinking about building large monolithic, brittle systems. We need to really start thinking about building smaller apps and widgets that let me plug other apps and widgets together."

TAKEAWAYS:

- The data must move very quickly across the network in order to put a weapon on a target. Applications and widgets can be put together to help move data quickly.
- Organizations must understand the lifecycle of data—when it is born and where it needs to go.
- Interoperability happens through driving specifications and standards, providing APIs, and being more rigid in how systems are developed.
- The challenge in C4I is how to drive to enterprise level set of services, and how to build and sustain them.

CAPTAIN ROBERT CROXSON

Program Manager, Multifunctional Information Distribution System, program Office (PMA/PMW-101), U.S. Navy

"When I'm in an aircraft and I'm being targeted, I need the data right then and there. I don't need someone … showing full motion video sucking up the bandwidth. I have to have that data that I need at the right time."

TAKEAWAYS:

- Organizations need to start with the end in mind and work their way back from there.
- The right data must be delivered at the right time to the warfighter. There's a need to prioritize data, encourage interoperability and avoid stovepipes.
- We won't be able to get to the sensor-to-shooter concept unless the Navy gets rid of barriers, some of which are rules of engagement.

STEVE SOULES

Executive Vice President

Lead, Navy/Marine Corps C4ISR

Defense & Intelligence Group

Booz Allen Hamilton

"You need an enterprise contract to go with the enterprise testing and acquisition processes."

TAKEAWAYS:

- In the early days of network-centric warfare, the Navy did not take into account the significance of the cyber threats to its systems.
- Changes in acquisition and contracting are essential to supporting the evolving vision of information warfare.
- One example of information warfare in the Navy: A tactical cloud at sea.

GREG WENZEL

Greg Wenzel

Executive Vice President

Lead, Digital Solutions/C4ISR

Strategic Innovation Group

Booz Allen Hamilton

"We [have to] network ourselves together—we don't want out get 'out-Ubered' by the asymmetric threats."

TAKEAWAYS:

- Being network-centric means there is no center to the network; building systems vertically is no longer a good option.
- Common, standard interfaces and a plug-and-play approach are essential to the present and future of information warfare.
- Interfaces should be defined at the network level, not at the system level.