CHIPS magazine

Summer 2004

Dennis M. Bauman
Program Executive Officer C4I & Space

Dedicated to Sharing Information - Technology - Experience

Department of the Navy Chief Information Officer
Mr. Dave Wennergren

Space & Naval Warfare Systems Command
Rear Admiral Kenneth D. Slaght

Space & Naval Warfare Systems Center Charleston
Commanding Officer
Captain John W. R. Pope III

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Web support by Tony Virata and Bill Bunton
DON IT Umbrella Program.

CHIPS is sponsored by the Department of the Navy Chief Information Officer (DON CIO) and the DON IT Umbrella Program Office, Space & Naval Warfare Systems Center, San Diego, CA.

CHIPS is published quarterly by the Space & Naval Warfare Systems Center, Charleston. USPS 757-910 Periodical postage paid at Norfolk, VA and at additional mailing office. POSTMASTER: Send changes to CHIPS, SSC Charleston, 9456 Fourth Ave., Norfolk, VA 23511-2130.

Submit article ideas to CHIPS editors at chips@navy.mil. We reserve the right to make editorial changes. All articles printed in CHIPS become the sole property of the publisher. Reprint authorization will be granted at the publisher's discretion.

Requests for distribution changes or for other assistance should be directed to Editor, CHIPS, SSC Charleston, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 444-8704; DSN 564. E-mail address: chips@navy.mil; FAX (757) 445-2103; DSN 565. Web address: www.chips.navy.mil.

Features

Page 6

"We're seeing that our C4I systems now are recognized not just as combat support systems but as weapons systems in and of themselves."

Dennis M. Bauman
Program Executive Officer
C4I and Space

Page 10

"… the speed of modern warfare creates a continuum, not a succession of phases."

The Honorable Michael Wynne
Acting Under Secretary of Defense for Acquisition, Technology and Logistics

Page 14

"NMCI is now the largest single network in the world … the second largest is an IBM network (319,000 users) … the third largest is for the United Kingdom government (100,000 users) and the next largest is for General Motors (80,000) …"

The Honorable Gordon R. England
Secretary of the Navy

CHIPS SUMMER 2004

Volume XXII Issue III

4 Editor's Notebook
By Sharon Anderson

5 From the DON CIO
By Dave Wennergren

6 Decision Superiority for the Joint Warfighter - An Interview with Dennis M. Bauman
Program Executive Officer C4I and Space

10 The Opportunities and Challenges of Change
By the Honorable Michael Wynne
Acting Under Secretary of Defense for Acquisition, Technology and Logistics

13 DON IT Umbrella Program Info Alert

14 Why We Need the Navy Marine Corps Intranet
By Sharon Anderson

18 Network Warfare Simulation
By Chris Alspaugh, Tom Hepner, Cam Tran, Ph.D., Wonita Youm, Albert K. Legaspi, Ph.D., Steve Ferenci, Richard Fujimoto, Ph.D., and Myung Choi, Ph.D.

23 DON 2004 eGov Award Winners
By Lynda Pierce

24 Building a Better Information Mousetrap... The Technology eXchange Clearinghouse
By David J. Roberts, DBA

26 Global Technology Watch
By Ronald Neil Kostoff, Ph.D.

28 The SSC San Diego Concept of the Composeable FORCEnet
By the SSC San Diego Composeable FORCEnet Team

30 Can You Hear Me Now?
By the DON CIO Spectrum Team

32 New DoD Enterprise Software Initiative Agreements

33 Communities of Practice Get Underway at Keyport
By Marietta Atwater

34 The PACOM Command Center
By the Space and Naval Warfare Systems Center San Diego Staff

36 The IIDBT Meets the Demands of Modern Warfare with Speed and Accuracy
By Lt. Cmdr. Eric Higgins and Jason Hall

37 DON eBusiness Operations Office Solicits Pilot Project Proposals

38 Capabilities-Based Acquisition ... From Theory to Reality
By Philipp Charles and Lt. Cmdr. Phil Turner

40 IT Sailors, Navy and EDS Reap Benefits of NMCI
By Eric T. Mazzacone

40 NMCI by the Numbers

41 Is It Scuzzy Enough?
By Patrick G. Koehler

43 The Lazy Person's Guide to Mobile Telephony
By Retired Air Force Maj. Dale J. Long

46 Under The Contract
By the DON-IT Umbrella Program Team

Editor's Notebook

The spring issue feature article about Navy Knowledge Online (NKO) drew kudos for the Navy's efforts regarding the NKO from the — Army! Army personnel I spoke with were impressed with the many educational and training; professional development; financial; and healthy lifestyle resources available to NKO users. Army personnel asked if they could use the resources on NKO. An NKO spokesman informed me that the NKO is currently not funded for joint service use.

"Personnel from the other services cannot log on unless they are sponsored as guests. Given the intent of NKO, it is not currently funded for joint service use. Only NKO administrators can provide guest access, which means in special cases, they can manually enter a user profile. Most often guest access is given to contractors who are working on one of our projects. These contractors have a valid need to access NKO because of their participation in the Revolution in Training initiative."

Army personnel cannot use their Army Knowledge Online (AKO) user identification and password to access the NKO at this time nor is accessibility available between the AKO and NKO Web sites.

"While accessibility between AKO and NKO would be an ultimate goal, there are no definite plans at this time."

With all the enthusiasm for NKO you can imagine my chagrin when I found a voice message from Lt. Susan Henson, Public Affairs Officer, Naval Personnel Development Command, telling me that I had used an incorrect URL on the CHIPS Spring 2004 cover (of all places!) for the NKO Web site. The correct URL is https://www.nko.navy.mil. The URL was correct in the remainder of the magazine.

My sincere apologies to the CHIPS readers who were inconvenienced by the error, and to the NKO staff, who work so hard to provide the invaluable career and learning resources on the NKO Web site. I'll never make last minute tweaks to the cover again!

CHIPS was an exhibitor with the DON CIO at the NMCI Industry Symposium, June 20-23 in New Orleans, and we partnered with the Information Professional (IP) Officer Community at TechNet International, May 11-13 in Washington, D.C. It was a pleasure talking with CHIPS readers and exploring topics for future issues. Thank you for your feedback. Our thanks to the DON CIO, NETWARCOM and the IP Officer Community for providing these opportunities.

Welcome new subscribers!

Sharon Anderson

Clockwise left to right, U.S. Senator Conrad Burns (R-MT), SPAWAR Charleston computer scientist, Jerri Baeumel, CHIPS senior editor, Sharon Anderson and the Department of the Navy Chief Information Officer support team: Bob Alderman, Jim Knox, Rob Lewis and Charlie Meyers at the NMCI Industry Symposium.

DON CIO, Dave Wennergren, speaking at the NMCI Industry Symposium.

Below: Rob Lewis and Charlie Meyers.

DON CIO

Putting information to work for our people

Rear Adm. Chuck Munns, who has been selected for promotion to vice admiral, will be leaving his job as director of the Navy Marine Corps Intranet (NMCI) in a couple of months. Our loss in the Department's information technology community will undoubtedly be the fleet's gain as he assumes the post of Commander, Naval Submarine Forces.

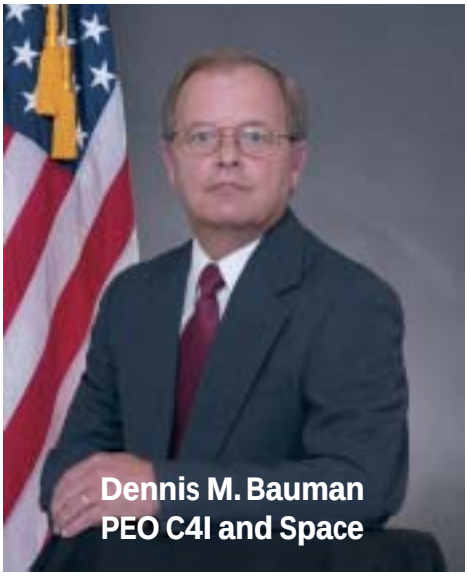
We owe Rear Adm. Munns our thanks. He has worked tirelessly to implement NMCI, the largest intranet in the world and a change management effort of epic proportions. His steady hand, intellect and innovative spirit have turned the tide, and taken this very challenging project to the point of well over 300,000 people using the network daily. As pointed out at the recent NMCI Industry Symposium, NMCI implementation has demonstrably improved access, interoperability, information assurance, failover and redundancy; and innovative new training opportunities are now available to our military personnel.

Despite the progress we have made on NMCI, an incredible amount of work remains to be done to truly achieve the transformational potential that this intranet offers us. Our success will be measured by our ability to devote our energies to solving problems and accelerating the pace of transition. While the cutover of seats is of paramount importance to get our Navy and Marine Corps users into the NMCI collaborative environment, we must not lose focus on shutting down legacy applications and networks. The price of maintaining duplicative systems and infrastructure is an anchor around our neck that must be lifted to achieve our vision of Naval Power 21, knowledge dominance and network-centric warfare. The security achievements of NMCI are noteworthy, but the rapid transition to Public Key Infrastructure (PKI) digital certificates on the Common Access Card for cryptographic log on, access to secure Web sites, and digital signatures, will not only dramatically strengthen our information security posture, but will also be the key that unlocks the power of eGovernment and the elimination of our labor-intensive paper processes.

Each of us has a leadership role to play in this Naval transformation. Let us renew our commitment to provide the network-centric environment that our Sailors and Marines need to fight and win in a world where the flow of the right information to our forces, anywhere in the world, in real time, is crucial. Let us bring to bear the strength of our Naval shore establishment to win the global war on terrorism. Each day spent making NMCI the foundation for this transformation to net-centric operations is a day of success. Any moment spent not working constructively to face and work through the challenges of this daunting transformation is a moment lost to the men and women serving this great nation.

Dave Wennergren

Decision Superiority for the Joint Warfighter


Dennis M. Bauman
PEO C4I and Space

Vision: PEO C4I and Space, whose mission is to acquire, field and support C4I and ground-based space systems, ultimately produces "decision superiority" for the joint warfighter. In the words of its Program Executive Officer, Dennis M. Bauman, "Our job is to implement and to field capability. We turn resources — that is, money and people — into capabilities for the warfighter."

PEO C4I and Space was established in November 2002 and works closely with its organizational partner, the Space and Naval Warfare Systems Command, to dramatically enhance current and future C4I systems. SPAWAR's Office of the Chief Engineer develops the architecture and standards for FORCEnet, the Navy's vision for network- centric warfare. "We in PEO C4I and Space," explains Bauman, "apply these architectures by acquiring, aligning and fielding systems to make this vision a reality."

Bauman, and the 12 program offices he oversees, manage more than 100 acquisition programs and projects that cover all C4I disciplines — applications, networks, communications, intelligence and electronic surveillance systems for both afloat platforms and shore commands. These systems support the Global Information Grid (GIG) development strategy and strengthen operational interoperabillity with allied and coalition partners.

A Snapshot of Dennis Bauman's Service Career

⇒ *U.S. Navy weapons officer and qualified surface warfare officer aboard an amphibious ship*

⇒ *Head of NOSC Submarine Communications and C4I Systems Division (1992-1997)*

⇒ *SPAWAR Program Director for Information Warfare (1997-2000)*

⇒ *SPAWAR Program Director for Command, Control and Intelligence and Combat Support Applications (2000-2002)*

⇒ *Program Executive Officer for C4I and Space (2002 - present)*

⇒ *University of California at San Diego faculty member, Computer Science and Engineering Department (1980-2000)*

⇒ *Member of the Senior Executive Service and the Navy's Acquisitions Professional Community for Program Management*

In a recent interview with CHIPS Magazine, Bauman discussed how his organization delivers "holistic, interoperable C4I solutions across the Navy" and is transforming the Navy's approach to network-centric warfare.

CHIPS: I understand that FORCEnet is an architectural framework, it's not a program of record, and there are no milestones involved. I've heard you talk about the iterations of FORCEnet. Can you explain that?

Bauman: As you said, FORCEnet is an architectural framework. It's how the Navy is going to increase its network-centric warfare capabilities, serving as a forcing function for organizing, planning and investing in the Navy's tactical information architecture and C4I in general.

To reiterate what Rear Admiral Ken Slaght, SPAWAR Commander, has often said — it's an ongoing process rather than a program of record, and it doesn't have a definitive set of milestones. The architecture is built around the Office of the Secretary of Defense's GIG precepts for network-centric warfare. In PEO C4I and Space, we're charged with implementing both the precepts of the GIG architecture and the architectural framework of FORCEnet, defined by SPAWAR's Office of the Chief Engineer. We acquire, align and field the systems that increase the net-centric readiness of our naval platforms.

CHIPS: So could we say that warfighters are using the concept of FORCEnet right now?

Bauman: Absolutely. There are things that happened in Operation Iraqi Freedom (OIF) that I would characterize as early FORCEnet capabilities. C4I used to be considered a combat support system. It's now becoming a weapons system based on how it was used in OIF and Operation Enduring Freedom (OEF).

As an example, a very high percentage of strike planning in OIF was done in chat rooms. Five years ago in a command center you would hear a lot of voice circuits while watch officers planned strikes and coordinated fires. If you went into one of those spaces during OIF you would hear almost no voices. What you would hear is the clattering of keyboards engaged in chat rooms. The implication is an overall increase in the speed in which we can synthesize information about the battlespace, coordinate quickly and act on that information to achieve decision superiority.

In support of a common operational tactical picture and ballistic missile defense in OIF, we fielded a capability on the USS Higgins that was able to take cuing information from its Spy-1 radar and send it near instantaneously to Army Patriot batteries in Kuwait. They used that information to engage inbound Scud missiles.

Let me give you another example. We are fielding a coalition networking capability called CENTRIXS (Combined Enterprise Regional Information Exchange System). Our Navy warfighters often collaborate in network-centric fashion using SIPRNET, but our allies cannot access SIPRNET for security reasons. When we've interoperated with our coalition partners and allies in the past, we weren't able to collaborate via SIPRNET. Therefore, we've produced a separate set of bilateral and multilateral networks called CENTRIXS, and we've rolled them out into the fleet over the past year and a half.

CENTRIXS allows us to network with individual groups, coalition partners and allies, which had a huge impact in OIF and OEF. For the first time, CENTRIXS allowed our coalition partners and allies to leverage some of the same network-centric capabilities that we benefit from.

CHIPS: You mentioned the GIG and how that fits into the FORCEnet concept. Could you expand on that?

Bauman: It's actually the reverse. I would say that FORCEnet fits into the GIG concept. I say that because the GIG is the OSD architecture and vision for the entire Department of Defense for joint network-centric warfare. There are maritime components of that capability that the Navy needs to address. FORCEnet encompasses what the GIG defines and extends it into the maritime realm because Naval forces have unique operational and environmental challenges.

At the strategic level, there are a number of pillars that support GIG development. They are designed to provide a global architecture that is joint in nature. The Navy, through what we're doing in FORCEnet and what we're doing through PEO C4I and Space, is very much involved with developing these strategic pillars. Let me explain the GIG strategic pillars because I think it's important to understand what the GIG is from one level of detail down.

The first one is the Transformational Communications Architecture or TCA, which is a space-based communication architecture to support the high bandwidth Internet Protocol traffic of the future.

The second part is the Bandwidth Expansion part of the GIG, known as the GIG-BE, which brings high data rate connectivity to worldwide bases and facilities.

The third pillar is the Teleports that connect current and future satellite communications architectures with the terrestrial GIG networks.

The fourth pillar, the Joint Tactical Radio System (JTRS), is a very important element. JTRS will provide a family of completely joint and interoperable radios to enable joint tactical voice, data and video communications for mobile military users in the air, on the ground and at sea for the digital battlefield. It is a software programmable and modular radio system with a set of different form factors for the Army, Navy, Marine Corps and Air Force.

JTRS also does routing to enable ad hoc networking in-theater. Let me further explain this ad hoc networking capability. Currently, to get into a Link 16 network, a fighter aircraft has to be part of the planning that set up that architecture days ahead of it being used. With JTRS routing and ad hoc networking capability, a fighter aircraft will be able to fly into an area of operation, and by virtue of the JTRS architecture, be able to come online dynamically. That's a huge advantage, making JTRS much more than just a next generation radio.

The fifth pillar is GIG Enterprise Services (GIG-ES), which is also called Network Centric Enterprise Services. This brings an enterprise perspective to the applications and processes through which information is handled through the architecture. It is an Internet-like, smart-pull services architecture that is provided for application across the GIG.

Another key pillar that becomes more and more important every day is Information Assurance, which protects the network that we're building. We want to be sure we fully protect ourselves as we rely more and more upon this C4I weapons system.

Finally, the DoD push for increased network-centric capability will be Internet Protocol Version 6. It will add security and quality of service for our communications, which vastly increases the addressing architecture and allows us nearly unlimited expansion of our networks.

That is the framework of the GIG and the vision of OSD. FORCEnet uses those same pillars and applies them to the maritime environment. We in PEO C4I and Space apply these architectures by acquiring, aligning and fielding systems to make this vision a reality.

CHIPS: What are the decision-making factors that guide you in buying, building and fielding network-centric warfare systems?

Bauman: Our job is to implement and to field capability. We turn resources — money and people — into capabilities for the warfighter. A few months ago, we put some of our best and brightest together to look at those architectures, to examine where we are today and where we're going in the Program Objective Memorandum for C4I systems. They built what we call our PEO C4I Integrated Roadmap.

"For the first time, CENTRIXS allowed our coalition partners and allies to leverage some of the network-centric capabilities that we benefit from."

They mapped the operational goals of our warfighters, the DoD attributes that I've mentioned as we've talked about the GIG, and they identified three basic characteristics that our Naval platforms need to have in the future. The three characteristics build on each other and are very much interdependent.

The first one is *bandwidth enabled*, which

provides access to the entire network with the ability to rapidly access information with minimal latency. Bandwidth enabled doesn't mean all the bandwidth you want. What it really means is to eliminate bandwidth as a constraint of capability.

The second characteristic is a *service-oriented network architecture,* which allows the ability, flexibility and capacity to access information on the network. It has to be service-oriented, but not stovepiped, as most networks are today.

The third characteristic is *user-centric information systems.* By this we mean systems designed to put the user in the center and allow that user access across disparate applications at various security levels. It allows the user to synthesize information as the user deems appropriate, having consistent data quality from the radar to the common operational picture.

Using this model, we look at each program or effort that's been planned in the past and programmed in the POM to determine if they contribute to one or more of these three characteristics. To what extent does it contribute? Does it follow the architectural precepts of the GIG and FORCEnet? Then we compare the programs based on that lens and determine where we should spend the money in conjunction with the warfighter and the resource sponsor.

That's how we look at programming decisions, with the strategic goals of effectively and efficiently increasing the net-centric warfare capabilities of our Naval platform.

CHIPS: When you're looking at C4I acquisitions, how much do you confer with the other PEOs in the Navy?

Bauman: There is something interesting about PEO C4I and Space that makes us a little different than most other PEOs: The capabilities we implement and field are used across the products that the other PEOs produce. PEO Information Technology and PEO Integrated Warfare are exceptions, but most of the other PEOs are platform centric – subs, ships, carriers, etc.

"There's something interesting about PEO C4I and Space that makes us a little different than most other PEOs: The capabilities we implement and field are used across the products that the other PEOs produce."

We work very closely with the other PEOs because we provide interoperable C4I solutions that fit on the platform, scaled to what the platform needs and seamlessly interoperable across all the platforms. That presents particular challenges and requires us to work very closely with the other PEOs.

One reason why Mr. John Young, the Assistant Secretary of the Navy, Research, Development and Acquisition (ASN (RDA)), formed PEO C4I and Space a year and a half ago was to better align us at a peer level with these other platform PEOs so we could give them more holistic, interoperable C4I solutions across the Navy.

CHIPS: How will the new PEO Space Systems affect your acquisition of C4I capabilities?

Bauman: I'd like to provide clarity about the difference between PEO C4I and Space and the new PEO Space Systems that was recently established (May 2004). The last thing we want to do is create confusion as to why there are two PEOs with "space" in their names. There's a very easy interface between what we do and what PEO Space Systems does. We field the ship- and ground-based terminals that communicate with our space-based systems.

PEO Space Systems produces the on-orbit capability and the ground monitoring and control capability to maneuver and control satellites. So the interface between the two PEOs is between the earth-based terminals, leveraging information from space-based satellites and the space-based satellites themselves. That's where the seam is.

Mr. Young, Rear Admiral Rand Fisher, Program Executive Officer for Space Systems, and I discussed where we should draw the line. Should it be in that gap between space-based systems and the terminals on the ground or should the terminals be included in Space Systems?

We decided that the interface was a lot cleaner between the terminals and the spacecraft than it would be between the terminals and the remainder of the C4I systems. The rationale has to do with a complex interface between satellite terminals and ground stations and the networks that they connect with.

PEO Space Systems represents the Navy's efforts to streamline space acquisitions management. It is the PD 14/PMW 146 (Navy Communications Satellite Program Office) part of SPAWAR that has now been realigned into a PEO. The difference is that the program manager reports directly to the PEO, who, in turn, reports directly to ASN RDA without anyone in between.

I share spaces with PMW 146 in San Diego — I'm actually collocated with them in our SPAWAR facility — and we will continue the close interface we had when it was PD 14.

CHIPS: It's easier to interoperate when systems are "born joint." How do you further that goal?

Bauman: We're involved with the other Services in some transformational examples of born joint. We've talked about JTRS, which is a great example. JTRS has clusters. The Navy used to have Cluster 3, which was maritime fixed, both afloat and ashore. There was a Cluster 4, which was airborne and developed by the Air Force. We recently combined those to form JTRS AMF, which stands for airborne, maritime, fixed. We now have a programmatic partnership between the Navy and the Air Force with the respective clusters.

It's a common acquisition approach with one contract to develop both the maritime-fixed and the airborne aspects. The program management structure is unique. An Air Force colonel is the current program manager, I am the program executive officer, and the Service acquisition executive is from the Air Force.

We're going to rotate this structure over time, so here's an example of how we are building JTRS with software waveform supplied by a joint program office. We're also joining with the Air Force to make sure that we are even more interoperable in the tactical and the maritime fixed environments.

Another example is the Common Link Integration Processing capability. It provides a tactical networking and gateway capability between JTRS waveforms and legacy tactical data links, including Link 16, Link 11, Link 22, Enhanced Position Location and Reporting System, and Joint Range Extension.

This program is also a joint Air Force and Navy program between PEO C4I and Space and the Air Force Electronic Systems Center (ESC) Hanscom, with PEO C4I and Space providing acquisition and contracting lead. The Army is monitoring the effort and may soon join as a full member.

We have another effort underway with the Air Force called NESI, or Net-centric Enterprise Solutions for Interoperability. It's a joint initiative to further interoperability and commonality. This collaboration is aimed at defining software application development standards to be followed, at a minimum, by Navy and Air Force command and control and C4I programs.

The present work by PEO C4I and Space, ESC Hanscom and SPAWAR to implement NESI are consistent with the GIG-ES. We are also engaging the Army to ensure consistency of effort across the Services. So, we have many efforts underway to make sure that programs are born joint, and we're using a lot of these standards when we make significant upgrades to existing legacy systems to make them more joint.

CHIPS: The "plug and play" or "plug and fight" concept is supposed to shorten the decision cycle for the battle force commander. What are some of the capabilities using this concept?

Bauman: This concept is centered on how warfighters are going to access needed information quickly and efficiently to obtain decision superiority. It is intended to span the entire tactical spectrum from the strike group commander down to the unit ships and Marine battalions in the field.

Netcentricity greatly increases the availability of information, and it recognizes that users best define their information sources and determine what they need operationally and when they need it.

Tactical information under this concept is pulled off the network instead of having the warfighter sift through myriad data sources. We call that concept smart pull, which means that information is gathered in a way defined by the warfighter. The cycle time of information gathering is in seconds, the infrastructure is interoperable, the networks are robust, the bandwidth is available and secure, and information security and support protection are in place.

The result is a warrior, out on the tip of the spear, who is able to access critical information at the right time with an acceptable latency. OIF and OEF gave the warfighter just a taste of this network-centric capability. Naval forces, in particular C4I systems in those conflicts, catalyzed a faster and more efficient planning mechanism that helped us deliver the chat room-planned lethal fires that I explained previously. It was at a pace unmatched compared with any other conflict.

We're seeing that our C4I systems now are recognized not just as combat support systems but as weapons systems in and of themselves. C4I is fundamentally part of how the warfighter fights. It's integrated into virtually every weapon we use — our command and control systems, our precision guided munitions, our unmanned aerial vehicles — and it really gives us the ability to marshal assets on the fly to get the job done.

"We're seeing that our C4I systems now are recognized not just as combat support systems but as weapons systems in and of themselves."

It's not the weapons or the platforms but the C4I systems that are the common connection points. C4I systems are transforming the way we approach warfare, and that's what network-centric warfare is all about.

For more information about the Program Executive Officer C4I and Space, go to the SPAWAR Web site at http://www.spawar.navy.mil, and click on the PEO C4I and Space seal.

Editor's Note: For more information on the FORCEnet concept, go to page 28 for an article on the Composeable FORCEnet by SPAWAR Systems Center San Diego.

The Opportunities and Challenges of Change

By the Honorable Michael Wynne
Acting Under Secretary of Defense for Acquisition, Technology and Logistics

Wynne was sworn in as the Deputy Under Secretary of Defense (AT&L) on July 17, 2001. He also served as the Principal Deputy to the Under Secretary of Defense for Acquisition, Technology & Logistics. In 1999, Mr. Wynne retired as Senior Vice President from General Dynamics, where his role was in International Development and Strategy. He spent 23 years with General Dynamics in various senior positions with aircraft (F-16), main battle tanks (M1A2), and space launch vehicles (Atlas and Centaur). He also spent three years with Lockheed Martin, having sold the Space Systems Division to [then] Martin Marietta. He integrated the division into the Astronautics Company and became the general manager of the Space Launch Systems segment, combining the Titan with the Atlas Launch vehicles. Prior to joining industry, Wynne served in the Air Force for seven years, leaving active duty as a captain and assistant professor of astronautics at the U.S. Air Force Academy teaching control theory and fire control techniques. Wynne graduated from the U.S. Military Academy and holds a master's degree in electrical engineering from the Air Force Institute of Technology and a master's degree in business from the University of Colorado.

Acting Under Secretary Wynne's article has been edited from his remarks at AFCEA TechNet International 2004, May 13.

One hundred years ago, the U.S. Army was engaged in a controversial, protracted, irregular war, in a distant land, against insurgent opponents in the Mindanao phase of the Philippine Insurrection. Our military forces were small, composed of volunteers and service professionals. Because of inadequate planning and the stress on forces supporting global expeditionary operations, the military departments began to transform to fight in what we now call Industrial Age warfare.

We got that transformation right — eventually. June 2004 marks 60 years since the landings in Normandy; arguably the largest joint military operation ever attempted — and we did it while simultaneously executing sizable joint amphibious attacks in the Mariana Islands. We proved supremely adept at fighting Industrial Age warfare. Through its practice we defeated two powerful rivals, secured the safety and prosperity of our own country and those of our allies, and had the means to face down another superpower for over 40 years.

Because the long view in Washington seldom extends past the beginning of an administration, it is tempting to view our current transformation through the lens of the last two years — that is, through our campaigns in Afghanistan and Iraq, each fought with unprecedented, unorthodox methods that highlight not only the superb courage, flexibility and skill of our forces, but the extraordinary technology that we employ in taking the fight to our enemies. Transformation is not unique to our time, it isn't something that happens overnight, and it doesn't happen all by itself. We have to decide, we have to act, and we have to manage our choices.

Current DoD Transformation Efforts

The goal of our current transformation is to enable us to fight war on our terms, which our Director of Transformation, retired Navy Adm. Art Cebrowski, says will mean trading industrial mass for information technology. This is not a matter of simply changing one form of war for another; it's about developing the determination and the capability to change; not once or twice — but as the situation demands. As Art says, "If you are not making any big bets; you are a fixed strategic target and at risk."

One big bet we are making is on network-centric operations. We see this as a path to ensure sustained competitive advantage, and to create new competitive areas — both imperatives if you are serious about creating and sustaining change. On the acquisition side, this means decreasing cycle times and managing the devolution of "sunset" capabilities and processes. It means we are serious about spiral development and about reinvigorating the lost art of system of systems engineering.

Network-centric operations require us to field new kinds of forces. We understand now that the speed of modern warfare creates a continuum, not a succession of phases. Our forces will have to be more expeditionary (lighter, more lethal); capable of precision engagement; able to leverage persistent ISR [intelligence, surveillance and reconnaissance]; with tighter sensor-shooter times, and with expanded unmanned capabilities: Unmanned Aerial Vehicle (UAV); Unmanned Combat Air Vehicle (UCAV); Unmanned Undersea Vehicle (UUV); and robotics.

It's obvious that none of these changes will happen overnight; it's less obvious that we have been struggling with these changes for a generation. At least as far back as the comparatively small, short-legged expedition to Grenada in 1983, we've known where the deficiencies in command and control, battle management and joint operations are. We have exhaustively studied them, then responded with robust management, mind-boggling acronyms, elaborate codification of technical language, long-term commitments to programs and, of course, money. Our command and control bill for the Department continues to grow and is currently at the level of tens of billions of dollars in the POM (Program Objective Memorandum).

During the campaign in Afghanistan, special operations ground controllers needed to tailor the target location data they were sending based on the kind of aircraft that was going to drop the ordnance because different planes take different formats. This is a digital, information age variation of Army and Marine radios that couldn't "net" in Korea or Grenada, or of the incompatible Air Tasking Order formats used by the Air Force and Navy during Operation Desert Storm. The guy on the ground shouldn't have to sort out who it is that is sending help before he can ask for it.

If we are not careful, we are in danger of proliferating the command and control gaps that we identified during our transformation to Industrial Age warfare with the speed and efficiency of Information Age systems. While we clearly are in a different era of technology, it is far more important to recognize we are in a different era of national security, with dangerous and immediate threats that demand innovation, practical, near-term responses and efficient resourcing.

Joint Battle Management

I can think of no more critical need than the development and fielding of a joint battle management capability; I see JBMC2 (Joint Interoperability and Integration and Joint Battle Management Command and Control) as not only the path forward, in terms of capability but also as a test case for system of systems acquisition. A key objective is to provide robust capabilities and innovative approaches for the full spectrum of potential missions using a system of systems approach. This approach to acquisition identifies interdependencies between systems that are related or connected.

We need a joint "plug and play network" that is self-organizing and built using a mission execution-focused approach. Our future theater C2 structure must ensure that all U.S. and allied forces can act as a unified force. The goal should be to enable the rapid employment of inherently-joint force modules that can operate together en route to and within the theater of war, without extended "shakeout" periods or train-up times. A major initiative we have to improve for the joint warfighter is our JBMC2 Roadmap. The roadmap guides both material and non-material aspects of approximately $47 billion worth of programs within the Department.

The standard for a battle management architecture is deceptively simple, for example: A Navy pilot flying off an aircraft carrier on a strike mission to support a ground force ashore needs to move through and see a common maritime picture while seeing a real-time common air picture. This, among other things, will give updates on the enemy's integrated air defense envelope, then move seamlessly to a common ground picture that will enable a precision strike on precisely the right target ashore — AND — update target effects to determine if a re-attack is necessary.

The Army guy on the ground, who nominated the target, needs to be confident that his sight picture is being sent to that Navy pilot, and that it is being transmitted accurately to the ordnance. And as the guy who called for the strike, he has to know if the results are successful. *Seamlessly — without workarounds, air gaps, data collision or multiple headquarters and command centers managing the mission.*

Think of what we have right now in our information gathering arsenal: JSTARS (Joint Surveillance and Target Attack Radar System) and Rivet Joint; U-2s, Global Hawks, Predators, imagery of every conceivable kind – hyperspectral and infrared; Synthetic Aperture Radar; Humint, Sigint, Masint (Human Intelligence, Signal Intelligence, Measurement and Signatures Intelligence) and; the combat reports of all those dust-covered military personnel reporting over a list of different communications paths as long as my arm.

> We understand now that the speed of modern warfare creates a continuum, not a succession of phases.

The questions are:
Will all the information generated by all those systems be available to a unit leader at the platoon or even squad level, to pilots, to logisticians supporting a fast-paced fight or ship captains at sea, providing offshore fires or defeating interdiction threats; and will that information be clear, unambiguous, continuous and reliable?

Other Opportunities

Metrification of the Littorals: The concept of littoral warfare continues to be studied and the expectation for a minimal amount of situational awareness accepted. A key concept within littoral warfare is what I call "metrification" of the littorals, where we would know every square meter, if you will, of a given area or region and have the ability to track all passage through that region. There are a finite number of littoral areas where offensive or defensive operations might occur. Many lie just off the coast of America and some off other continental shelves. This finite list would naturally include the major harbor areas for our shores and some estuaries that the military uses. In the case of our partners, there may be a similar concern and perhaps a larger program envisioned.

The concept of metrification of the littorals would place measuring devices in a lattice work design across this littoral space, making certain that there would be no traffic that could traverse that space without surveillance. The measuring devices would be similar in fashion to the SOSUS (Sound Surveillance System) devices used to good advantage in the Cold War but at an enhanced level of sophistication. This system could be coupled for defensive or offensive operations with other sensors to prepare the battlefield, though it may be covered with water.

At least within our national littorals, this system could be coupled with a form of RFID (Radio Frequency Identification) tagging, with readers being hosted by the buoy system, basically registering both inbound and outbound traffic. When coupled with tagging technology and the current buoy system for channel control, positive control for all the approaches to our coastline could be established, and offensive operations could be made

far easier with this underwater equivalent to C4ISR. In an offensive situation, there might be available differing sensor arrays that could provide confirmation to complete the ISR picture. Thus, the lattice work would provide baseline information for an area, and on-call sensors could provide the rest.

Metrification of High Threat Areas: We have a potential contemporary case study in the six-mile distance between Baghdad International Airport and the city itself. As you know, that stretch of road has proven deadly to our Soldiers. What if we could bring an integrated, networked body of information capabilities to the periodically deadly short stretches? We might be able to parse that one mile down to several increments of several hundred yards. Perhaps we could then parse each of those increments down even further so that we could eventually monitor, anticipate and control each increment efficiently and reliably. But this cannot happen until we press coordinated and integrated signals, combined with fused imagery and human intelligence information to our lowest command levels.

This kind of approach, along with the hard experience of recent military operations, underscores our need to dominate the electromagnetic spectrum — whether it is for protection purposes such as defeating IEDs (Improvised Explosive Devices), or for information warfare purposes to deny enemy situational awareness and disrupt command and control — at the same time protecting our own sensors and networks.

The importance of information operations and electronic warfare has been especially apparent in Afghanistan and Iraq. The combined use of kinetic and non-kinetic attacks yielded a pace of operations unmatched by our adversaries. The Department is investing in many promising electronic warfare initiatives to achieve spectrum dominance. We are working to enhance electronic warfare capabilities to provide robust non-kinetic solutions to the warfighter where kinetic effects are undesirable or our rules of engagement dictate non-kinetic actions.

Sense and Respond Logistics: There is a revolution in supply chain management in the private sector: smart tags, real-time links from inventory to production and anticipatory restocking. Our vision for the logistics officer of the future is that he or she will be the commander's combat power manager. At the logistics officer's fingertips will be the precise account of how much combat power (expressed in combat systems, munitions, fuels, replacement stocks) is at hand, and how much will be expended over a given course of action.

This capability is technologically feasible; the Department is looking for a company that can deliver it to us. This is a fertile area, and could use some smart thinking. It is one of the cornerstones of an agile force. Trust in replenishment is as important as trust in indirect fire support.

Challenges

Here's something that keeps me up at night: I fear that each time the Secretary of Defense sees one of those gee-whiz, lightning bolt charts, regardless of whether it's from the Services, the Joint Staff, a unified command or OSD, he really thinks we can do all that stuff. Those charts should force us to think: How many systems do we need? How do we control configuration? Who becomes the central arbiter for canceling the money for redundant systems, and demanding that all the Services and battlefield agencies use common solutions?

Another concern: It's obvious by now that software is the crucial component here, but why is it that software projects are routinely managed so poorly? Where are the systems engineers and the discipline of tools first, product second? Where is it written that software manufacturers do it right the first time and need no discipline and no help? Perhaps it is the culture of speed to market, but we have 13.5 million lines of code for the Future Combat System and 15 million for the Joint Strike Fighter. Frankly, the standard rules of configuration control, requirements flowdown and agreed to content aren't being enforced.

A final, most important concern is changing the culture of power over information. It is no longer enough that flag officers and their staffs have access to the knowledge we can now gather. Information needs to be routinely available, useful and transferable among the squad leaders, helicopter pilots and special operations teams. And it must be accurate, comprehensive, integrated, networked, unambiguous, consistent and reliable. All levels of warfighters must be able to track and engage the enemy remotely. Decision and engagement cycles must be compressed even further. And logistics must complement, not impede, this new pace.

These are fundamentally cultural, not technical, challenges. If we cannot overcome our own cultural barriers, our technical prowess and skill will be wasted. I don't mean to suggest these barriers are malicious obstacles placed deliberately in our path by our predecessors. Face it: Today's tough problems come from yesterday's brilliant solutions. When current culture is no longer useful in solving urgent problems, then we have a professional obligation to change it.

Future electronic warfare systems and sensors should be flexible and enable rapid reprogramming to extend the basic capabilities. They should use common modular components and software to field a common capability on multiple platforms. All of these developments point toward our vision of a lighter footprint, and smaller forces working jointly. The perfect example is trusted fires: A unit in contact calling for help doesn't care what Service or system provides the fire, but it has to trust it will arrive on time, on target.

Whatever networked force we build has to work for both a young infantry captain on the ground and the grizzled ship captain at sea — it has to be accepted, employed and trusted culturally to be effective operationally.

My thoughts have been about change and transformation; there's no let up in the volume or frequency in cries for change. Change is both risk and opportunity. Think differently first, then address change to make it happen. It isn't easy. As Thomas Edison put it, many good opportunities go unnoticed because they show up in overalls and look like work. ▭

DON IT Umbrella Program Info Alert

A reminder to Department of Defense personnel that no-cost, downloadable antivirus software is available to DoD users for home use. Antivirus software that provides multilayered protection at the desktop, server, gateway and network levels is available for home computers.

Licenses extend beyond protecting desktops, servers, gateways and networks. Products are available for home computers, home and office firewalls, and wireless or Personal Digital Assistants (PDAs). By expanding products to home use, the DoD acknowledges that safeguarding home computers is as important as safeguarding computers in the workplace.

The license includes enhanced management/system administration tools, as well as global enterprise technical support. And most importantly, these products are provided at no additional cost to the government. However, please be aware that there is a cost associated with some upscale options. These products are available at a special DoD-negotiated price.

All Combatant Commands, Services, DoD agencies and military academies; DoD personnel within joint, NATO and coalition forces; DoD contractors authorized to use government-furnished equipment; and the Coast Guard are authorized to download and use this software. The savings to the Defense Department and the taxpayer are in the tens of millions of dollars, and protection extends to more than 3 million DoD users worldwide.

The software is offered through a fully funded and centrally purchased software enterprise license under the DoD Enterprise Software Initiative (ESI). Through ESI, a variety of software is available for free download to all DoD users who have a .mil Internet Protocol (IP) address.

These licenses provide the latest generation of antivirus technologies and capabilities as well as multilayered protection with "best-of-breed" combinations of software. The multilayered protection strategy is also known as "Defense in Depth."

The key element of this strategy is to implement a variety of products that provide protection at different levels within a network so a single point of failure is not created should a software vulnerability arise. The advantage is that this strategy minimizes the chance of a vulnerability in one product compromising the overall integrity and operability of the entire network.

Antivirus software available for download includes McAfee, Symantec and Trend Micro products. These products can be downloaded by linking to either of the following Web sites.

NIPRNET site: http://www.cert.mil/antivirus/antivirus_index.htm

SIPRNET site: http://www.cert.smil.mil/antivirus/antivirus_index.htm

Although product documentation is also available for download, please contact DISA's DoD-CERT AntiVirus Team if you have questions about a product's installation or use. The AntiVirus Team can also help if you have problems downloading the software. Be advised that all products may not be interoperable. For example, if you install a personal firewall from Symantec and an antivirus product from McAfee, your system may generate errors.

Additionally, users are required to renew software use each year by entering a key code, which can be secured by contacting the AntiVirus Team. The AntiVirus Team can be reached by e-mail at virus@cert.mil or by phone at (703) 607-6500, DSN 327 or 1-800-357-4231.

For more information about the Enterprise Software Initiative, please visit the ESI Web site at http://www.don-imit.navy.mil/esi/ or contact your Software Product Manager via the DON IT Umbrella Web site at http://www.it-umbrella.navy.mil/ or ITEC Direct at http://www.itec-direct.navy.mil/.

New Umbrella Contract Added ERP Systems Integration Services

Enterprise Resource Planning (ERP) systems integration services provides the procurement of configuration, integration, installation, data conversion, training, testing, object development, interface development, business process reengineering, project management, risk management, quality assurance and other professional services for COTS software implementations.

Ordering under the BPAs is decentralized and open to all DoD activities. The BPAs offer GSA discounts from 10 to 20 percent. Firm fixed prices and performance-based contracting approaches are provided to facilitate more efficient buying for systems integration services. Five BPAs were competitively established against the GSA Schedule. Task orders must be competed among the five BPA holders in accordance with DFARS 208.404-70 and Section C.1.1 of the BPA. Acquisition strategies at the task order level should consider that Section 803 of the National Defense Authorization Act for 2002 requirements were satisfied by the BPA competition.

Go to page 48 or the Web links below for more information.

Web link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_services/erp-esi.shtml/.

Web sites to remember:

DON IT Umbrella Program: http://www.it-umbrella.navy.mil

ITEC Direct: http://www.itec-direct.navy.mil

Why We Need the Navy Marine Corps Intranet

By Sharon Anderson

Rear Adm. Munns, Director NMCI and the Secretary of the Navy, the Honorable Gordon R. England.

Lt. Gen. Edward Hanlon, Commanding General, Marine Corps Combat Development Command and Deputy Commandant for Combat Development.

Dave Wennergren, Department of the Navy Chief Information Officer.

New Orleans was hot June 20-23, but it just wasn't the temperatures, the 2004 NMCI Industry Symposium, a forum for Department of the Navy (DON) leadership, users and industry to candidly discuss the successes and friction points of the five-year NMCI program, raised the definition of "inspired leadership" and "interested users" up a few degrees.

During the two and half-day gathering, discussion centered on NMCI challenges, solutions and progress. Rear Adm. Chuck Munns, NMCI Director, who has been tireless in his dedication to ensure the success of NMCI, emphasized the importance of working through NMCI performance issues to harvest the benefits of NMCI's capabilities.

"NMCI is not just an e-mail system; it will provide a warfighting advantage and reach-back capability that the Navy never had before," said Rear Adm. Munns.

Populating the NMCI with capabilities is the essential next step in fulfilling the vision of an enterprise network serving the needs of the DON. But first the completion of the rollout of the more than 400,000 seats is a top priority.

Lt. Gen. Edward Hanlon, Commanding General, Marine Corps Combat Development Command and Deputy Commandant for Combat Development, acknowledged the enormity of the task at hand, but expressed his disappointment that seat rollout for the Marine Corps was not going as quickly as anticipated.

Hanlon explained the Marine Corps' initial frustration a year ago in having to dismantle the Marine Corps enterprise network, a fully functional and dependable system to move to the NMCI.

"Our network had a reputation for secure, effective and responsive service. But, we also recognized that NMCI was a transformational effort …"

"NMCI implementation is a huge job, and it's going to present us with challenges. I've talked about friction in the implementation process, and I know that can come across as a strictly negative message. But I don't think about it like that, and you shouldn't either," said Hanlon.

"One of the colonels on my staff said something to me the other day that I'd like to quote," continued Hanlon, "'Without friction, there can be no traction.' That's a very insightful statement, and I think that it can be applied to any undertaking of the complexity and magnitude of NMCI."

Hanlon pledged the Marine Corps' commitment to the success of NMCI and belief in its advantages, "In fact, we're counting on it as a critical enabler — foundation if you will — of our process of transformation."

Vice Adm. Patricia Tracey, Director Navy Staff, who also heads up the Functional Area Manager (FAM) process to reduce the number of Navy applications and ensure their compatibility within the NMCI; and Rear Adm. Anthony Lengerich, Vice Commander, Naval Sea Systems Command, also outlined their concerns with NMCI performance as well as its successes.

Vice Adm. Tracey said EDS, prime contractor for the NMCI, was superb in relocating the Navy's Operations Center to the Navy Annex when the center was destroyed during the 9-11 attack on the Pentagon. In 24 hours the Navy was back in business due to the decisive action of the EDS Information Strike Force.

"We need NMCI," said Vice Adm. Tracey.

DON leadership encouraged industry to seek enterprise solutions for the Navy's network-centric environment. Rear Adm. Lengerich said that if an industry proposal cannot operate within the security and structure of NMCI, "I'm not particularly interested in it."

"The Navy must have 21st century business processes, and NMCI is the path."

In his remarks, Dave Wennergren, Department of the Navy Chief Information

Officer (DON CIO), addressed the need for industry and the DON to work as a team for matching requirements with enterprise solutions.

"Our greatest strength is in our partnership together — industry and government. Many of the tools that industry has developed for the Navy have been used for the entire federal government. So if you have more ideas, more tools, let us know."

Mr. Wennergren also stressed the importance of aligning Navy's efforts to find solutions that will benefit the larger Navy-Marine Corps Team. "We must align to an enterprise view. We can no longer afford to build duplicative local area solutions. Instead, we must find the best set of commercial solutions that will optimize operational effectiveness and deliver the transformation of our warfighting and business systems."

Wennergren closed with suggestions on how to successfully work as cross-organizational teams to break through the cultural change barriers that face the Navy and offered the tools below as some information resources.

√ *Execution: The Discipline of Getting Things Done by Larry Bossidy and Ram Charan*

√ *Leadership Is An Art by Max DePrees*

√ *Leading Minds: An Anatomy of Leadership by Howard Gardner*

√ *Empowerment Takes More than a Minute by Ken Blanchard, John P. Carlos and Alan Randolph*

√ *The Department of the Navy Chief Information Officer Information Management/ Information Technology Strategic Plan*

The Secretary of the Navy, the Honorable Gordon England, forcefully expressed his support of the NMCI in his address, "I believe in and support this program.... I have made every effort to make sure it survives and thrives .... It's too important not to."

The secretary emphasized that NMCI is much more than hardware, an e-mail system or large-scale network.

"I want to dispel a rumor … one of the complaints I hear about NMCI from Naval constituents is that they can get the same thing at Best Buy or Circuit City for less. They can't," continued Secretary England.

"NMCI buys everything behind the user's PC. Investments that EDS was required to provide to engineer a complete IT service to the Department — local area networks, wide area networks, guaranteed network performance, security, all network support, all help desk support, training, user satisfaction, etc., — are all covered under NMCI."

"NMCI is now the largest single network in the world … only the Internet itself has more users than NMCI."

"This was simply not the case with our legacy networks. All of that investment has to perform to the service levels specified in the contract … or we don't pay the full cost," explained Secretary England.

The secretary talked about NMCI progress, which he is closely monitoring. This includes four NMCI Network Operation Centers (NOCs) up and running, 27 unclassified server farms and six classified server farms — all designed to keep the Department operating through fires, floods, blackouts, hurricanes and unplanned deployments.

There are currently about 360,000 users online with over 55 percent cut over to the desired end state.

"NMCI is now the largest single network in the world … the second largest is an IBM network (319,000 users) … the third largest is for the United Kingdom government (100,000 users) and the next largest is for General Motors (80,000 users; also supported by EDS)," said England.

"In fact, only the Internet itself has more users than NMCI."

The secretary pointed to the Department's achievement in eliminating approximately 90,000 duplicative and costly stovepipe-legacy applications. The Department estimates the current number at less than 10,000.

"The NMCI effort has focused us on our applications and pushed us to a much needed reduction of applications — a 90 percent reduction."

Secretary England talked about what the numbers signify, "… these numbers really mean that we are fundamentally changing the way we think about IT in the Department. We now talk about numbers — things that we can measure and compare; means by which we can gauge progress and assess our efforts against our aims."

"Prior to NMCI, the Navy's IT environment was severely challenged …. We had basically 28 separate commands budgeting, developing, licensing and operating IT autonomously. It was inefficient and from the larger Department perspective, produced results that were far from optimal."

"NMCI allows the Department to focus its energy where it is most needed — on war fighting — not desktop information technology. One of the things we discovered is that we were not very good at accounting for IT costs before NMCI. We often didn't even break out IT costs separately; rather, they were included in line item costs. They were generally not accounted for in the IT budget or even known by the claimant budget and chief information officers."

"No chief executive officer in business could afford this situation and the Department could no longer afford it either," stressed England.

Locking down network security was another factor which led to the NMCI enterprise solution.

"One of the most pressing areas that needed attention was security. It wasn't just that we weren't following our own rules; in many cases we weren't even aware of them," said England.

"For example, every Department of

Above left to right: Founding Fathers panel: Dr. Lee H. Buchanan III, Mr. Charlie Nemfakos, Mr. Dan Porter, retired Adm. Archie Clemins, Mr. Joseph Cipriano, retired Marine Col. Dave Litchfield and (not pictured) William Ryzewic. Left: Retired Adm. Clemins and Dan Porter.

Defense (DoD) network is supposed to do something called DITSCAP or the DoD Information Technology Security Certification and Accreditation Process, a process by which a command certifies that the applications on its network have been certified and accredited for use on the network. This policy has been in place since 1997 — well before NMCI came into being."

"When the Naval Audit Service measured compliance with this requirement … on some of our legacy networks, the results were not good. One major command's compliance rate was in the single digits. And those results were just for the applications that the Audit Service could find."

"The lack of security was probably the most deficient aspect of our legacy networks. Our legacy IT was insecure because we bought it and built it that way."

"NMCI is fixing this problem," said England, "it's taking time, money and people … and sometimes our users don't like the compromises that security requires, but security is paramount. In short, NMCI is replacing our disparate, costly, inefficient shore-based networks and providing a worldwide reach-back capability to deployed operational forces."

Secretary England acknowledged the struggles with the NMCI deployment schedule saying that initial projections were much too optimistic because both EDS and the DON did not fully understand the complexity of the task to be accomplished, but he also noted that NMCI is one of the few systems of its kind that actually started with a design, a plan and a schedule of what needed to be done.

"Before NMCI, the Department of the Navy did not schedule our networks … rather, we grew them. There's a huge difference. In the past, someone started a network and then added on a capability as technology, funding and the situation allowed. Some of our organizations did a pretty good job in growing their networks, but most did not have the resources," said England.

"Putting together the NMCI contract was not only a groundbreaking move — it was the right move …"

Commenting on some of the financial setbacks that EDS has experienced, the secretary stated that the Navy and EDS are in a "committed partnership" to ensure the success of the NMCI.

"Today, the DON is paying 85 percent of the seat price. Obviously, EDS is anxious to receive 100 percent and we are just as anxious for them to achieve this goal. It is in the interest of EDS — and the Department of the Navy to complete this basic task as soon as possible. For the contractor, it's financially important and for the Navy, it's operationally important," said England.

A highlight of the symposium was a panel discussion by the *Founding Fathers* — some members of the leadership group who envisioned the NMCI concept and nurtured it through its early stages. Panelists included former Commander in Chief, U.S. Pacific Fleet, retired Adm. Archie Clemins, who acted as moderator; former Assistant Secretary of the Navy for Research, Development and Acquisition, Dr. Lee H. Buchanan III; former Program Executive Officer for Information Technology, Joseph Cipriano; former Deputy PEO-IT and Director of NMCI Services, retired Marine Col. Dave Litchfield; former Senior Civilian Official, Financial Management and Comptroller Department of the Navy, Charlie Nemfakos; former DON CIO, Dan Porter; and Executive Director for Fleet Maintenance U.S. Pacific Fleet, William Ryzewic.

Retracing the steps that led to the NMCI, panelists discussed the $8 billion dollar shortfall the Navy was facing in FY 2000 in providing IT services to ashore users. The

shortfall actually acted as a catalyst to the NMCI contract vision.

Dr. Buchanan and Charlie Nemfakos said executive leadership had already discussed outsourcing IT services as the only way the Department could go to reduce costs, get a handle on IT spending — and provide a secure enterprise network.

"Putting together the NMCI contract was not only a groundbreaking move — it was the right move for the Navy," said Buchanan.

Mr. Cipriano spent three months investigating industry alternatives for outsourcing network services because there was not a government contract model with the scope and complexity of the NMCI.

"When I talked with IBM executives about how they outsourced this service, they cautioned me that the first two or three years would be hard for users, and that users would not be happy. But they also said that after those first difficult years everyone would be very glad we went this route," said Cipriano.

Mr. Porter commented that the security vulnerabilities discovered during the Department's cleanup of the Y2K bug were alarming. "Command compliance was sketchy at best," said Porter. "The security benefits of the NMCI alone are worth the investment."

The NMCI contract includes about 240 service level agreements (SLAs), specific tasks and levels of performance that prime contractor EDS must execute in order to receive payment.

Rear Adm. Munns announced that the Navy has been working for the last two and half months to reduce the total number of SLAs, some of which were ambiguously defined and difficult to measure.

"We are going to have fewer SLAs, but they are going to have a greater effect and be more measurable," said Navy Capt. Chris Christopher, Deputy Director for Future Operations, Communications and Business Initiatives, NMCI.

The symposium was also an opportunity to recognize outstanding individuals and organizations who have championed the success of the NMCI project. Rear Adm. Munns recognized winners at the 2004 NMCI Excellence Awards Reception.

Rear Adm. Mike Sharp, ASN (RD&A) Chief Engineer and SPAWAR Vice Commander, with Sarah Lamade, SPAWAR CIO, accepting the NMCI Spirit Award presented to SPAWAR and to commands whose transition to NMCI best captures the fundamental spirit of the NMCI partnership between industry and the DON.

Attendees applauded Department leadership's commitment to resolve NMCI problems, expressed relief that their frustrations with performance issues were being heard — and gained a deeper understanding of the NMCI advantage.

Jerri Baeumel, a computer scientist and new hire under the SPAWAR Systems Center Charleston New Professionals Program, was among those who said that they had not fully understood the significance of what the NMCI means to the Navy until attending the symposium.

"I have never heard what the NMCI will really do once fully deployed or how important it is to the Navy explained so well. I learned so much; I wish more people could have heard Secretary England and the other speakers talk about all the capabilities that the NMCI will provide and how urgently they are needed."

"I think people could quickly get over the temporary inconveniences if they understood the long-term benefits of what the NMCI will do for the Navy," said Baeumel.

For more information regarding the symposium and the NMCI, go to the NMCI Web site at http://www.nmci.navy.mil/.

Ms. Anderson is the CHIPS senior editor. She can be reached at chips@navy.mil.

Lt. Antonio J. Scurlock, NNSOC Detachment Ford Island, accepting the NMCI Leadership Award from Rear Adm. Munns. The award was presented to individuals who have shown extraordinary levels of commitment to the success of NMCI. Recipients contributed through improving morale surrounding transition to NMCI.

Capt. Peggy Feldman, Commander SPAWAR Information Technology Center, accepting the NMCI Command Achievement Award from Rear Adm. Munns. The award was presented to bases or commands whose transition to NMCI created notable and significant benefits to the DON .

NETWORK WARFARE SIMULATION

By Chris Alspaugh, Tom Hepner, Cam Tran, Ph.D., Wonita Youm, Albert K. Legaspi, Ph.D., Steve Ferenci, Richard Fujimoto, Ph.D., and Myung Choi, Ph.D.

Background

The Office of the Chief of Naval Operations (OPNAV N61), Navy Modeling and Simulation Management Office (NAVMSMO), has supported Network Warfare Simulation (NETWARS) since its inception. In 1998, the Military Communications-Electronics Board (MCEB) selected NETWARS to be the Department of Defense tool of choice for network communications modeling. The benefit of NETWARS for the Services is that it provides a reusable and interoperable modeling environment to conduct service-specific analysis within a joint framework.

One of the key goals of NETWARS is to combine the communications Modeling and Simulation (M&S) efforts of each of the military Services and establish a common simulation-based assessment and planning architecture that addresses the needs of the Joint Task Force (JTF), as well as the individual Services. To accomplish this objective, the NETWARS program established an Architecture and Standards (A&S) Working Integrated Product Team (WIPT), which is comprised of recognized leaders in communications M&S from each of the Services.

The Space and Naval Warfare Systems Center San Diego (SSC San Diego) is the Navy representative for NETWARS-related efforts, which include A&S WIPT contributions, model development and assessments.

Introduction

The NETWARS program is managed jointly by the Command, Control, Communications, and Computer (C4) Systems Directorate of the Joint Staff (J-6) and the Defense Information Systems Agency (DISA). NETWARS, the network M&S tool, is designed to assess military communications networks. It is used to conduct simulations at the joint task force level, which involve thousands of networked participants with tens of thousands of messages down to the tactical unit level.

The SSC San Diego C4ISR laboratory develops communications models of systems for NETWARS to assess military communications networks and the impact of communications on C4ISR operations. By federating (i.e., combining) NETWARS with other M&S tools we can leverage each tool's strengths. We initiated an effort to integrate the force-on-force M&S tool, Naval Simulation System (NSS), with NETWARS to create a NETWARS-NSS federation.

NETWARS Architecture

NETWARS is a discrete event simulator developed using the Optimized Network Engineering Tool (OPNET) Development Kit (ODK). It is designed to analyze military communications networks through the use of reusable communications device models (CDM), military doctrine and network traffic information in the joint arena. NETWARS consists of five functional elements, which are: (1) Database libraries; (2) Scenario Builder; (3) Capacity Planner; (4) Simulation Domain; and (5) Results Analyzer.

Database Libraries

NETWARS makes use of four primary databases: (1) Communications Device Model Library; (2) Operations Facilities (OPFACs) Library; (3) Organization Library; and (4) Information Exchange Requirement (IER) Library. The simulator uses these libraries to obtain detailed information about the communications systems used during the analysis. The CDM library contains the fundamental building blocks used in NETWARS, and the models that have been developed by the Services to represent the protocols and functionality that are found in physical devices.

Examples of Navy CDMs include radios, patch panels, multiplexers and tactical communications data links. The OPFAC Library is used to represent logical collections of CDMs, such as a tank or a Naval Operations Center (NOC). The Organization Library is built from one or more OPFACs that are connected with various communications links. These include point-to-point, wireless and broadcast links. Information Exchange Requirement Libraries are used to provide the simulation with details about the traffic, such as the type (voice, video or data), the source and destination of the message, its size, and the frequency with which the message is sent.

Scenario Builder

The Scenario builder defines how the OPFACs, Organizations, links and IERs will be used during the simulation. OPFACs and Organizations can be developed, and links can be assigned. Mobility can be given to organizations to represent the real-time movement of units throughout the course of the simulation. IERs are associated with devices, and message attributes are defined here. Periods of failure and recovery of OPFACs are also specified within the Scenario Builder.

Capacity Planner

The Capacity Planner evaluates and optimizes network link capacities. The Capacity Planner evaluates a given scenario to determine the configured network's average utilization, hop count and capacity. It can also optimize a network by using a simulated annealing algorithm that mutates the current solution to create new solutions for choosing an optimum solution. It can determine optimum link capacities and utilizations.

Simulation Domain

The Simulation Domain consists of the Simulation Engine (OPNET Modeler) and a Simulation Conversion Module. The Simulation Conversion Module translates the organizational

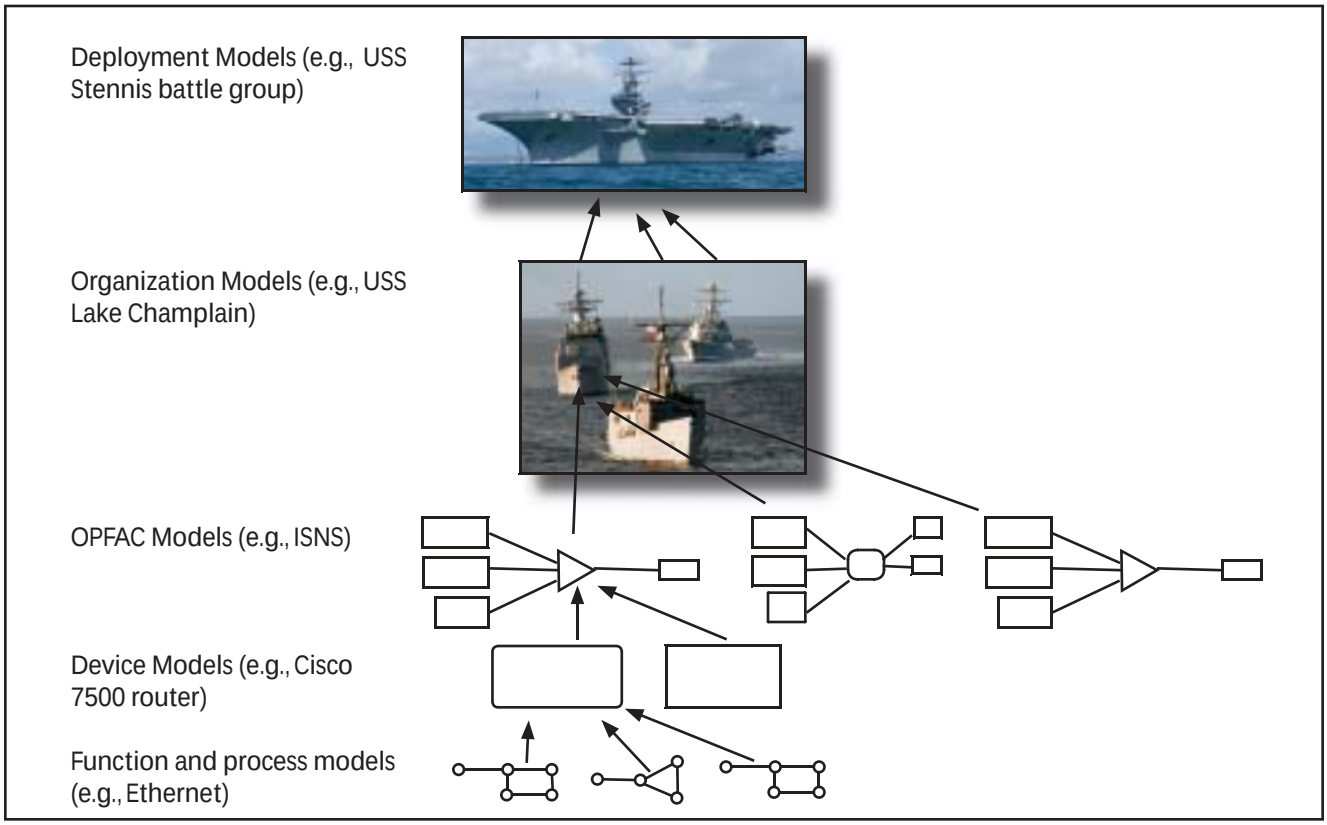


Figure 1. NETWARS Model Construction Hierarchy

representation and data flows into discrete events between the sender and receiver of specific communications equipment representations understood by the Simulation Engine.

Results Analyzer

The Results Analyzer allows an analyst to examine the Measures of Performance (MOPs) that are collected during a simulation. These MOPs are grouped into six categories: MOPs for a destination OPFAC; MOPs for a source OPFAC; global MOPs; device-level MOPs; MOPs for inter-OPFAC links; and MOPs for broadcast radio networks.

Model Interoperability Benefits

The Defense Department employs a wide variety of communication systems and technologies. These include commercial-off-the-shelf (COTS) technologies, such as IP-based devices and government-off-the-shelf (GOTS) technologies, such as Link-16. Each Service acquires different technology families to meet varying mission requirements of the warfighter. NETWARS provides a communications simulation environment that supports assessments of all these technologies. Rather than invest in the development of a communications model library that represents all of the existing and planned communications assets that would be required to support a Joint Task Force, NETWARS leverages a significant amount of model development resources from Service acquisition programs and simulation efforts.

Models may be added to the NETWARS library, for example, models may be high or low fidelity. All of these different model types may be valid for their original intended use; however, the challenge of promoting interoperability among these models is significant. A common approach for promoting interoperability among disparate models is to develop sets of architecture standards that provide a common model design and development approach for model construction. Standards may apply to different model characteristics such as interfaces, attributes, fidelity and documentation.

NETWARS implements several model development standards and guidelines to promote interoperability among contributed models. However, NETWARS avoids the overuse of standards, which is a common pitfall when using this approach. By establishing too many model development standards, the development environment may become too restrictive and inhibit or even preclude the development of certain types of models.

Development Guidance and Architectures

The primary resource for model development guidance and architectures is the NETWARS Model Development Guide (MDG). Model developers and contributors use these architectures to classify models into common categories. Models within the same category use similar sets of construction architectures, guidelines and requirements that ensure a high level of interoperability for simulations. The model categorization approach may also be used for converting existing OPNET models into a NETWARS-compatible format. Recently we began to contribute many of these models, including Link-11, Link-16 and the Automated Digital Network System (ADNS) into the NETWARS library. Two NETWARS model categorization architectures are provided within the MDG. The first architecture defines a model construction hierarchy. A Navy example of his hierarchy is illustrated in Figure 1.

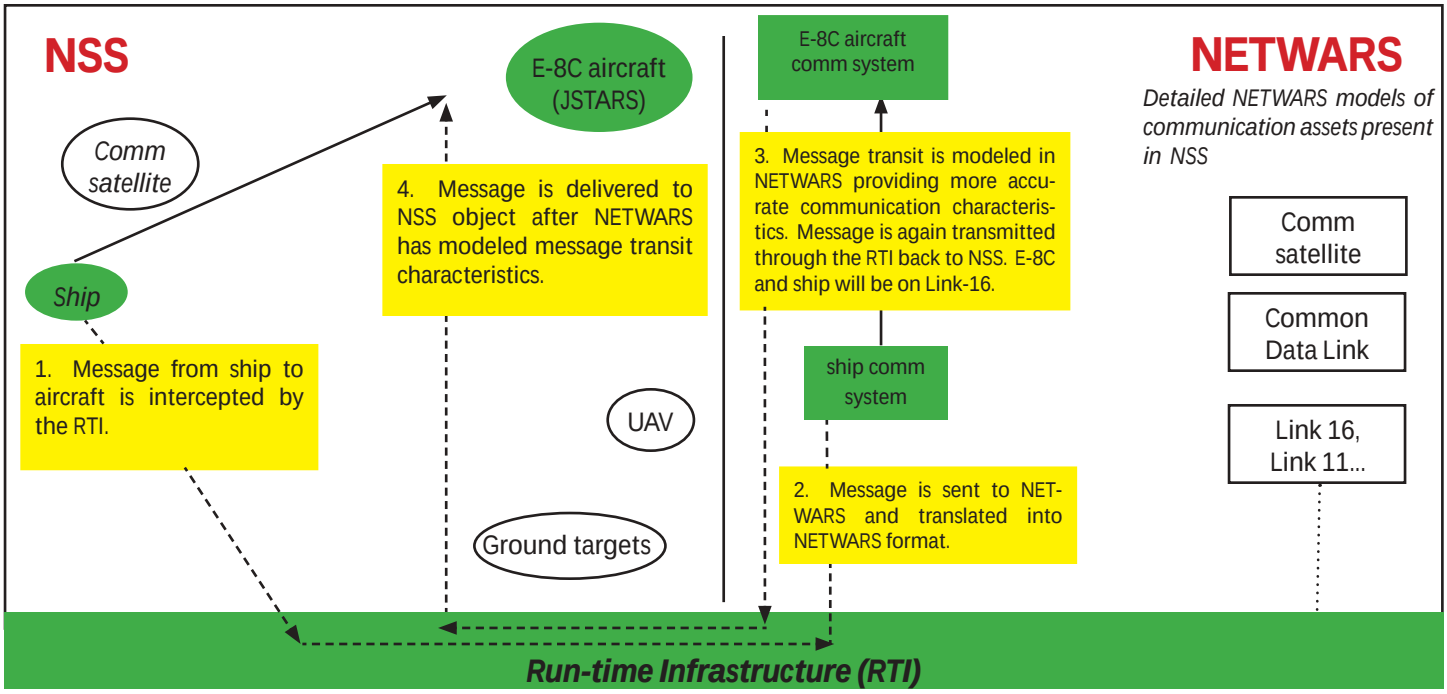


Figure 2. High-level description of NSS-NETWARS interactions

An example of the use of the Organization model is our modeling of the Network Operations Center that is currently being developed at SSC San Diego. There are four NOCs worldwide; however each NOC has differences. The Pacific Region NOC (PRNOC in Wahiawa, Hawaii) was considered the most generic of the four; so it was used as the template Organization. The template NOC Organization includes three Organizations: the SIPRNET, NIPRNET and ADNS enclaves.

Within each of the three enclaves are several OPFACs representing different network devices such as routers, switches, computers and multiplexers. Several of these OPFACs were created using OPNET model device libraries and had to be slightly modified to fulfill the requirements delineated in the NETWARS MDG. Modifying the template enabled the construction of three other NOCs: the Unified Atlantic Region NOC (UARNOC), the Indian Ocean Region NOC (IORNOC) and the Europe Central Region NOC (ECRNOC).

Another NETWARS model categorization architecture exists at the device model level (within the model construction hierarchy). NETWARS created the device model categorization architecture to provide developers with specific requirements and guidelines for each category of device models. By specifying guidelines and requirements at this level, interoperability can be ensured among new and existing device models of the same category. Device model categories were selected to emulate real-world communications equipment. For example, layer 3 network device models represent real-world layer 3 devices, such as Internet Protocol (IP) routers.

NETWARS also provides many model construction guidelines. These guidelines are not requirements, but promote a common, software development process. The NETWARS model development process is a valuable resource; it provides example code segments that may be reused by developers, and emphasizes model Verification and Validation (V&V) and documentation practices.

Core Component Model Standardization

In a contributed model environment such as NETWARS, a critical interoperability issue is dealing with multiple versions of the same model. For example, the Navy may contribute one variant of an IP model while the Army may contribute another. While most device models that implement the same protocol process models interoperate, device models that include different implementations of the same protocol model rarely interoperate and often may not coexist within the same simulation.

In cases where models are contained within isolated, standalone networks, this is not much of a concern. However in joint, connected Wide Area Network (WAN) systems that implement a variety of commercial communications protocols, this presents an interoperability issue. NETWARS addresses this issue by standardizing on a relatively smaller set of models within its library. This standard set of models includes technologies and protocols such as IP, Ethernet and ATM.

Any device model in NETWARS that implements a model of these technologies or protocols must be constructed using the corresponding NETWARS standard process model. NETWARS only standardizes on robust, high-fidelity, multifunctional models. In general, standard models are based on OPNET models, which have been thoroughly validated by OPNET technologies and employed for several years by the worldwide OPNET user community.

In addition to providing a common approach to the specification of scenario input data, NETWARS also addressed simulation outputs or statistics in a similar fashion. Simulation studies have

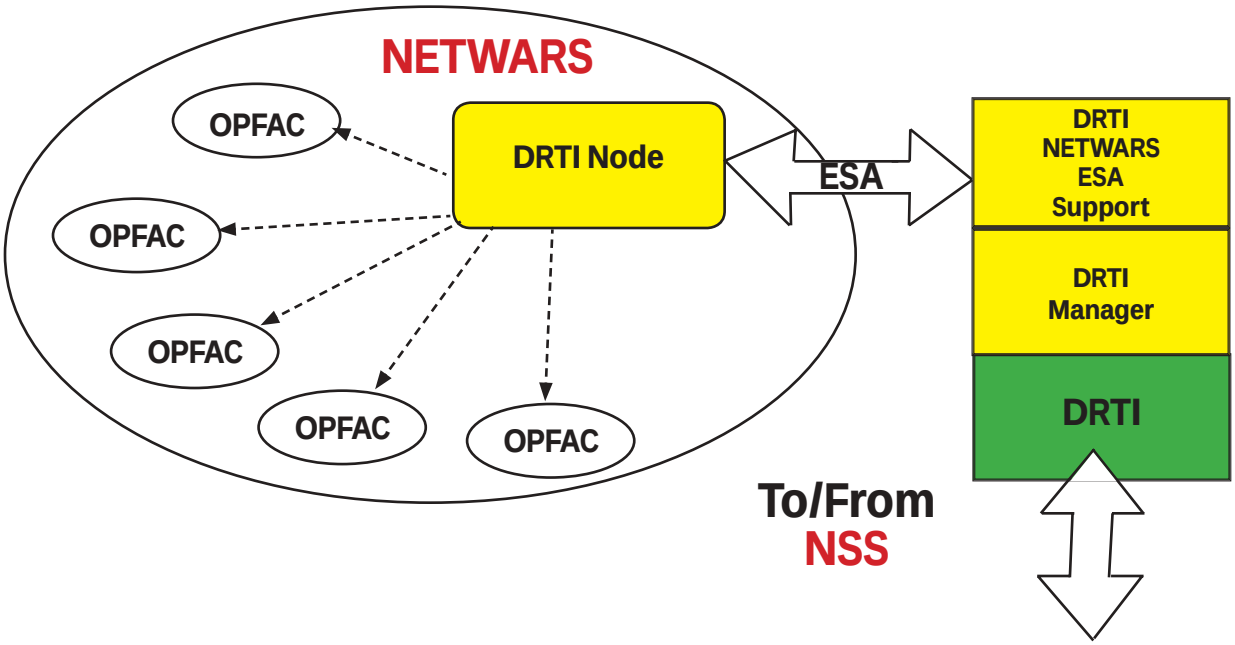


Figure 3. DRTI NETWARS Plug-in Architecture

the ability to examine a wide variety of output statistics. These statistics can be very system-specific, such as a Link-11 net cycle time. However, many communication simulation statistics are similar. These include end-to-end statistics such as message delivery latency and loss performance. To promote the highest level of model and results interoperability, NETWARS defined a core set of simulation output statistics, or Measures of Performance (MOPs), which are often examined in communication system assessments.

NETWARS-NSS Integration

The Naval Simulation System is an object-oriented Monte Carlo, discrete-event modeling and simulation tool originally developed by SPAWAR PD 15 and Metron, Inc., for the Chief of Naval Operations (CNO) N6M. NSS is designed to support operational commanders in developing and analyzing operational courses of action at the mission, group and force levels.

NSS has been used for Naval operations support including plan development, evaluation, refinement and execution. It is a well-known analysis tool for understanding the capabilities, performance and interactions of forces and C4ISR systems in combat. NSS has been deployed in numerous Navy exercises, including fleet exercises, fleet battle experiments and wargames, including the Navy Global Wargame.

To support multi-warfare scenarios, NSS offers low-to-medium fidelity warfare entity models. Communication systems in NSS are not well developed. Its low-resolution communications models (assured and unassured communications) and medium-resolution models (routed communications) are generically applicable to a variety of operational systems. At the high-resolution level, NSS provides three system-specific communications models, Link-11, Link-16 and TRAP/TRE (TRE Related Applications Program/Tactical Receive Equipment). These three high-resolution models are based on 1994 composite warfare model implementations.

NETWARS does not possess any operational support and warfare analysis capabilities, but users can implement new or leverage existing, system-specific communications models of required fidelity. The logical objective is to incorporate the highly developed communications modeling capability of NETWARS into NSS, which is well recognized for its force-on-force engagement simulation and analysis capabilities. To support this objective, we must provide the functionality necessary to allow entities in the NSS simulation domain to interact with entities in the NETWARS simulation domain. The approach we have taken is to federate NSS with NETWARS using a High-Level Architecture Run-Time Infrastructure.

Integration Overview

Figure 2 illustrates the NETWARS-NSS interoperability process. A message originating from a ship to an aircraft is intercepted by the RTI (step 1). The message is transmitted through the RTI to NETWARS. In NETWARS the message transmission is modeled (step 2), and upon receipt of the message, the transmission characteristics are reported to NSS via the RTI (step 3). Finally, in NSS the message arrives at the aircraft (step 4).

The Georgia Institute of Technology Federated-Simulation Development Kit (FDK) is used as the glue to facilitate the movement of information between NSS and NETWARS. The FDK contains a high performance High Level Architecture Run-Time Infrastructure (HLA-RTI), called Detailed RTI (DRTI), which provides the functionality needed for creating federations.

Two main features of the integration architecture are the extension of the Pegasus Federation Object Model (FOM), and the DRTI NETWARS Plug-in. First, since the NSS simulator can use HLA-RTI directly and supports the Pegasus FOM, the most logical approach to facilitate the NETWARS-NSS integration is to extend the Pegasus FOM to include additional interactions between NSS and NETWARS. The extension consists of a pair of interactions: Combat_Transmission_Request to notify NETWARS when

to send a message and Combat_Transmission_Receipt to return to NSS the status of the message transmission, and the delay when the transmission is successful.

Secondly, since the NETWARS does not directly utilize RTI services, middleware software is needed to enable a NETWARS simulation to interact with an NSS simulation. The functionality of the DRTI NETWARS Plug-in is divided into three components: (1) DRTI Process Model and Model Modifications; (2) DRTI NETWARS ESA (External Simulation Access) Support Module; and (3) DRTI Management Module. Each component or layer has a specific set of tasks to shuttle information between the NSS domain, the RTI and NETWARS. The DRTI Process Model provides the functionality to directly interact with entities within the NETWARS domain. The DRTI NETWARS ESA Support Module uses OPNET's ESA interface to create a bridge between the DRTI Process Model and the DRTI Manager. The DRTI Manager Module handles initialization of the RTI and all updates and interactions delivered by DRTI. Figure 3 shows the relationship of these components.

Technical Issues and Lessons Learned

There were several technical issues and lessons learned during the course of our study. The following describes two major issues: lookahead and model fidelity.

Lookahead

By definition, if a federate (i.e., member of a federation) has a lookahead L, then it will generate messages at least L time units after the current time. Consequently, events can be safely scheduled at least L time units prior to when they actually occur. In reality, IER interactions are zero-lookahead events. When NSS wishes to fire an IER at time x, the IER must be fired in NETWARS at time x. With zero lookahead, performance is expected to be poor, essentially turning a distributed simulation into a sequential simulation. To overcome the poor performance an artificial lookahead is added to IER interactions (Combat_Transmission_Request and Combat_Transmission_Receipt interactions) between simulators. We are exploring what are good lookahead values with respect to performance, and the impact this artificial lookahead has on MOPs.

Model Fidelity

In the initial NETWARS-NSS federation, the NETWARS Joint Tactical Information Distribution System (JTIDS) was identified as the major contributor to the slow federation runtimes. Further investigation of this model revealed that it explicitly simulated very detailed JTIDS transmission functions, thus contributing to its slow runtime performance. This high-fidelity model was developed to investigate prototype JTIDS slot access schemes and slot-sharing algorithms. For use in the NETWARS-NSS federation, the JTIDS model was modified to increase simulation runtime performance. This reinforces the notion that simulation runtime remains a key obstacle when modeling communications performance at very high levels of fidelity.

Chris Alspaugh *is an electrical engineer at SSC San Diego. He is the lead for the development of OPNET and NETWARS models. He holds a Bachelor of Science degree in electrical engineering from the University of California, San Diego.*

Thomas A. Hepner *is a computer scientist at SSC San Diego. He is the program manager for the Navy NETWARS program. He holds bachelor's and master's degrees in computer science and artificial intelligence from San Diego State University.*

Cam Tran *is a scientist at SSC San Diego. He has a doctorate degree in mathematics from the University of California, San Diego. He supports the NETWARS model development and integration efforts.*

Wonita Youm *is an electrical engineer at SSC San Diego. She builds organization models for Navy networks and develops model animations for various projects. She has a bachelor's degree in electrical engineering from the University of Washington.*

Albert K. Legaspi *is an electrical engineer at SSC San Diego. He supports the Navy Modeling and Simulation Management Office (NAVMSMO) on NETWARS-NSS federation. He is the head of the Network Centric Warfare Analysis Branch and a former chair of the IEEE Communications Society in San Diego. He has a doctorate in electrical engineering from the University of California, San Diego.*

Steve Ferenci *is a full-time research scientist in the College of Computing, Georgia Institute of Technology and is working toward a doctorate in computer science. He has a Bachelor of Science degree in computer science and mathematics from Rutgers University. He won best paper award at the 2002 Parallel and Distributed Simulation (PADS) workshop for his work in updateable simulation.*

Richard Fujimoto *is a professor at the College of Computing, Georgia Institute of Technology. He received doctorate and master's degrees from the University of California, Berkeley and bachelor's degrees in computer science and electrical engineering from the University of Illinois. He has been a researcher in the parallel and distributed simulation community since 1985 and has published over 70 technical papers on parallel and distributed simulation. He led the definition of the time management services for the DoD High Level Architecture (HLA) effort. Dr. Fujimoto is an area editor for ACM Transactions on Modeling and Computer Simulation.*

Myung Choi *is a research engineer and has doctorate degrees in electrical and computer engineering from the Georgia Institute of Technology. Dr. Choi developed simulations of various communications and networking technologies using OPNET and NS2. He successfully developed and prototyped a packet-size based queuing algorithm testbed.*

DON 2004 eGov Award Winners

By Lynda Pierce, DON CIO Communications and Public Affairs

Navy and Marine Corps teams continue to work on projects that are successfully transforming Department of the Navy (DON) business and warfighting processes to reduce costs, improve mission performance and support effective information sharing. The 2004 DON eGov Award winners will be presented at the second Naval IT Summit, scheduled for September 2004. Congratulations to the following teams for their outstanding efforts.

NAVSEA PEO Submarine eTasker Team and the USS Texas (SSN-775)

The USS Texas will be the first submarine in history to be 100 percent digitally certified! This significant milestone will be accomplished through the use of a new innovation in task assignment and tracking — eTasker. This system provides a single source of authoritative data, 24/7 accessibility and a streamlined, uniform methodology for tracking commitments. The entire review and approval process will be initiated, tracked, and commented upon within the eTasker Commitments module, thus providing auditable Objective Quality Evidence (OQE) for certification purposes.

Marine Corps Network Operations and Security Command (MCNOSC) Forward Element

The MCNOSC Forward Element vastly improves Department of Defense combat mission effectiveness in support of Marine forces in Operation Iraqi Freedom. The MCNOSC Forward Element capitalized on existing contracts for information assurance equipment, Marine Corps standards and innovative training. It provided network routing optimization to support video teleconferencing; Internet Protocol voice calls (VoIP); enhanced firewall capability; and SIPRNET and NIPRNET local area network architecture enhancements. The MCNOSC completed these tasks within two months and for less than $77,000. This modest investment realized significant returns by saving countless man-hours otherwise required for re-baselining networks.

NAVFAC and DON eBusiness Operations Office JEWLS Project Team

The Joint Expeditionary Warfare Logistics System (JEWLS) pilot project was sponsored by the DON eBusiness Operations Office and developed in cooperation with the Naval Facilities Expeditionary Logistics Center and Naval Facilities Engineering Service Center. The project team developed a Web-enabled logistics decision support and execution system that provides total logistics awareness, and material and operational readiness visibility in a joint command environment. The JEWLS project offers significant time and cost savings and can substantially improve readiness for deployed forces.

U.S. Pacific Fleet Joint Task Force 519 Operational and Training Web Sites

The Joint Task Force 519 Operational and Training Web sites, sponsored by the Space and Naval Warfare Systems Command and developed by Commander, U.S. Pacific Fleet, have provided an unmatched ability to train, plan, develop and execute critical and time-sensitive assigned missions with members of every military service dispersed throughout the world. The Task Force developed a Web-based tool that replaced manually intensive, paper-based planning, training and real-world operations, eliminating the need for hard copy preparation and distribution of all phases of Joint Task Force operations. This tool offers significant time and cost savings and speeds the decision-making process.

NAVFAC Applications Rationalization and Management

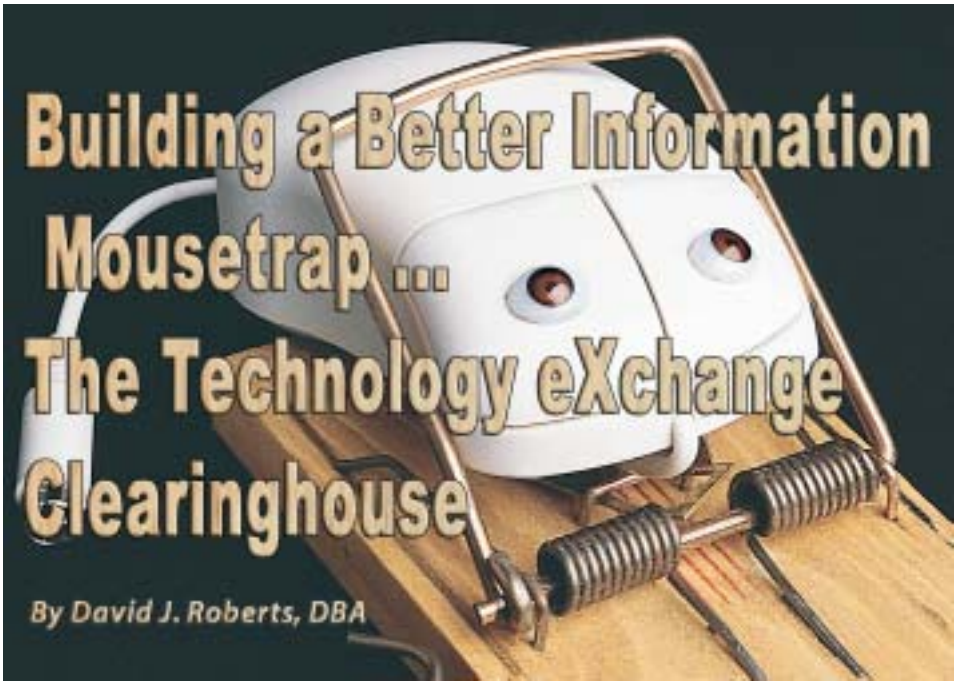
The Naval Facilities Engineering Command (NAVFAC) distinguished itself among Navy echelon II commands by demonstrating exceptional leadership and innovation in legacy applications rationalization and portfolio management. NAVFAC developed a standards-based application portfolio through a process that forced choices among legacy applications, resulting in a significantly reduced portfolio and associated costs. NAVFAC executed a claimancy-wide approach for applications to transition to NMCI, avoiding redundant media collection, testing, packaging and deployment costs. Four echelon II groups have applied NAVFAC's rationalization methodology, resulting in a significant reduction of applications in the Navy portfolio.

DON eBusiness Operations Office, PEO C4I and Space and SPAWAR SCAMP

The Speed to Capability, Approval, Management, and Planning (SCAMP) process pilot project, sponsored by the DON eBusiness Operations Office and developed in cooperation with PEO C4I and Space and SPAWAR, reengineered existing stovepiped processes into a centralized process that optimizes command-wide communication and coordination of tasks to deliver improved speed to capability. The SCAMP team developed an overarching business process that includes standards, guidance and a Web-based supporting tool set, which is extensible across the DoD. Initial implementation of SCAMP has demonstrated significant speed to capability resulting in improved fleet readiness and direct cost savings.

Marine Corps MERIT

The Marine Corps Equipment Readiness Information Tool (MERIT), developed by the Marine Corps Logistics Command and the Marine Corps Systems Command, provides a dynamic adaptable view of equipment readiness by commodity, functional area and organization. An automatic graphics generator feature provides customized information for current and historical readiness, and is ideal for developing readiness related briefing charts at all levels. Use of this system resulted in a direct savings of over 2 million man-hours per year. As a result of this team's efforts, the Marine Corps has a common operating picture (one watch) for Marine Corps Equipment Readiness.



Introduction

From the American consumer to the American warfighter, the ability to retrieve meaningful, current, useful information from the vast universe of information sources via the World Wide Web, is growing increasingly difficult. Not only is there an almost limitless number of information sources, but the problem is compounded by how information is interpreted. What the reader understands from retrieving the information may not be what the originator intended in providing the data. Fortunately, at least for the warfighter, help is on the way.

The Space and Naval Warfare Systems Command, in partnership with the Department of the Navy eBusiness Operations Office, developed the Technology eXchange Clearinghouse. TXC is an end-to-end ebusiness solution that provides early identification and integration of cutting edge technologies for the Navy.

TXC not only benefits official acquisition "programs of record," but it can also be applied to the fleet's latest operating concepts such as Sea Power 21 and FORCEnet. TXC is all about bringing technological innovation to the fleet rapidly — and as an ongoing process.

The roots of TXC lie in decades of research and transition efforts by Navy scientists and engineers. The Clearinghouse automates what was formerly an exhaustive manual process. Starting as a pilot program fall 2003, the program is currently managed by the SPAWAR Chief Information Officer, with development performed at SPAWAR Systems Center San Diego. TXC was integrated into DON data services spring 2004.

TXC is more than a Web-enabled repository of technology information. Rather than capturing information in a single hierarchical format, information is stored in several industry and government classification schemes. Technology producers can describe their research or products using one of several industry standard classification schemes, such as the Association for Computing Machinery (ACM).

DON operating constructs, such as FORCEnet, are also mapped to the body of information. A FORCEnet user could search for specific technological capability, such as low-bandwidth collaboration, and learn what the latest developments are and how those developments might be integrated into a FORCEnet environment.

Additionally, TXC has the ability to filter information by mission requirements (context), to provide innovative and comprehensive technology-based solutions. For example, in the context of "speed to deploy a technology," the filter of "maturity" could be applied. Resulting searches would return only technologies sufficiently mature to be useful.

Thus, TXC provides a Web-enabled method to search thousands of pieces of information to find relevant technology solutions. The specific search method used in TXC is powerful and easy to use thus enabling both producers and users of technology products and services to navigate the TXC.

TXC Architecture ...

TXC's architecture uses a SPAWAR enterprise-wide license based on Oracle's 10g implementation (see Figure 1). The Oracle Orion Web server is used because of the high level of integration, security and performance required of the system. The database is accessed via Web services offered by the Java Enterprise Edition (J2EE) midtier. TXC supports both portal/portlet and direct application Web services.

Two physical servers are employed: one to provide front-end Web services and one to provide the back-end database. The front-end server is PKI-enabled, offers Web services and provides a firewall for the non-routable back-end network. To address future growth, the back-end server can be clustered under Oracle 10g beyond its initial quad Xenon processors with more than 700 gigabytes of main system storage.

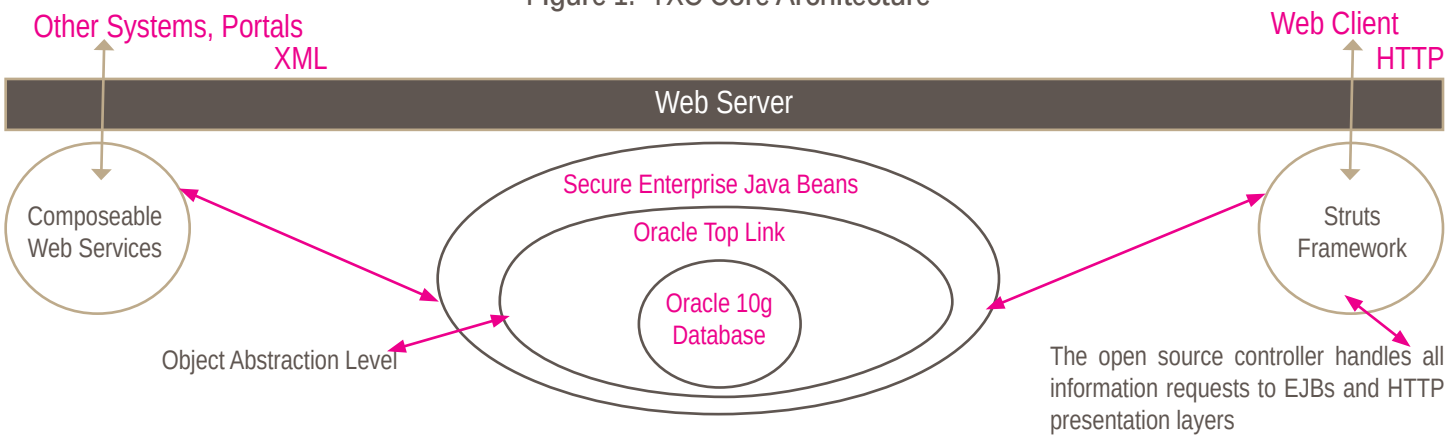
Both front-end and back-end clustering will be used for processors and system storage as the system grows. Data archiving of aged information to secondary optical storage devices will be used to maintain the responsiveness of the primary system storage.

The security model used within TXC employs a role and group access scheme. Security is maintained at field level access throughout offered Web services. Access to the system is limited, and access to individual product records is strictly enforced. Owners of product information are limited to information about their records only.

General information concerning the number of times a product record was accessed, times, dates, access group, etc., will be available as feedback to the product record owner.

The key to TXC's success is that it allows program managers, technologists, system designers and engineers to view retrieved information through their own frame of reference. Functions that can be performed include: Gap Analysis (actual

Figure 1. TXC Core Architecture



versus available capabilities); Duplication Analysis (multiple technologies with the same capabilities); Risk Analysis (maturity, funding, technical); and Capability Assessments (matching mission requirements).

TXC was designed from the ground up to provide Web services; its architecture is clearly a departure from traditional data warehouse strategies. Web services are only dependent on the level of access of the client. TXC simply publishes information for use by the client-base. Clients can reuse TXC information in either a portal or application context at their discretion.

An important feature of TXC is that it meets all Navy Marine Corps Intranet requirements for software on the client workstation, user authentication, client/server certifications and security restrictions. Any NMCI or PKI-enabled workstation can access TXC through any Internet browser.

Problems Solved ...

TXC provides a "one-stop shopping" solution to the chaos of multiple technology databases within both the commercial sector and the Department of Defense.

TXC provides vendors and owners of technologies an access point for the evaluation of their technologies and products, and it provides the Navy with a method for finding technology-based solutions.

These capabilities are combined with a collaborative forum to promote innovation and partnering. TXC translates many commercial and government groupings of information (ontologies) into navigable structures, with a primary focus on the capabilities that technologies bring to solve mission oriented problems.

TXC incorporates existing vendor information from the federal Central Contractor Registration (CCR) and FEDLOG to prequalify and pre-register clients. Potential clients access the system through the Internet at: https://TXC.SPAWAR.navy.mil/.

Additional access information is submitted and the client is approved for record input or access by the TXC staff. Once approved for access, a client can add product or service information through an easy-to-use pull-down menu structure. Existing product sources are also assimilated, such as the DON's Fleet Certified Product List through a bulk information sharing agreement.

Benefits ...

Beyond TXC's initial return on investment of more than 10 to 1 over previous manual methods, TXC offers the following benefits:

√ Speed to deployment ... TXC provides a process to guide the integration of the right technology into Navy systems. It reduces the overall time to collect technology information, review it and match it to capability requirements.

√ Better decisions through "instant trade studies"... TXC provides the ability to perform trade studies literally at the push of a button. Users are able to select the criteria for the TXC report filter, including maturity, technology category, potential mission area, etc., and display the corresponding technology information.

√ Cost savings through competition ... With the ability to perform instant trade studies, the user can shop vendor offerings for the best capability values. Additionally, in a fair and open market, the government can be assured of the best value. All vendors will have the opportunity to bid.

√ Comprehensive and timely information ... Technology developers and owners have a vested interest in maintaining their data records. The owners of the technology determine what public information they are willing to disclose, and the terms and points of contact for proprietary discussions.

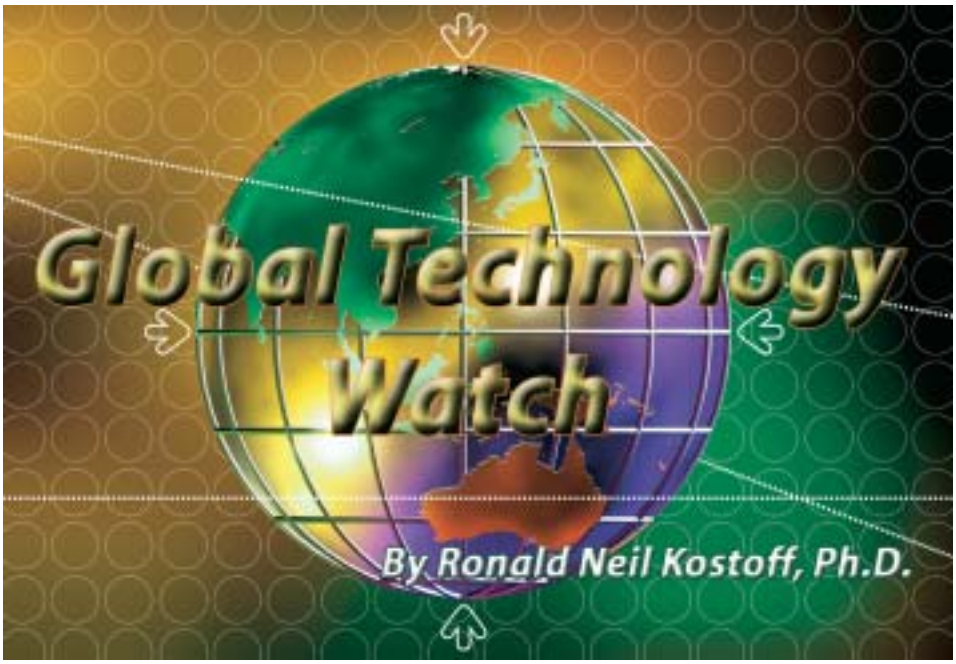
TXC should not be viewed as a single solution, but rather as an enabler to the age-old process of bartering and trade. Both developers and users of technology-based solutions are able to engage in safe and meaningful interactions to determine if matches or partnerships are possible.

The Future Team ...

TXC has formed cooperative relationships with industry and government, and continues to offer partnerships with government and research communities. Sharing is part of the TXC business philosophy, to reduce overall development costs and grow the client community. New members to the partnership are always welcome.

To register a product or technology services from anywhere on the Internet, please go to https://TXC.SPAWAR.navy.mil/.

Roberts has bachelor's degree in cognitive anthropology with a minor in chemistry, a master's degree in public administration and a doctorate in business administration (DBA) with an emphasis in computer graphics. Roberts is the program manager of the Technology eXchange Clearinghouse sponsored by the DON eBusiness Operations Office.



Overview

Governments and industry worldwide rely on advances in science and technology (S&T) to maintain a competitive advantage. To this end, they need ready access to the results of global research to:

– Track the impact of research to help identify benefits
– Evaluate science and technology programs
– Avoid research duplication
– Identify promising research directions and opportunities
– Perform myriad oversight tasks
– Support every step of a strategic research process that makes optimal use of S&T investment resources

In addition, recent counterterrorism concerns highlight the need for ready access to information that links people, technology and organizations together to stop the threat of terrorist activities. To combat this threat, more advanced technology is required, especially in the areas of surveillance, detection and prediction.

Since science and technology are global enterprises, with expenditures approaching $1 trillion dollars annually, (depending on one's definition of S&T), no single organization or nation, can begin to research and develop the full spectrum of S&T required for a modern competitive economy or military. There must be cooperative development efforts including identifying, leveraging and exploiting external efforts — if an organization or nation is to remain competitive.

Global Technology Watch maintains awareness at all levels of global S&T through a combination of human-based overt and covert activities, and automated approaches for analyzing and tracking the myriad S&T outputs. These outputs include text (reports, papers, patents, etc.), other media, physical products and technically trained people.

This article describes how information technology can help an organization maintain awareness of global S&T efforts by extracting useful data from large volumes of structured and unstructured S&T text. It is targeted to the researcher, intelligence analyst and information technology professional.

Powerful information technology techniques, such as text mining, now exist to identify and extract relevant data from the global S&T literature. Text mining is especially useful in making sense out of disjointed and disparate data. At the Office of Naval Research, we have developed and used these techniques to substantially enhance the retrieval of useful information from global S&T databases, such as the following.

• Science Citation Index (SCI) – current and retrospective bibliographic information, author abstracts and cited references found in 5,600 of the world's leading scholarly science and technical journals covering more than 150 disciplines. The Web-based Science Citation Index Expanded, used at the Office of Naval Research, has 2,100 more journals than the CD-ROM version.

• Engineering Compendex – a compendium of more than 5,000 journals, conference proceedings, technical reports and foreign translations addressing applied research and technology development.

• MEDLINE – published by the National Library of Medicine and the National Institutes of Health, containing medical data covering basic and applied research.

• National Technical Information Service (NTIS) – the largest central resource for government-funded scientific, technical, engineering and business related information available today with more than 600,000 information products covering over 350 subject areas from over 200 federal agencies, including the Defense Technical Information Center Technical Reports. The technical reports and other DTIC databases are easily accessible on the DTIC Web site at http://www.dtic.mil/.

• Inspec – published by the IEE, is an English-language bibliographic information service providing access to the world's scientific and technical literature in physics, electrical engineering, electronics, communications, control engineering, computers, computing, information technology, manufacturing and production engineering.

• RADIUS – created by the Rand Corp., in cooperation with the National Science Foundation, contains narratives of U.S. government agency research and development programs at five hierarchical levels, ranging from 24 narratives at level 1 (reflecting overall descriptions of the research and development activities of the 24 major R&D sponsoring agencies) to 592,000 narratives at level 5 (award levels from these 24 agencies).

• U.S. Patent and Trademark Office – patent database.

The extracted data is used to identify the technology infrastructure, including authors, journals, organizations, etc., of

a technical domain and the experts for innovation-enhancing technical workshops and review panels. It is also used to:

• Develop site visit strategies to assess organizations globally using bibliometrics (e.g., counts of publications, patents, citations and unpublished data) and other science and technology indicators.

• Generate technical taxonomies (classification schemes) using clustering methods.

• Provide roadmaps for tracking innumerable research impacts across time and applications areas based on text mining. This has important consequences for Web-based corporate and national security intelligence.

Text mining has the potential to serve as a cornerstone for credible technology forecasting. It helps predict the technology directions of global military and commercial adversaries. Text mining has also been used to identify asymmetries and stratifications in technical databases where none were expected, potentially leading to an improved understanding of system structure and dynamics.

Components of S&T Text Mining

There are three major components:

• Information Retrieval – the selection of relevant documents or text segments from source text databases for further processing.

• Information Processing – the application of bibliometrics, computational linguistics and clustering techniques to retrieved text to provide ordering, classification and quantification to formerly unstructured material.

• Information Integration – the combination of computer-generated output with human cognitive processes to produce a greater understanding of technical areas of interest.

Steps in a Text Mining Study

A typical text mining study (by our group), without the literature-based discovery component, includes the following steps:

√ Identify the technical scope of the problem.

√ Develop a query to retrieve published records comprehensively and accurately. This involves high recall and precision.

√ Select appropriate source databases for analysis.

√ Retrieve records from databases.

√ Generate publication bibliometrics.

√ Generate citation bibliometrics.

√ Generate background section, whose content is based on contribution of seminal papers.

√ Generate taxonomy of retrieved literature to identify technical structure, including themes and relationships, using manual and/or statistical clustering. Include phrases and words, document clustering and hierarchical and/or flat taxonomies.

√ Determine adequacy or deficiency of levels of effort (based on numbers of publications) in each category of taxonomy.

Conclusions

The confluence of comprehensive technical databases, sophisticated information extraction algorithms and advanced text-mining processes offers the capability of substantially increasing awareness of global S&T. Expanded awareness fits in with the requirement for maximal technology advancement to combat terrorism and to ensure a competitive economy. Successful global S&T text mining requires an intrinsically interdisciplinary approach, incorporating information technology and technology-specific expertise.

For further information, I suggest the following resources, which are available through technical libraries.

Kostoff, R. N. "Text Mining for Global Technology Watch." In the Encyclopedia of Library and Information Science, edited by M. Drake. Second Edition. Vol. 4. New York: Marcel Dekker, Inc., 2003: 2789-2799.

Kostoff, R. N. "Stimulating Innovation." In The International Handbook of Innovation, edited by Larisa V. Shavinina. Oxford, UK: Pergamon Press, 2003.

Hearst M.A. "Untangling text data mining." Proceedings of ACL 99, the 37th Annual Meeting of the Association for Computational Linguistics, University of Maryland, June 1999.

Zhu D.H. and A.L. Porter. "Automated extraction and visualization of information for technological intelligence and forecasting." Technological Forecasting and Social Change, 2002. 69 (5): 495-506.

Swanson D.R. and N.R. Smalheiser. "An interactive system for finding complementary literatures: a stimulus to scientific discovery." Artificial Intelligence, Vol. 91, 1997. (2): 183-203.

Kostoff received a doctorate in aerospace and mechanical sciences from Princeton University in 1967. At Bell Labs, 1966 to 1975, he performed technical studies in support of the NASA Office of Manned Space Flight and economic and financial studies for AT&T. At the Department of Energy, 1975 to 1983, he managed the Nuclear Applied Technology Development Division, the Fusion Systems Studies Program and the Advanced Technology Program. He joined the Office of Naval Research in 1983 as the Director of Technical Assessment for 10 years. He invented and patented (1995) the Database Tomography process, a computer-based textual data mining approach that extracts relational information from large text databases.

After managing the Navy Laboratory Independent Research Program for five years, he established a new effort in textual data mining. He recently received a full-spectrum text mining system patent application, called TexTosterone. He has written many papers on his research and is listed in Who's Who in America, 56th Edition (2002), Who's Who in America, Science and Engineering, 6th Edition (2002) and 2000 Outstanding Intellectuals of the 21st Century, 2nd Edition, (2003). See also http://www.onr.navy.mil/sci_tech/special/technowatch/.

The SSC San Diego Concept of the *Composeable* FORCEnet

By the SSC San Diego Composeable FORCEnet Team

In describing his vision of the Navy of the future, Sea Power 21, Chief of Naval Operations, Adm. Vern Clark, cites three fundamental concepts: unprecedented offensive power, which he terms Sea Strike; defensive assurance or Sea Shield; and operational independence or Sea Basing.

Adm. Clark states that the architecture and the enabler to achieve Sea Power 21 is FORCEnet, "an overarching effort to integrate warriors, sensors, networks, command and control, platforms and weapons into a fully netted combat force." FORCEnet, he says, is the Navy's means to make network-centric warfare an operational reality.

With the opening of the Composeable FORCEnet Human Systems Integration (CFnHSI) Laboratory, SSC San Diego has expanded testing and evaluation capabilities to address human performance as part of FORCEnet.

Initiating what the CNO has characterized as "the best example of a fully netted force that I've ever seen," innovative technical personnel of the Space and Naval Warfare Systems Center San Diego fashioned a vision for an essential supporting concept — the "Composeable" FORCEnet. The team believes this capability will provide joint warfighters operating in a FORCEnet-enabled environment, superior decision-making capability enabling the joint force commander to achieve full spectrum dominance.

The key word in this construct is composeable because commanders must have the ability to compose a command and control capability that meets their warfighting requirements from a broad array of components, including multitiered networked platforms, sensors and dynamic bandwidth capabilities — all with the capability to interpret and create any visualization to meet mission requirements. This will provide the framework to achieve fast, flexible and agile speed to capability in the face of rapidly evolving threats and missions — enabling commanders to make informed decisions.

To illustrate this concept, the SSC San Diego team developed a demonstration, which has been shown to visitors at the center, including Adm. Clark, and to large audiences at various joint technical conferences and trade shows. The demonstration, based on a simulated scenario, illustrates the capabilities that evolving Web technologies provide when applied to warfighting. During the demonstration, the underlying conceptual framework is described, the functionality provided by Web services and tools is shown, and this functionality is then applied to several operational missions to demonstrate the warfighting implications of the concepts.

"If the engineering community can provide a capability that enables a warfighter to compose the C4ISR capabilities needed at a particular place, at a particular time, to deal with a particular operational challenge, in other words, 'on the fly,' then we will have provided our military with the means to achieve maximum agility and effectiveness against any threat," said Jeff Grossman, one of the SSC San Diego technical leaders developing the Composeable FORCEnet.

The complexities of FORCEnet will require substantial time and effort to instantiate a final engineering architecture for a robust, survivable system. As a result, SSC San Diego personnel believe demonstrating an early instantiation of Composeable FORCEnet is important to enable Defense Department and DON decision makers to fully appreciate "the art of the possible" regarding what it can deliver to the operational commander.

Two key concepts are emphasized with Composeable FORCEnet. One is the concept of composeability, which is the ability to compose warfighting capabilities from Web-enabled information and systems, Web services and Web tool components. The second concept is to provide mechanisms to transform fused data into information of known pedigree and then into actionable knowledge in a manner that directly supports decision making at all levels of command.

Composeable FORCEnet can dramatically change C4ISR operations by providing the means to achieve shared awareness through an intuitive, map-based operational picture where information from any source may be geo-referenced, and anyone with appropriate permissions can participate in collaborative sessions. The following are examples of the functionality that SSC San Diego has demonstrated using the composeable concept.

√ Provides the ability to represent multidimensional aspects of the operational picture using a geo-spatial reference

environment — a map metaphor. This provides decision makers with the ability to interact with information in a familiar and intuitive environment.

√ Users can place any Internet address on a geographical location; overlay high-resolution maps and images, which can include elevation data on locations of interest; and even drag and drop data and documents (e.g., Microsoft Word) onto the map.

√ Users can integrate searches of Web content that can be linked to the map or objects on the map by the user, which can subsequently be shared with other users.

√ Users can tailor any representation with the intuitive and interactive interface based on well-known metaphors, such as Web browsers, search tools and graphical user interfaces. This dramatically reduces training requirements.

√ Provides a representation of information, allowing both access to and the ability to manage data through several key human-computer interface metaphors. The central metaphor — a map is based on the recognition that warfighters have historically planned and executed operations using a map — the metaphor for actual geo-space.

The use of electronic-based maps, together with Web tools and services, opens up new opportunities for expanding the map metaphor into an extensible, adaptable, pluggable new human-computer interface for FORCEnet. A second human-computer interface metaphor is the browser. Over the past several years, the concept of hyperlinked information available through "point and click" manipulation has become commonplace.

One of the current browser interfaces used in the Composeable FORCEnet demonstration was adapted from another SSC San Diego project, known as Knowledge Web. It is based on client-server architecture and provides an organization, notably a military command staff, with speed-to-decision capability through the ability to post information to a server available to authorized individuals continuously, rather than at specified briefing times. Significantly more information is available — more widely and more quickly than ever before.

Moreover, consumers of information, including top-level commanders, need minimal or no training beyond familiarity with the browser interface because of the simplicity of the KWeb design for information displays.

KWeb was implemented on board the USS Carl Vinson during its deployment to Operation Enduring Freedom; it was found to be extremely valuable in assisting information producers and users with the transformation of data into information — and information into knowledge.

In the conventional sense, the operational construct of Composeable FORCEnet provides the ability to conduct and coordinate operations efficiently and effectively. This means warfighters or an organization can: (1) Collaborate with anyone, anywhere, anytime; (2) Allocate bandwidth according to mission priorities

The CFnHSI has the ability to assess and evaluate human performance effectiveness in new and modified systems and applications. The lab supports HSI compliance within FORCEnet and serves as a means to transition human-centered R&D from laboratories to the fleet.

for particular information, applications or individuals; (3) Define the quality of service standards; (4) Show when and where sensor coverage is needed, and see the coverage and resulting sensor products; (5) Tailor information requirements and presentations to support missions; and (6) Put the right weapon on the right target with speed and precision.

Composeable FORCEnet can also provide the backbone for: quality of life improvements; medical treatment; logistics management; training and education; innovation and experimentation; and navigation. Thus, it is capable of supporting the CNO's supporting triad of organizational processes for Sea Power 21: Sea Warrior, Sea Trial and Sea Enterprise.

As operational commanders of Navy forces build their own, personalized, warfighting systems, it will likely drive these same individuals to put specific demands on the engineering community for future instantiations of FORCEnet, enabling operators and engineers to better communicate on what is, arguably, one of warfighting's most important issues: How to deliver the right information — at the right time — to the right people, while preventing an adversary from gaining access to the same information.

Ultimately, it is the naval and joint warfighter, not the engineer, who will use the capabilities needed for the immediate operational and tactical problem. SSC San Diego research suggests that warfighters operating in a Composeable FORCEnet-enabled environment will soon be able to compose the C4ISR components developed by the engineering community at their discretion to ensure superior decision making.

This capability can enable the joint force commander to achieve the maximum degree of operational effectiveness across the entire spectrum from warfighting to peacemaking — and to do it faster than ever before. FORCEnet can enable command and control constructs that are limited only by the operational and tactical imagination of the commander. ▭

Can You Hear Me Now?

Spectrum-enabled RFID tags store and share data

By the DON CIO Spectrum Team

Even if you have never heard of Radio Frequency Identification (RFID), you probably recognize the names Wal-Mart and Target. Both retail giants made big technology news last year. In November 2003, Wal-Mart defined a requirement for its largest suppliers to tag all cartons and pallets with wireless RFID sensors by Jan. 1, 2005. Target followed suit in February 2004, requiring some suppliers to use RFID tags on each case and pallet shipped by mid 2005.

RFID, a wireless spectrum technology that has existed for over 50 years and has been used by the Department of Defense (DoD) since World War II, has made it big in the commercial retail market. Although the commercial use of RFID made the news, the RFID trendsetter role can still be claimed by DoD and in particular by the Department of the Navy (DON).

Oct. 2, 2003, DoD issued a policy memorandum directing the immediate use of high-data capacity, active RFID technology that will affect all companies supplying goods to the DoD. But even earlier, during May 2003, the U.S. Navy Bureau of Medicine and Surgery implemented a Tactical Medical Coordination System.

Using versatile RFID technology, this custom-developed system simplifies hospital administration, reduces medical practice errors, provides better medical care, tracks common injuries and analyzes long-term trends by transferring patient information stored on RFID tags. Linking to a wireless local area network, unique data are exchanged, further eliminating manual reentry at a computer workstation.

While high cost components deserve the supply chain tracking benefit of RFID, it is notable that the DON found among its first applications, a solution to care for its most valued assets: Sailors and Marines.

Each patient admitted into Navy Fleet Hospital Three in Iraq is tagged with an RFID-enabled wristband. U.S. military personnel and other patients, including prisoners of war and the indigenous populace, are tracked by unique ID numbers embedded in the RFID tags. Medical staffs use RFID readers to scan the bracelet to confirm identity and enter information on diagnoses and treatments.

Turning from the humane to the mundane, during FY 2004, DoD will acquire more than $24 billion worth of supplies (beans, bullets, bandages) and services to support America's fighting forces, and that tangible supply chain will translate into a lot of logistics-related RFID tags.

How does an RFID system work?

A basic RFID solution is comprised of a minimum of three components – a radio frequency tag, which is actually a microchip that is an electronically programmed transponder containing unique information, an antenna device and a transceiver to communicate and decode the stored information.

When the transceiver sends out its electromagnetic waves, they form a magnetic field which "excites" the antenna on the RFID tag. A passive RFID tag accepts the magnetic field and powers the microchip's circuits. The chip then modulates the waves that the tag sends back to the reader and the reader converts the new waves into digital data.

The recent activity within the RFID industry will definitely improve the cost of components, but for the benefit of this discussion we need some baseline understanding. Passive paper tags, probably the least expensive tag in use, may be available for less than 20 cents, and hardened active tags on reusable containers are available for approximately $20. Transceivers are roughly $1,000 each.

Hospital corpsmen console a four-year-old Iraqi child with a shrapnel wound to the right foot. Note the RFID tag on the child's wrist. The child was transferred for follow-up treatment aboard USNS Comfort. U.S. Navy photo by Chief Journalist Al Bloom.

There are several spectrum bands associated with RFID use (see Table). Spectrum for RFID technology has not yet achieved harmonized international regulations, so use of specific spectrum bands associated with RFID is still a regulatory issue for each administration. Lacking a single standard, organizations could receive product tags for various spectrum bands requiring a transceiver in each of those bands to capture the tag data. In a normal operating environment, the result can be many tags and a number of frequency compatible transceivers.

Since RFID is based on proximity, unlike bar codes and their line-of-sight associated readers, the transceiver can process and analyze all of the "packages" as an entire pallet transits a loading dock. The

Frequency Band	Benefits	Concerns	Typical DoD Applications
100-500 kHz (Low Frequency)	• Inexpensive • Better penetration of non-metallic items	• Short to medium read range • Slow reading speed	• Access control • Inventory control
10-15 MHz (High Frequency)	• Short to medium read range • Medium reading speed	• Potentially inexpensive	• Access control • Smart cards
850-950 MHz (Ultra-High Frequency)	• Long read range • High reading speed	• Line of sight required • Expensive	• Vehicle Identification and Entry Control Systems
2.4-5.8 GHz (Microwave)	• Long read range • High reading speed	• Line of sight required • Expensive	• Vehicle Identification and Entry Control Systems • 802.11 generation of WLANs

A comparison of the benefits, concerns and applications related to different spectrum frequency bands.

time savings by not requiring visual contact with the tag are significant.

Tag Types: Passive, Active, Semi-passive

In the commercial implementation it is likely that passive RFID devices will be the norm. However, DoD's current policy anticipates supporting both active and passive devices. Passive RFID tags weigh less than active tags, are less expensive, and their operational lifetime is not dependent upon battery life. But they have shorter read ranges, more limited data storage than active tags and require a higher-powered reader.

Active RFID tags come with a battery and transmit a signal to a reader. Active tags can be read from 100 feet or more away, but at present they are significantly more expensive than their passive sibling. They are used for tracking expensive items over long ranges. Currently, the U.S. military uses active tags to track containers of supplies arriving in ports.

Active RFID tags are typically read/write, i.e., tag data can be rewritten and/or modified. Some active tags operate with up to 1 MB of memory. This flexibility supports variable application requirements. Semi-passive RFID has an internal power source to monitor conditions, but, similar to passive tags, requires RF energy from the reader/interrogator to power a response.

Tag Physical Form

Forms, shapes, sizes and protective packaging for tags vary with the article transit and storage environment. The common antitheft hard plastic tags deployed in stores are really RFID tags that also track inventory. Other RFID functions include credit card-shaped door access systems and animal tracking devices about the size of a pencil lead, which are inserted beneath the animal's skin.

Tag Coding – Standards for Clarity

The Electronic Product Code™ (EPC) is a number composed of four distinct elements – a header and three sets of data. The header is the key indicator identifying the tag version number. That version number keys the reader for the expected data length or other features that would be version specific.

The first set of data, actually the second part of the number, identifies the EPC Manager, which logically correlates to the manufacturer of the product. The second set of data, known as object class, refers to the exact type of product, most often the Stock Keeping Unit. The final data set is the serial number, which is unique to each item.

The Electronic Product Code stored on the RFID tag offers IT systems a method of matching the EPC to information about the associated item. Similar to the Internet's Domain Name Service (DNS), the EPC world has the Object Name Service (ONS), which provides a global lookup service to associate an EPC with an automated referral service that directs enquiries and applications to one or more Internet Uniform Reference Locators (URLs) where further information on the object may be found on the World Wide Web.

Currently the tags are available as either 64- or 96-bit electronic product coded units; the 96-bit EPC number is the most common. Using an EPC, the identity of the manufacturer, the product class, and specific instance of the individual product can be stored in a single tag. Today's most robust EPCs can be used to identify up to 268 million unique manufacturers, each with 16 million types of products. Each unique product can include up to 68 billion individual items, meaning the format can be used to identify hundreds of trillions of unique items.

With emerging requirements, the Uniform Code Council and European Article Number Association have endorsed proposals to expand EPC capacity, while other standards organizations are still reviewing the proposal. The draft EPC-256 is a 256-bit representation of the Electronic Product Code. The EPC-256 is designed for the long-term use of the Electronic Product Code as a universal identification scheme, not just a physical object.

DoD Specifications for Tags

The specification for EPC tags is relevant, since under the Defense Federal Acquisition Regulation Supplement Rule titled "Unique Item Identification and Valuation" published in December 2003, the government's tag requirement can be satisfied with the commercially adopted EPC standard.

The rules further state that DoD unique item identification, or a DoD recognized unique item equivalent, is required for defined acquisitions. Important to note, the

rule also stipulates that any commercial identifier can be considered by the DoD for use as a DoD unique identification (UID) equivalent if it meets all of the following criteria:

• Contain an enterprise identifier
• Uniquely identify an individual item within an enterprise identifier, product or part number, and
• Have an existing Data Identifier (DI) or Application Identifier (AI) listed in American National Standard (ANS) MH10.8.2, Data Identifier and Application Identifier Standard.

RFID Applications

The myth and reality of commercial RFID technology converge when manufacturers use the tags to monitor movement in a factory environment or distributors can track deliveries and inventory in a warehouse. This ability to monitor items has baseline applications in asset tracking, inventory management and supply chain automation. These are all standard technology applications that can benefit from wireless data collection.

Consumer products manufacturers like Proctor & Gamble Co., Johnson & Johnson, Kimberly-Clark and Kraft Foods Inc., focus on the RFID benefit of keeping products on shelves as a contributor to profit margins and evaluating new product success or failure. For DoD, implementation of RFID reduces inventory processing time, and improves asset visibility and maintenance of materiel. Thus within the DoD environment this technology will experience a rapid acceptance.

A cautionary note is that as RFID is introduced into the commercial and consumer market, there may be social issue debates about privacy rights and technical options for tagged products.

Efforts are underway to reach international associations and increase involvement by international ministries of defense. The following countries have been engaged to participate in the proposed system: United Kingdom, Canada, Republic of Korea, Australia, France, Sweden, Italy, Germany and NATO Allied Committees.

A DoD-wide application called Wide Area Work Flow-Receipts and Acceptance (WAWF-RA) is proposed to eliminate paper from the receipt and acceptance process. The goal is to enable authorized Defense personnel and contractors to create invoices and receiving reports, and access all contract related documents electronically.

Navy and Marine Corps RFID Applications

The Navy and Marine Corps are conducting extensive shipboard testing to determine whether emissions from RFID tags will interfere with ships systems or whether ships systems will affect the function of the RFID system. The tests successfully used RFID tags to automatically track material movement around the ship. Proof of concept projects underway at the Navy Automatic Identification Technology (AIT) Project Office include:

RFID Early Entry Deployment Support Kit (EEDSK): RFID capability anywhere in the world within a week, requiring no permanent RFID infrastructure.

Smart Stores: RFID Inter-ship stores and inventory tracking system.

Advanced Technology Ordnance Surveillance (ATOS): Real-time surveillance and inventory updates for ordnance.

DoD RFID initiatives will invariably impact Navy and Marine Corps information technology. The expanded scope of logistics management enabled by RFID will assist the warfighter, the command and control elements, and the essential support team members.

The impending change in DON business processes due to RFID adoption is not likely to be disruptive, despite the scale of the effort, because at critical stages the technical and policy decisions embraced a standard shared in the commercial world.

Contact the DON Spectrum Team at DONSPECTRUMTEAM@navy.mil.

New DoD Enterprise Software Initiative Agreements

Department of Defense Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs) were recently established for Systems Integration Services with Accenture, BearingPoint, Computer Sciences Corp., Deloitte and IBM.

The BPAs include the procurement of configuration, integration, installation, data conversion, training, testing, object development, interface development, business process reengineering, project management, risk management, quality assurance and other services for commercial-off-the-shelf (COTS) software.

Benefits include a streamlined acquisition process, standard terms and conditions, fixed-priced services tied to proven methodology, and reduced risk by following proven methodology and best practices. Estimated annual cost avoidance to the DoD is $160 million or $800 million over five years. These BPAs are open to all DoD Components, the U.S. Coast Guard, the Intelligence Community and authorized Defense contractors.

This groundbreaking program marks the first time that the DoD ESI negotiated technology services on a DoD-wide basis, and presents an opportunity to reduce the government's average implementation-to-software cost ratio, currently at 15 to 1, toward the industry average of 5 to 1. In addition to achieving substantial cost avoidance, these BPAs provide a performance-based approach with factors tied to the customer's key business priorities and fixed-priced configurations.

Finally, these agreements will contribute toward achieving the Navy's net-centric vision of Web services and support the Navy's Sea Enterprise initiative by the deployment of enterprise applications.

Go to http://www.itec-direct.navy.mil for more information..

Communities of Practice Get Underway at Keyport

By Marietta Atwater

Imagine you are trying to "beat the clock" to finalize a proposal, when you hit a roadblock. You need more information about risk management, and your traditional sources are on travel. Since you are pretty familiar with your Community of Practice (CoP) virtual workspace, you just click on the "White Pages" (expertise locator), and initiate a Search for "Risk Management." Tom, Neal, Cathy and Rick are listed as potential contacts. Using the e-mail addresses in the White Pages, you send each of them an urgent message and within minutes you receive a phone call from Rick, the subject matter expert, who supplies the information you need.

What if your automated test equipment is generating an error you haven't seen before? Maybe you are new on the job or just new to the software, but everyone is busy — and you are stuck. Thinking it might be worth a try, you log on to your CoP Web site and find several options in the online collaborative working environment. The "Best Practices" and "Lessons Learned" links capture your attention. Searching for the circuit card by name, you quickly discover one of the senior shop technicians has previously detected the same obscure failure and added it to the Web site. You are off the hook and on to the next task.

At the Naval Undersea Warfare Command (NUWC) Keyport, Wash., building Communities of Practice has been an opportunity to put a great idea into practice. If you aren't on board yet with why CoPs are important, what they can do for you, for your command and for the Navy — and why you will want to be involved — here is a quick overview.

The NUWC Concept of Operations defines CoPs this way: "CoPs are a network of people engaged in a particular profession, occupation or job function, who actively seek to work more effectively, to share knowledge and information relevant to their community and to understand their work more fully. They accomplish this objective by participating in peer reviews (not performance), sharing lessons learned, and jointly addressing emerging challenges and opportunities in their respective areas of specialization."

NUWC's Capt. Dan Looney addressed the topic of CoPs in a letter to supervisors last January, by saying, "…The primary focus of CoPs is the maintenance and improvement of core technical disciplines…. CoPs are focused internally to provide a forum for people who practice within the same discipline to enable knowledge sharing, develop networks and establish common tools. The CoP will become a mechanism for improving our processes, reducing the costs to paying customers and sustaining our core capability…."

Many of you remember Quality Circles, Process Improvement Teams and other quality measures over the years, and may think this is just more of the same. CoPs are different because they are not comprised of a few people trying to make a difference — CoPs allow every employee an opportunity to contribute; the resources (online and person-to-person) help us do our jobs better and as subject matter experts, we are able to help other members of the community do their jobs better through mentoring, problem solving or coming up with a "better idea."

Karen Danis

Karen Danis, technical manager for Knowledge Management and Community Builder at Keyport, has taken the lead in helping Keyport CoPs get started by providing training, structure and guidance.

"I'm delighted to see that NUWC has embraced this proven technique for improving efficiency, effectiveness and innovation. Knowing we have another vehicle for sharing ideas, lessons learned and best practices, and having resources to draw upon, will impact the bottom line and improve our quality of life," said Danis.

Keyport is employing a phased CoP approach. There are 32 Communities of Practice topics identified; however, Keyport has initiated seven CoPs to set the stage for others to follow. NUWC Newport, R.I., is also developing eight CoPs in the same areas, and both divisions will share their expertise, success stories and lessons learned. The CoP leaders and their core members have developed charters for each CoP that define the CoP's purpose, scope and initial focus areas. Hearing from a couple of Keyport's CoP leaders will help you capture the CoP vision and enable you to consider some ideas as to how CoPs can improve your area of expertise.

"The Software Engineering CoP provides developers with a way to share expertise, design methods, standards and even the first building blocks of software products. By harnessing this potential we hope to make development easier and more fun. In the software world this translates into higher quality products and highly productive engineers," said Joe Alyea, Software Engineering CoP Lead.

"The Workforce Development Community develops guidelines and improves processes for the development of our workforce to ensure we maintain and grow our core capabilities," said Mike Lehman, Workforce Development CoP Lead.

When CoPs succeed, we all benefit, not only at Keyport but throughout the greater community of the Department of the Navy!

Atwater is the managing editor of Keynotes, the newsletter of the Naval Undersea Warfare Center Division Keyport. This article has been edited from an original article, which appeared in Keynotes.

The dramatic south view of the Nimitz-MacArthur Pacific Command Center. All photos by Neal Miyake, SSC San Diego assistant project manager.

The new headquarters for the U.S. Pacific Command (USPACOM) located on Camp Smith, Hawaii, was dedicated in April. Named the Nimitz-MacArthur Pacific Command Center (NMPCC), the striking six-story, 274,500 square-foot facility overlooks Honolulu and replaces a nearly 60-year-old structure originally built as a hospital during World War II.

The new command center, equipped with more than 100 cutting-edge command and control and communications systems, is a model for future command centers. Accommodating more than 1,350 personnel, the NMPCC provides the commander and staff members with new information and decision-making technologies to effectively conduct the USPACOM mission throughout the Pacific and the world.

The NMPCC is one of the nation's premier facilities for Command, Control, Communications, Computers and Intelligence (C4I) systems. C4I plans were developed around the "battle cell" concept for distributed command and control. The systems architecture integrates new and existing systems into a flexible, joint, interoperable environment and greatly enhances collaboration capabilities throughout the Asia-Pacific theater. An engineering team from the Space and Naval Warfare Systems Center San Diego, located on Pearl City Peninsula, designed, engineered, integrated and installed the complex C4I systems.

The mammoth task of seamlessly transitioning command headquarters personnel and C4I systems was made more challenging by the requirement to sustain 24/7 operations during the transition. The C4I team's comprehensive installation plan, which included installing 12,000 data channels throughout the building, meticulously tracked system interdependencies while managing transition timetables, risks and related issues. Some of the capabilities include unclassified and classified data networks, telecommunications and voice systems, satellite communications (SATCOM), the J2 (Intelligence) Information Technology Support Office and the Joint Operations Center. New integrated video services provide enhanced capabilities such as multiple, simultaneous video teleconferencing.

For decades, SSC San Diego personnel provided C4I engineering and installation support to the U.S. Pacific Command. Their early involvement in this project allowed the C4I infrastructure to be integrated into the building plan rather than being imposed later into an existing design. The expertise of C4I engineers and technicians proved invaluable in fulfilling the project's technical requirements, while accommodating the operational processes unique to USPACOM.

The new headquarters provides USPACOM with critical information and advanced decision-making tools for real-time crisis management. Extensive connectivity and interoperability enhance collaboration among a wide range of resources, from the President of the United States, the Secretary of Defense and the Joint Chiefs of Staff, to service components, subordinate unified commands, and joint task force groups, as well as to coalition partners and local government agencies.

Using Space and Naval Warfare Systems Command guidance, the C4I team identified requirements with USPACOM staff and determined engineering solutions. The team collaborated with the Naval Facilities Engineering Command Pacific Division (PACDIV), the PACDIV Resident Officer in Charge of Construction and the building contractor to ensure the correct infrastructure was built into the facility. The team also worked with equipment and furniture contractors, USPACOM security and the Transition Task Force. In many cases, C4I planning influenced scheduling and the design of other efforts.

Early in the planning process, USPACOM determined that all systems, or information service domains, were to be described using the USPACOM Information Capabilities (IC) Framework model. Accordingly, the C4I team structured the information technology design package to align with the IC Framework, most notably in the Information Capabilities Requirements Analysis Document. This document provides a system engineering methodology by which a complex information technology infrastructure can be broken down into the different service area components it comprises.

To simplify management of the project, the C4I team used the IC Framework model and divided the project into eight functional areas which became the cornerstones of the overall C4I effort.

1. Inter-building cabling. Provides connectivity from the NMPCC to spaces in outlying buildings throughout Camp Smith and facilitates the circuit transition process.

2. Telecommunications. Administrative phone services via a Private Branch Exchange (2,000 lines) and the Defense Red Switch Network provide secure voice services (100 handsets).

3. Tech Control. More than 130 unclassified and classified circuits were transitioned to new position points in the new headquarters with cryptographic and messaging support. A state-of-the-art automated tech control was installed to monitor and route circuits with the capacity to manage more than 500 channels.

4. Networks. A backbone local area network (LAN) with multiple security levels was designed and engineered for classified legacy networks via 25 virtual LANs. The C4I team coordinated their plan with the Navy Marine Corps Intranet (NMCI) effort, assisting in the transition of NMCI secret and unclassified LANs and 2,400 associated workstations.

5. J2 Information Technology Support Office (ITSO). This is the directorate in charge of USPACOM intelligence. Intel and bilateral circuit management along with intel LANs and video teleconferencing (VTC) assets were consolidated into a centralized location. The J2 ITSO was outfitted to provide cryptographic support and patch connectivity to outlying temporary secured working areas.

6. Radio frequency/satellite communication. Antenna farms and radio rooms were created to provide command and control and tactical satellite communication. Radio-remoting technology and external cryptographics were used to more efficiently manage ultra-high frequency systems.

7. Briefing and display/video architecture (BDVA). Twenty-one specialty rooms were equipped with audiovisual (A/V) capabilities for visualization and advanced collaboration. Key efforts included: VTC across multiple classifications, robust A/V source switching, environment control system and specialized display and audio systems. Display technologies included: video walls, front and rear screen projection, liquid crystal display and plasma flat panel screens. An A/V control facility was created as the central control hub for VTC scheduling and source routing.

8. Joint Operations Center (JOC) and associated cells. In crisis management, the JOC provides battle staff with decision-making tools and information; the C4I team provided coordinated installation of all C4I assets, especially five national command and control systems. A robust cable infrastructure was provided to the JOC floor and outlying areas to harness all C4I assets within the building.

One key goal of the NMPCC was to support the battle cell concept where specialty rooms, including directorate conference rooms, would have virtual presence to the JOC via A/V systems and networking. This arrangement allows the JOC to be supportable from beyond the confines of the JOC floor and facilitates the management of multiple crises. The common thread is the BDVA Command Briefing System which allows the specialty rooms to share sources and to communicate with the JOC and battle staff.

Above: Video wall for the Joint Operations Center at the Nimitz-MacArthur Pacific Command Center.

Above: Front view of the Nimitz-MacArthur Pacific Command Center. For more information about USPACOM or SPAWAR San Diego, go to their Web sites: http://www.pacom.mil or http://www.spawar.navy.mil/sandiego/.

In addition to many other C4I-related projects such as overall configuration management, transition planning and risk management, the C4I team was responsible for engineering and installing the Integrated Physical Security System. This $4.3 million project includes an access control system using proximity, password and biometric authentication. The system is forward compatible with the Department of Defense Common Access Card, and includes surveillance cameras, an intrusion alarm system, remote alarming and a control room integrated with the visitor's control center.

Through conceptual and technological innovations like the Nimitz-MacArthur Pacific Command Center, the Navy is leading the military transformation to an effective joint warfighting force for the 21st century.

The IIDBT Meets the Demands of Modern Warfare with Speed and Accuracy

By Lt. Cmdr. Eric Higgins and Jason Hall

Investing in a Winner

The DON eBusiness Operations Office is an innovative ebusiness center that seeds pilot projects focused on improving DON business processes. It evaluates proposals from Navy and Marine Corps customers and funds selected information technology projects with an enterprise-wide view.

In FY 2003, the DON eBusiness Operations Office chose a project from Commander Second Fleet called the Integrated Interactive Data Briefing Tool (IIDBT). This project earned the DON eBusiness Operations Office and the Second Fleet a Microsoft Government Innovation Award, and business partner, the Herres and Lee Corp., a grand prize in the Microsoft System Partner Solution Builder Contest.

Commander Second Fleet Information Needs

Accurate information is the lifeblood of the military. Throughout history, gathering, exploiting and protecting information have been essential in command, control and intelligence operations. Better access to information and improvements in the speed and accuracy of prioritizing and moving data are essential.

The Second Fleet is responsible for Navy operations in the North Atlantic Ocean and for training and certification of East Coast Carrier Strike Groups and Expeditionary Strike Groups. To carry out this mission, timely and accurate information must be available to the commander and his staff. To this end, each morning, the admiral in command of Second Fleet requires an operational brief, known as the Commander's Update. This update provides information about the readiness and operation of assets throughout the fleet.

Traditionally, producing the update was a decentralized, manual process that was time-consuming; it produced static data that was typically several hours old. Assembling information required 15 to 20 staffers analyzing a variety of data sources (Web sites, databases, text messages, e-mails, etc.) to create a series of Microsoft PowerPoint slides that the Battle Watch Captain (BWC) would later organize into a single presentation for the admiral. This process was not only labor intensive; it also resulted in staff members getting information from different sources or at different times, which resulted in data inconsistencies throughout the brief.

Improve the Process … Improve the Information

Recognizing that much of the required data was already stored in electronic format throughout various Navy information technology systems, the admiral's staff saw the need for an integrated, Web-enabled solution that could automate the processes required to assemble the update. They realized that they could automate the data gathering process using Web services that could pull data directly from authoritative sources, bringing it into a format that is easy to manipulate and validate.

The Second Fleet staff turned these ideas into a proposal that the DON eBusiness Operations Office selected. The project was completed with exceptional results. This functionality now frees the staff to focus on data analysis rather than the more time-consuming data gathering. By automating these formerly manual processes, the IIDBT is saving some staffers an estimated 3.5 hours per day.

The IIDBT centralizes and streamlines the process of collecting, formatting and preparing the update. The IIDBT allows users to dynamically extract and present data from disparate repositories using XML Web services that do not require modifications to the fleet's existing back-end legacy systems while allowing information to be seamlessly shared within the Navy's SIPRNET. Using commercial-off-the-shelf (COTS) technology, developers also created applications that consume these Web services to integrate data directly into the update. The presentation is delivered on screen as Web content and allows viewers to drill down into the source data in real time during the brief.

The source data comes from a variety of standard reports generated by ships or other assets throughout the fleet. The fleet already maintains the data across several different systems, such as the TYCOM Readiness Management System, the Innovative Readiness Reporting Initiative, the Ships Operational Readiness Training Status (SORTS), the Conventional Ammunition Integrated Management System (CAIMS), as well as Casualty Reports (CASREPs) that document equipment failures.

The IIDBT's Web services automatically extract selected data from these sources and paste them into PowerPoint format. The commander's staff can continue using PowerPoint to customize each day's content, but the IIDBT dynamically converts the final presentation into HTML so that displaying and viewing requires only a Web browser.

Better Information … Better Decisions

Before the IIDBT was available, Second Fleet staff received data via electronic text messages that duplicated the same data that was already being fed directly into various database systems. Now, instead of having a team of people reviewing messages and manually copying data from them, IIDBT goes directly to the authoritative source for any given piece of data and automatically extracts it via Web services.

Second Fleet can do that as many times a

Left to right: Mike Stateler, technical lead, DON eBusiness Operations Office and Jason Hall, director of Sales and Marketing for Herres & Lee Corp., demonstrating the Integrated Interactive Data Briefing Tool at FOSE 2004.

day as it needs, and the update no longer relies on static information that was potentially out of date as soon as it was presented.

Using Web services also allows users to dynamically access information in response to questions from the admiral or other officers attending the brief. Before, when the admiral had a question, someone would have to find the information and get back to him later. Now, those questions can be answered on the spot because the IIDBT allows users to interactively tap into data sources.

Technical Advantages

By presenting the update in HTML format instead of the large PowerPoint files that were formerly used, the IIDBT also helps reduce the presentation's bandwidth demands. Using HTML format is a major advantage whenever there is a need to share the presentation with ships afloat with low bandwidth data links. The PowerPoint files could grow to 20 megabytes in size, which made downloading very difficult for ships with smaller pipes.

Another critical advantage of the IIDBT's methodology is that using XML Web services does not require special modifications to existing data sources. Regardless of how the IIDBT evolves to meet the admiral's information needs, the fleet's backend data repositories are not affected.

Using XML Web services also simplifies ongoing management of the IIDBT platform by providing a layer of abstraction that allows the fleet to modify and replace technology within the data management layer without affecting the applications or services that consume the data. In addition, while many of the fleet's data sources run on Microsoft SQL Server, the IIDBT's XML Web services interact just as seamlessly with the fleet's legacy platforms.

Wide-reaching Benefits

The Navy and Marine Corps can apply the savings provided by the IIDBT wherever data must be transformed into knowledge to support critical decisions. Speedy information retrieval and use of state-of-the-art technology tools to empower decision makers are realized on demand.

In the future, instead of relying on massed forces, we will achieve information superiority by leveraging the power of technology. National defense, homeland security and e-government are dependent on information systems. The real payoff of IIDBT comes when data are translated into knowledge superiority used by decision makers to empower the warfighter.

Lt. Cmdr. Eric Higgins is the collaboration officer in the Information Management Division at Commander Second Fleet. He was the lead project officer for the IIDBT project. Jason Hall is the director of Sales and Marketing for Herres & Lee Corp., a Springfield Va., based information technology consulting firm and Microsoft Certified Partner.

DON eBusiness Operations Office Solicits Pilot Project Proposals

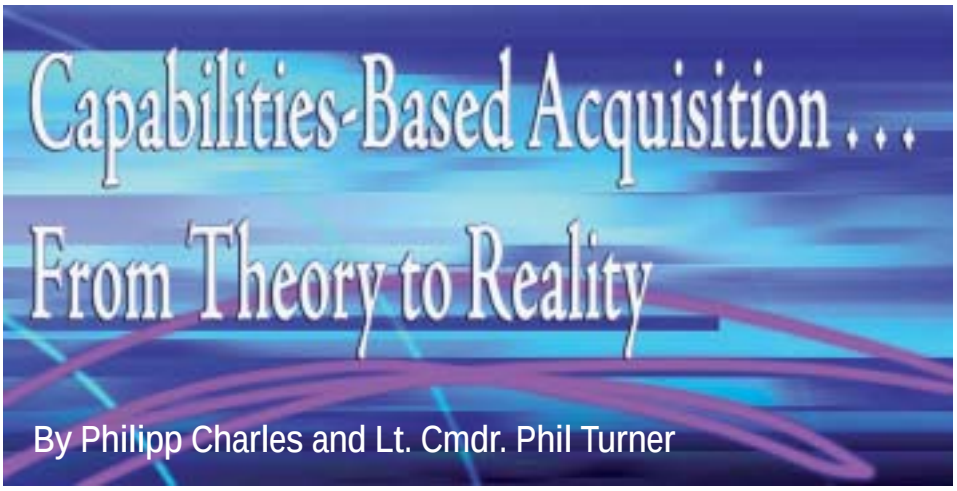
The Department of the Navy eBusiness Operations Office is now accepting pilot project proposals from Navy and Marine Corps ashore and afloat personnel, both military and civilian. Evaluation of these proposals for funding under the FY 2005 pilot program will be ongoing through July 30, 2004.

The eBusiness pilot program provides seed money for projects that use technology innovation to improve business processes across the entire DON. Successful eBusiness pilot proposals are of limited scope, cost and duration in order to rapidly develop working prototype solutions. Proposals are expected to address improving current DON business processes and to provide a positive return on investment.

The DON eBusiness Operations Office helps solve Navy and Marine Corps process gaps by combining business process reengineering with information technology infusion. Any business process improvement opportunity can be a focus area for a pilot proposal from maintenance or medical to logistics or learning. The proposal submission process is simple. Go to the eBusiness Operations Office Web site at www.donebusiness.navsup.navy.mil/, click on "Submit a Pilot Project" and complete the online submission form. This Web site also contains valuable information about proposal criteria and the selection process.

Pilot submissions are evaluated in the last quarter of the fiscal year for funding in the following fiscal year.

Phone (717) 605-9359, DSN 430-9359 for assistance.



Introduction

The concept of capabilities-based acquisition is fundamentally changing the way we buy and engineer systems in the Department of Defense (DoD). A capability can be defined as the ability to perform a course of action or sequence of activities leading to a desired outcome. The capabilities-based acquisition process requires that we identify these capabilities, their requirements, conditions and metrics, and then acquire the right equipment and information services to support the desired capabilities in an integrated enterprise environment.

In simple terms the concept is this: Instead of buying threat-based, service-specific systems, a mobile target-weapon pairing system, for example, and then identifying how that system can be integrated with other similar threat-based systems, we now identify the warfighting capabilities we want to achieve. Then we start with a "blank sheet of paper" to develop the systems architecture and technical standards necessary to allow seamless interaction using shared data and applications.

For instance, if our objective were to destroy a mobile inland target, we would identify the activities needed to accomplish our objective and the conditions and metrics required. In this case it would be the ability to: (1) detect the target; (2) track the target; (3) identify the target; (4) engage; and (5) assess the engagement, all within the required time line. This capability could be realized with a traditional solution, such as today's connected command and control (C2) systems and a manned strike aircraft.

Capabilities-based acquisition can also provide something less expensive that doesn't put warfighters at risk, such as an autonomous, uninhabited vehicle with weapons launched from offshore. Ultimately, the focus of capabilities-based acquisition is to find a solution that provides the optimum warfighting adaptability, while maximizing combat power and minimizing investment costs.

Capabilities-based acquisition is a new way of doing business that has already significantly affected how DoD defines requirements and acquisition processes. It can give decision makers more power to invest limited resources in the most efficient way possible, improve system interoperability and enhance the operational superiority of our military forces. The Navy's Mission Capability Packages (MCP) analysis and the Joint Capabilities Integration and Development System (JCIDS) are two examples of how this concept is affecting current acquisition efforts.

Engineering Challenges

Implementing capabilities-based acquisition is obviously much more complicated than the previous scenario, especially when considering the requirement to advance netcentric warfare concepts. Now, we face the challenge of not only transitioning from a traditional platform-centric paradigm, so called "stovepipe" acquisition, but also of moving to completely new modes of warfare where sensors and weapons on multiple platforms could serve as resources controlled by a variety of users on a network.

The implications for netcentric warfare on military operations, as well as the overall DoD culture, are immense and naturally beyond the scope of this article. Instead, we will examine how the engineering and architecture communities are working to make this paradigm shift happen, and we will give one example of this approach.

Managing the Transition

To effectively acquire complex systems of systems in a capability-based acquisition environment requires that we increase the use of integrated architectures to identify inter-relationships and resolve issues with system integration and interoperability that impact the operational effectiveness of warriors; platforms; sensors; command and control; networks; and weapons.

Well-defined architectures are an essential part of engineering assessments. They allow decision makers to look for the mix of assets that best optimizes the balance between cost and capability. The acquisition community determined that decision makers need the ability to perform detailed technical analysis, while maintaining traceability and repeatability. To support this need, the Space and Naval Warfare Systems Center, Charleston, S.C., spent four years developing and evolving the Global Engineering Methods Initiative for Integration and Interoperability (GEMINII).

GEMINII enables decision makers to understand the impact of their acquisition decisions. It captures capability-based analytical data, which helps to manage complexity in an almost ad hoc development environment. GEMINII meets the need for traceability and repeatability. It is both a process and a toolset based on achieving desired capabilities through activity decomposition, integrated architectures and semiautomated analysis of inter-system dependencies.

GEMINII development led to key lessons learned. Effective analysis must include information from the warfighter's perspective on capability definition, conditions, metrics, prioritization and impact on the Concept of Operations (CONOPS) and Tactics, Techniques and Procedures (TTPs).

Analysis requires information from an

acquisition perspective to analyze integrated architectures, which are candidates to meet the capability requirements. This includes dependencies on system milestones, migration plans and evolution strategies. Integrated architectures are also used to evaluate compliance with DoD and Naval architecture guidance.

The GEMINII process is only one example of how an enterprise environment can be developed. In this environment, it is critical to incorporate all of these authoritative sources wherever possible to facilitate the collection of complex information and minimize data calls.

Well-defined architectures are an essential part of engineering assessments. They allow decision makers to look for the mix of assets that best optimizes the balance between cost and capability.

If done properly, this process can produce a large quantity of information about complex systems of systems that can help guide programmatic decisions. Ultimately, the goal for this type of analysis is to help advance our understanding of both capabilities-based acquisition and netcentric warfare in engineering terms.

While the underlying philosophy of simultaneously tackling capabilities-based acquisition and netcentric warfare appears to go hand-in-hand, connecting the dots with analytic rigor can be extremely complex. The concept of netcentric warfare is centered on the ability of a warfighter to assemble services and information as needed, when needed. Services could be whatever warfighting capabilities are required by the user at any given time.

Making it Real: *a solution space*

Tools themselves can not provide capabilities-based acquisition. But when tools are combined with an integrated process to build a knowledge base, the results can be revolutionary. *Knowledge* emerges when the tools and process are combined. This knowledge can be applied effectively to yield a true capabilities-based acquisition paradigm.

The significant challenge from a knowledge discovery and management perspective; however, is to ensure that the process is automated (for quick turnaround time), repeatable (for stability of results and applicability to multiple suites of capabilities) and traceable (results mapped back to authoritative data sources).

The work being done by the SPAWAR Chief Engineer, SPAWAR Systems Center Charleston, and others, for implementing capability-based acquisition, focuses on increasing the speed and automation of engineering assessments of end-to-end warfighter capabilities, mapping capability to integrated architectures and portfolio management.

The ultimate goal for capabilities-based architectures is to provide a cost-effective analysis of alternative capabilities, system configurations and option characteristics (schedule, performance and costs) at any level of detail desired by a decision maker, structured so that all analysis and current issues are traceable.

This analysis process begins by breaking down warfighter capabilities into end-to-end mission descriptions by activity, information, platforms, systems and components. A static assessment is performed at this point to identify known interoperability issues based on authoritative databases of lessons-learned and technical problems.

Once the end-to-end mission capability descriptions are complete, the enterprise analysis environment can implement those components using a variety of modeling tools, such as Network Warfare Simulation (NETWARS) or the JUDY Theater Surveillance and Strike Simulation Model, to assess technical performance. Selection of the specific modeling tool is based on the appropriate validated model by determining which tool offers the best fidelity for the specific question.

Just because systems are interoperable and comply with network-centric warfare concepts does not necessarily mean that they will improve force effectiveness. To track improvements in warfighting, the GEMINII process incorporates campaign-level modeling tools such as the Joint Warfare System (JWARS) or the Naval Simulation System (NSS) to assess architectural decisions, component choices and acquisition assumptions against operational results and outcomes. Ultimately, this process can provide increased automation of system technical assessments, offering a rapid, cost-effective decision support environment.

The Way Ahead

In summary, the optimal decision support environment created by the integration of tools and an analytical capability is necessary to make informed decisions regarding Navy and joint capability acquisition.

The engineering and architecture communities are working together to provide the analytic tools needed to make capabilities-based acquisition a reality. And, they are evolving the process to support acquisition leadership by merging warfighter capabilities with integrated architectures. This proven process has already provided an effective framework for integrating all the factors required to rapidly deliver end-to-end capability to the warfighter.

Mr. Philipp Charles is the chief engineer for SPAWAR Systems Center Charleston. He provides technical leadership to 2,200 government personnel performing more than $2 billion worth of C4ISR technical business per year. He is also the coauthor of Using Architectures for Research Development and Acquisition, DoD Deskbook Series. After serving in the U.S. Marine Corps, he earned a bachelor's degree in electrical engineering from Rutgers University and a master's degree in engineering management from the Florida Institute of Technology. He is also a graduate of the Federal Executive Institute.

Lt. Cmdr. Phil Turner, an engineering duty officer, is currently assigned as the deputy chief engineer, SPAWAR Systems Center Charleston. In this position he has served as program manager for the Naval Tool for Interoperability Risk Assessment (NTIRA). He has led numerous architecture assessment efforts for the Office of the Chief of Naval Operations (OPNAV), SPAWAR headquarters and the Chief of Naval Operations Strategic Studies Group. He earned a bachelor's degree in history from the U.S. Naval Academy and bachelor's and master's degrees in astronautical engineering from the Naval Postgraduate School.

IT Sailors, Navy and EDS Reap Benefits of NMCI

By Eric T. Mazzacone, NMCI Director's Office Public Affairs

Navy forces afloat rely heavily on Information Systems Technician Sailors to maintain shipboard access and connectivity to IT-21. In fact, the Navy is "building a cadre of IT Sailors at sea who are very familiar with IT-21 operations, and who are becoming extremely literate in the management of tough technical issues with regard to IT connectivity," said Commander Naval Network and Space Operations Command (NNSOC), Rear Adm. John P. Cryer, in a briefing March 31, 2004.

These IT management skills are not going to waste when Sailors complete their sea duty tour. According to Cryer, many of those Sailors are returning to shore as part of the IT Military Detachment (MILDET) program to work alongside contractor personnel in the NMCI Network Operations Centers (NOCs) to gain more hands-on experience and enhance their technical skills prior to returning to the fleet.

"It was determined a long time ago that it would be very valuable as we stood up NMCI to provide an opportunity for these folks to go from sea duty to shore duty to work closely with the contractors to develop skills, which would be useful for the Navy at sea," said Cryer.

The training program has been "an unqualified success" according to Cryer, who explained that the benefits surrounding the program are threefold. "For the Navy at large we are reaping the benefit of these technical skills; the Sailors themselves are benefiting from the opportunity to receive this type of education; and clearly the industry is benefiting by the strong workforce that is partnering with them as we go through the process of getting NMCI up and operational."

Lt. Antonio Scurlock, NMCI enterprise training officer for NNSOC, provided details during the same briefing regarding the type of training Sailors are receiving. "MILDET Sailors are afforded the opportunity through an internship-like program to achieve Cisco, Microsoft and CompTIA certifications."

The sixty-month program, according to Scurlock, requires Sailors to spend "36 months rotating through various positions within the NMCI detachments (including the areas of help desk, systems, network, information assurance and base operations support) and 24 months at sea. The program is geared to place Sailors on afloat platforms in information technology critical billets, in order to keep those afloat units connected to the Global Information Grid [GIG]."

Perhaps one of the most critical aspects of the program is that it "develops a military member who is fully capable of administering, maintaining, analyzing and securing enterprise-wide networks, while ensuring a more responsive, highly-trained Navy system administrator is available to the fleet," explained Scurlock.

The first Marines are expected to report for duty to the Marine Corps Training Detachments within the NMCI NOCs in July 2004.

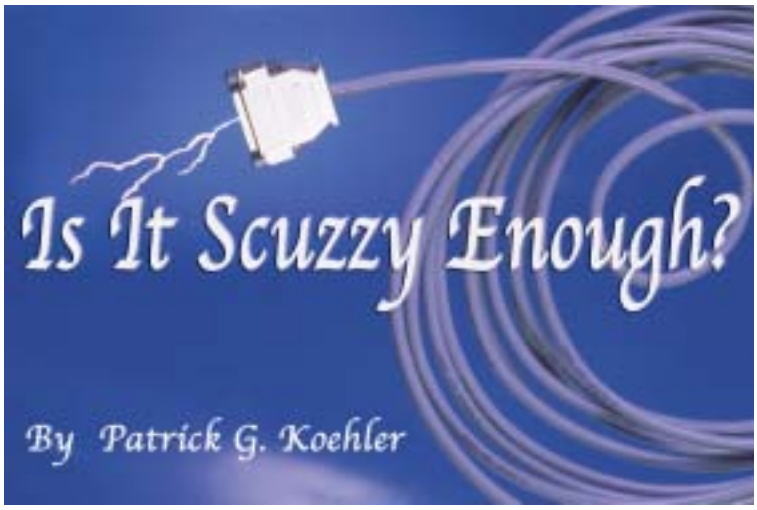
For more information regarding requirements for assignment to an NMCI MILDET go to http://www.nmci.navy.mil/Primary_Areas/Personnel/index.htm.

Eric Mazzacone now supports the National Guard. Article and NMCI statistics reprinted by the permission of the director of the NMCI Office.

NMCI by the Numbers

as of May 18, 2004

304, 324	**Seats in AOR**
179,629	**Seats in cut over**
0	Disruptions in Service
1	Department of the Navy Network
2	Enterprise Help Desks; 1,110,574 total contacts to Help Desks in CY 2003; 764,041 Trouble Tickets opened; 753,830 closed
4	Network Operations Centers (NOCs): Norfolk, San Diego, Oahu, Quantico
6	Classified server farms built; 21 planned; 41-terabyte storage capacity
24	Unclassified server farms built; 31 planned; 263-terabyte storage capacity
24/7/365	Enterprise Level Service
10 - 15%	Typical annual cost reduction that industries achieve by reducing the cost of the business process, i.e., server consolidation, application hosting, VoIP, Web services, etc.
45	Service Level Agreements (SLAs)
263	Commercial professional and NEC certifications attained by NOC-assigned Sailors to date — at no expense to the government
240	Separate performance measurement categories
4,000	Separate sites
1,000	Individual DON IT contracts assumed by EDS to date
1,877	Joint users at PACOM HQ
1,328	Seats deployed in support of Operation Iraqi Freedom and the global war on terrorism
2,033	New viruses detected in CY 2003; NMCI infected by 1 – Welchia
$3,922	Average price of a FY 2004 seat order
67,000	Navy legacy applications documented; 6,900 approved by VCNO for NMCI; 90% reduction
323,000	Users supported under the NMCI contract to date
700,000 +	Estimated users at end state
267,727,280	Unauthorized access attempts blocked at the outer routers in CY 2003; 30,563 attempts per hour, every hour of the day
$2,400,000,000 - $3,300,000,000	Estimated investment costs avoided by DON in contracting for service through NMCI
$8,900,000,000	Estimated value of contract including option years
$1,500,000,000	NMCI budget for FY 2004; about 24% of total DON IT budget



What is scuzzy? Scuzzy refers to the small computer system Interface (SCSI). SCSI is a parallel interface standard used to connect external hardware such as tape drives, removable drives, external CD-ROMs, etc., to personal computers, Unix systems and Apple Macintosh computers.

SCSI popularity was stifled by the onslaught of new technologies such as Firewire (IEEE 1394) and Universal Serial Bus (USB), but it continues to evolve and is the preferred choice for large servers or systems that support many peripheral devices. SCSI's backward compatibility and legacy support are the principal reasons for its survivability. Powerful computer operating systems using Microsoft Windows, OS/2 and Unix support multithreading and multitasking and helped SCSI devices gain in popularity.

SCSI features support many different components, allow faster data transfer and provide connection for multiple internal and external peripheral devices. Let's examine SCSI standards, characteristics and tips for buying SCSI peripherals. There are three SCSI standards: SCSI-1, SCSI-2 and SCSI-3. SCSI-2 is still in use, but SCSI-3 is the current standard.

A summary of current SCSI options includes:	
SCSI-1	8-bit bus supporting data rates of 4 MBps
SCSI-2	Same as SCSI, but with a 50-pin connector instead of a 25-pin connector to support multiple devices
Wide SCSI	Uses a wider cable (168 cable lines to 68 pins) supporting 16-bit transfers
Fast SCSI	8-bit bus, but doubles the clock rate supporting data rates of 10 MBps
Fast Wide SCSI	16-bit bus supporting data rates of 20 MBps
Ultra SCSI	8-bit bus supporting data rates of 20 MBps
SCSI 3	16-bit bus supporting data rates of 40 MBps. Also referred to as Ultra Wide SCSI

The Shugart Associates System Interface (SASI), a predecessor to SCSI, was developed in 1979. The American National Standards Institute (ANSI) ratified the first standard in 1986 calling it SCSI-1. SCSI-1 did not share a common standard which caused equipment incompatibilities. The first design had a narrow 8-bit bus, slow speed and short cable length. SCSI-1 included a single-ended (SE) transmission supported by a passive termination.

SCSI-2 was the revised, compatible standard, ANSI approved in 1994. A common command set was established so that a Seagate SCSI drive could easily work with an Adaptec SCSI or Western Digital controller. SCSI-2 was a definitive enhancement over SCSI-1. SCSI-2 featured a wider data bus doubling in size from 8- to 16-bit supporting 16 devices. The SCSI adapter takes up one device ID number. A Fast-Wide SCSI-2 can support up to 15 devices because the adapter requires one SCSI ID. SCSI-2 also introduced differential signaling methods: High Voltage Differential (HVD) and Low Voltage Differential (LVD).

HVD and LVD signaling methods increase data transfer speed and lengthen the signal on the SCSI cable. Technology enhancements further evolved SCSI-2 devices by using active and forced perfect termination (FPT) methods. The update added a new command set to support tape drives, CD-ROMs and CDR/RWs. SCSI-2 includes command queuing to allow a server or system to handle multiple requests at the same time, which increases performance for server farms, clusters and Storage Area Networks (SANs). Ultra SCSI-2 and Wide Ultra SCSI-2 increase data performance.

Internet SCSI (iSCSI) transmits data over Internet Protocol (IP). It is a protocol-based standard ratified by the Internet Engineering Task Force (IETF). iSCSI brings a new approach to data storage by using Host Bus Adapters (HBA) that appear to be like a network interface card (NIC) on the network that has its own IP address to communicate. The server then transfers data to the iSCSI device. This transfer is transparent to the user. iSCSI uses the common Ethernet infrastructure to communicate with the server, and it is flexible and easy to maintain.

iSCSI works with the new 10 Gigabit Ethernet standard to perform high speed data transfers, which are much faster than the typical NAS (network-attached storage) or SAN device. There is a security concern with iSCSI. As with other SCSI devices, encryption was not built-in, so a third party device, software or operating system configuration may be required.

Serial Attached SCSI, or SAS, is a recent standard that takes SCSI to new heights with faster data transfer rates that can travel greater distances. SAS brings to the table point-to-point topology using dedicated disk connections with scalable throughput. SAS performance has risen to 3.0 GBps (300 MBps) in 2004, doubling the 1.5 GBps (150 MBps) throughput available for Serial ATA (Advanced Technology Attachment) in 2002. It allows smaller cables for improved air flow while providing fewer signals for high density routing. SAS has good disk and backplane interoperability offering a wide range of deployment options. SAS is less expensive with the added benefit of ATA compatibility, which simplifies the upgrade process and keeps maintenance costs down.

Here are a few tips for selecting SCSI components.

• Signaling: Select the correct signaling, considering the distance between your controller and the target device(s). There are three types of signaling methods: SE, HVD and LVD. SE has a much shorter signal range (10 feet) than LVD (40 feet) or HVD (80 feet). The signaling method used is affected by the data bus width and whether it is 8- or 16-bit. The narrow data bus limits the cable length.

An important consideration in picking a SCSI adapter and devices is how long the cable has to be to connect all your SCSI internal and external devices. Length is affected by the data bus width, SCSI standard and whether you are connecting two or more devices. HVD signaling assures of you maximum cable length.

• Terminating: There are three types of terminators for SCSI devices: passive, active and FPT. Passive termination is rarely used today because it was designed for low-speed and short distance SCSI-1 devices. Active termination adds voltage regulators to the resistors used in passive termination, which allow more reliable and consistent termination of the bus. FPT eliminates any signal reflections and provides the best form of termination for a single-ended SCSI bus. The SCSI chain must be properly terminated on both ends. Improper termination will cause devices not to be recognized, and you may lose data or have connections that phase in and out.

• Selecting IDs: SCSI ID numbers are based on the size of the bus. The 8-bit bus supports 8 devices (0 - 7), the 16-bit bus increases support to 16 devices (0 - 15). The SCSI host adapter requires an ID number and will typically take the last one such as 7 or 15. If you are using a SCSI hard disk, the boot drive will take the first ID, which is 0. You can assign ID numbers to SCSI devices. SCSI plug and play host adapters typically make assigning IDs easy.

The SCSI standard arbitrates or decides which device has control of the bus first. In a narrow bus, the numbers 0-7 would be arranged with 7 being the highest priority and 0 being the lowest. In the case of 16-bit wide data bus, the numbers 0-7 still take a higher priority than the numbers 8-15. So a wide SCSI would have the following numbers from the highest priority to the lowest as 7, 6, 5, 4, 3, 2, 1, 0, 15, 14, 13, 12, 11, 10, 9 and 8.

When manually assigning SCSI devices keeping the boot drive ID as 0 will alleviate any potential problems with older software or hardware. Ensure that all SCSI IDs are different. If you have two SCSI IDs that are the same, only one device will be recognized. You could connect more than one SCSI host adapter to another adapter and connect 8 (or 16) additional devices.

•Using the right connector: There are three primary types of connectors. SCSI connectors include Type A (50-pin) for 8-bit SCSI, Type P (68-pin) for 16-bit SCSI and an 80-pin high-density connector called a single connector attachment (SCA) or an SCA-2. SCA, developed for use with Redundant Arrays of Independent Disks (RAID), allows you to replace hot swappable drives in a server while the server is still running. This is important for businesses that cannot afford to have their systems go down.

RAID uses multiple hard disk drives in an array that can be treated as a single logical entity. The series of drives can be formatted and partitioned like a single large, fast drive. This technology can be used to store duplicate copies of data on drives that are exactly the same. If one drive fails, it can be removed and replaced without losing any data.

Mixing narrow and wide SCSI devices can cause problems. First obtain a SCSI host adapter that will support separate segments or channels for connecting both narrow and wide devices. Be careful not to place LVD and SE on the same channel. If you place wide SCSI devices on the same chain as narrow devices, you will not only need a separate connector, but you will also reduce the wide bus throughput to the narrow speed. Narrow SCSI hardware cannot "see" over 7, so if you connect narrow devices to a wide adapter, the other 8 bits will have to be terminated. Use a high byte termination connector to get rid of extra signals so the narrow device can operate on a wide SCSI chain.

SCSI components rank supreme when it comes to connecting multiple devices together such as operating a server farm or setting up a server cluster or central data repository using multiple hard drives. Parallel SCSI is a proven technology with more than 20 years of reliability, flexibility and robustness.

For additional information, go to these Web sites:

√ American National Standards Institute – http://www.ansi.org is the home for ANSI standards. Related SCSI standards such as SAS, SCSI Fibre Channel and more are listed. There is a fee to download ratified SCSI standards.

√ SCSI Trade Association and Serial ATA Working Group – http://www.serialattachedscsi.com and http://www.serialata.org are sites devoted to the new SAS standard.

√ SCSI Source – http://www.scsisource.com for SCSI components, cables, etc.

√ Computer Cable Makers, Inc. – http://www.cablemakers.com for SCSI connectors, adapters, etc.

√Tech Support Alert – http://techsupportalert.com for information on SCSI installation.

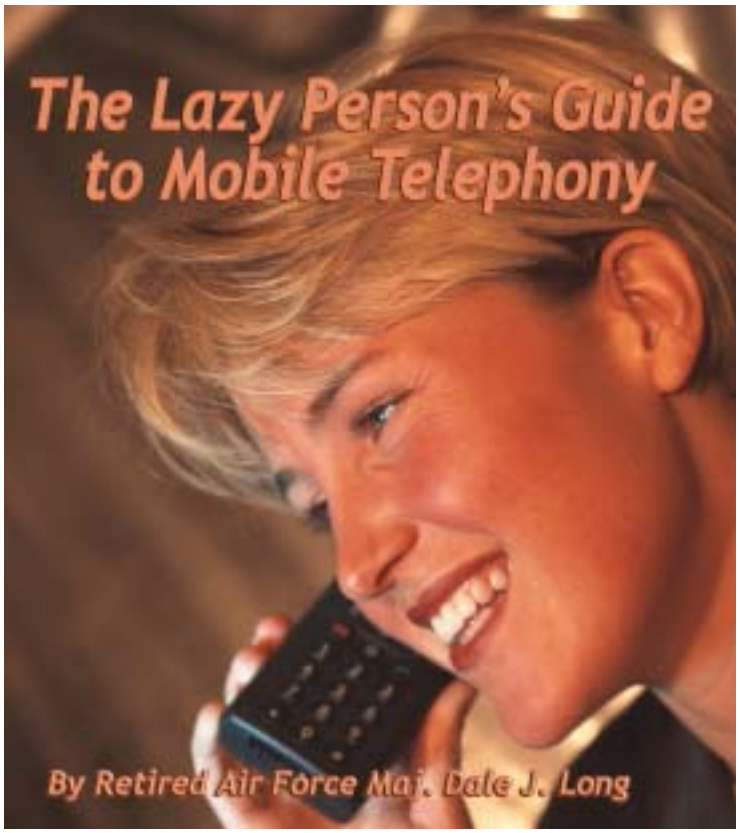
√ Adaptec, Inc. – http://www.adaptec.com/worldwide/support/driverindex.jsp?sess=no for Adaptec SCSI drivers.

√ CNET Networks, Inc. – http://download.com for all types of drivers.

√ DriverGuide.com – http://www.driverguide.com for all types of drivers.

Go to the Department of the Navy Information Technology (DON IT) Umbrella Program contract pages 46 - 51 or Web site at http://www.it-umbrella.navy.mil for savings on hardware, peripheral devices, software and much more.

Koehler is a member of the Technical Support & Acquisitions Branch. He has a bachelor's degree in computer information systems and holds certifications in A+, Network+, CCNA, MCDBA 2000, MCP/MCSA/MCSE Windows 2003, MOS Outlook/PowerPoint 2002, Security+ and Server+.



In the last two installments of the Lazy Person's Guide, we reviewed the history and development of analog and digital telephone systems and looked at Voice over Internet Protocol (VoIP). In this issue, we will detach ourselves from the wired world and look at mobile telephony, which may well dominate the world's communication environment within the next 10 years.

Mobile telephony is a good example of the behavioral dilemmas associated with convenience technology. People want the freedom to take a telephone everywhere. Then they complain that they have less freedom because people can call them any time, day or night. Enabling or annoying, mobile telephony is here to stay. Let's take a look at what it is, how it developed and where it may go.

Cellular History

Cellular telephone technology is a hybrid of radio transmission, wide-area networking and traditional telephony. This type of technology is called "cellular" because the system uses base stations to divide a service area into multiple "cells." As a user travels from cell to cell, cellular calls are transferred, or "handed off" from base station to base station.

The cellular telephone is essentially a radio, albeit an extremely complex one. The roots of cellular telephone service stretch back to the mid-19th century. In 1843, chemist Michael Faraday, arguably the world's first expert on electro-magnetism, began exhaustive research into whether or not "space" could conduct electricity. He discovered that the atmosphere could, under certain conditions, conduct energy. His work became the basis for all future work in radio communications.

After Faraday, Dr. Mahlon Loomis of Virginia developed a method of transmitting and receiving telegraphic messages by using the Earth's atmosphere as a conductor. His system used kites linked to the ground with copper wires, laced with copper screens. Between 1866 and 1873 he conducted several demonstrations where he transmitted messages without wires at distances of 14 to 18 miles. A generation before Marconi gained fame for his work with radios, Loomis was the first person to build complete antenna and ground systems, the first to successfully transmit wireless telegraph signals, the first to conceive the idea of transmission traveling in "waves" from his antenna, and he was the first person awarded a patent for wireless telegraphy. Unfortunately, Loomis never gained any significant recognition for his work and many contemporaries thought him a crackpot and fraud. However, Loomis undoubtedly inspired at least some of what came afterward.

The first mobile telephone was installed in a car by the Detroit Police Department in the early 1920s. The basic concept of cellular telephone service began to take shape in 1947 when researchers tried to improve the range of crude mobile car phones by using small service areas (cells) that shared the same frequencies. But the technology needed to support the concept did not exist at the time.

Another problem was prevailing policy. The Federal Communications Commission (FCC) considered mobile phones a type of two-way radio. In 1947, AT&T asked the FCC to allocate a large band of radio frequencies for cellular use. This would allow mobile phone service on a large enough scale to give AT&T an incentive to research cellular technology for commercial use. But the FCC decided to limit cellular phone frequencies so that only 23 cellular phone conversations could occur simultaneously in the same service area. That wasn't much of an incentive.

In 1968, the FCC reconsidered, and said it would increase mobile telephone frequencies if new technology improved the process. AT&T Bell Labs proposed the cellular telephone system we know today. In 1973, Dr. Martin Cooper, a former general manager at Motorola, set up a base station in New York with the first working prototype of a cellular telephone, the Motorola Dyna-Tac. Dr. Cooper is generally considered both the inventor of the first portable handset and the first person to make a call on a portable cell phone.

In 1977, public cellular telephone testing began in Chicago with 2,000 customers. However, because of the high cost of providing the infrastructure, cellular service did not progress beyond the testing stage until the Cellular Technology Industry Association issued practical guidance for cellular telephone providers in 1988. At that point the research and development framework was in place and demand was becoming strong enough to drive commercial development.

Cellular Evolution

The first cellular services used analog signals operating at 800 megahertz (MHz). While these early analog phones worked, they suffered from short battery life because of the power required to transmit the continuous wave used in analog systems. Advances in control systems allowed analog systems to carry 56 calls within a cell, instead of the original 23. Modern cell phones have mostly moved to digital transmission.

Unlike analog, which broadcasts a continuous stream, digital cellular systems sample pieces of the wave, divide it into chunks, and send it in bursts of data. Digital systems make better use of bandwidth, are somewhat more secure and use a lot less power when broadcasting. In addition to the digital shift, a change from nickel-cadmium to lithium-ion batteries significantly increased the average talk/standby time for cell phones.

The most common digital transmission systems use Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA). Cellular TDMA allows three different transmissions to share the same frequency by slicing each of them into pieces that take turns on the wavelength. For the technically-minded among you, it uses 30-kHz channel spacing and three time slots. This allows a cellular TDMA to carry three times as many (168) conversations as an analog cellular system.

CDMA uses a different approach. Each call is identified with a unique sequence code and sliced into pieces that may be broadcast over any available frequency within the entire available bandwidth. This is a form of "spread spectrum" technology, and it makes very efficient use of the available bandwidth of any cellular technology.

There is one other type of cellular system: Personal Communications Service (PCS). PCS is similar to other cellular phone services in its ability to carry voice traffic, but it also includes information-based personal services that are not part of traditional cellular voice services like paging, caller ID, Web browsing and e-mail. Remember, cell phones were originally invented with a limited set of functions for use in cars. PCS was designed by someone who took the time to study the behavior and information needs of people with the goal of making the PCS phone a digital hub. PCS uses TDMA, but a more robust version with 200-kHz channel spacing and eight time slots instead of the 30-kHz channel spacing and three time slots found in the older digital cellular version.

Modern cell phones are evolving at a faster rate than many other consumer technologies, adding new features almost daily. I think the cell phone will eventually become the principal mobile convergence device for most people based on its ability to combine information storage, access, portability and functionality.

Mobile Gestalt

Close inspection of modern cell phones will disclose an impressive array of information technologies packed into a relatively small package, including personal information managers, Internet Protocol capability, Web browsers, file storage systems, portable storage media, multimedia recorders/players, e-mail clients and wireless networking. It's not always a seamless or comprehensible whole, but vendors are getting better at integrating functionality and users are getting smarter about using their "pocket myriads."

The convenience of having any functionality available in one device will be too strong to ignore. There will; however, be some speed bumps along the way. Security will always be an issue. Any time you put all your eggs in one basket, you'd better watch that basket very carefully. Second, the current size and resolution of cell phone screens severely limit the type and amount of information you can present to a user. However, there has been some progress made in display technology in the last few months that will eventually find its way into cellular telephones.

The most striking example of this is the Sony development of "Librie," an electronic reader that reportedly has a 6-inch black and white screen with resolution of 600x800 dots at 170 dpi (dots per inch). The Librie's screen achieves this level of sharpness by using microcapsules 40 microns (A micron is one millionth of a meter.) in diameter that contain dozens of charged black and white particles (with opposite charges) suspended in an oil solution. The device uses electromagnetic fields to draw black or white particles to the surface of each capsule to render the image.

Until now, the best resolution available commercially in electronic displays has been about 150 dpi in high-end liquid crystal display (LCD) computer monitors. While this is considerably sharper than the 80 dpi of a regular computer display, it's not as close to the 200 dpi distinguishable by the human eye. And though the Librie only displays black and white or grayscale static images at the moment, research is apparently underway to modify the technology to accommodate motion and color.

The biggest challenge will be in finding appropriate uses for all this power at our fingertips. For some people, the only thing they will ever really do with a cell phone is call someone else. In those cases, any extra features might as well not be there. Before we take a more detailed look at the functionality of today's cell phones, let's look back at what happened with a somewhat similar attempt at mobile convergence about 14 years ago.

Radio Zippy

In 1990 I was assigned to an aircraft and ammunitions maintenance unit at a tactical fighter wing in the United Kingdom. Mobile telephones were an unknown luxury. Our principal mobile communication device in that era was the Land Mobile Radio (LMR), also known as "the brick" due to its size and weight. Someone got the bright idea to incorporate a telephone keypad on an LMR and develop a bridging system that would allow you to place phone calls through the radio base system to the base telephone system.

One day I was sitting down to lunch with another young captain named Dan when the wing vice commander decided to join us for lunch. Trailing the vice commander like a pilot fish follows a great white shark was Zippy, who had been temporarily detailed from the base communications squadron as the colonel's executive assistant. The vice commander had one of the new radio-phones and was waxing poetic about the possibilities of having his phone and radio in a single device. For example, he thought it would be convenient if instead of having to find a phone, he could call on his radio to reserve a racquetball court for later that afternoon. Zippy, never one to miss an opportunity to either play with a new toy or score some points with the boss, immediately volunteered to try it with the vice commander's new brick.

Five minutes later, both Zippy and the vice commander were a little red around the collar because the handheld refused to cooperate. If someone didn't intervene soon, Dan and I would forever be linked in the vice commander's mind with both Zippy and his

uncooperative LMR. Deciding that I had nothing to lose, I said, "Sir, I can show you how to reserve a court with that thing." Without a word, the vice commander plunked the radio down and gave me one of those focused stares he normally reserved for the gunsights of his A-10 Thunderbolt. To tell the truth, I hadn't the faintest clue how to make a phone call on that radio. But I did know how to get the court reserved. Hoping the vice commander still had a sense of humor, I picked up the radio, switched to the maintenance control center channel and thumbed the transmit key.

"EM-3 to MCC."
"MCC acknowledge. Go ahead EM-3."
"Copy MCC. Would you please call the gym and reserve a racquetball court for CV at 1600 today? Over."
"Copy that, EM-3. Wilco and out."

I looked at the vice commander. He had one eyebrow arched up and a thoughtful expression on his face. Then he laughed, took his brick back and said, "Point taken." If there's one thing a good operator appreciates, it's the simplest, most direct answer to a problem. All he wanted was a way to communicate; it didn't matter how, as long as you got the job done. There are reasons for "radio discipline," and making phone calls via the radio violated most of them. Every radio-phone call would occupy one of the precious radio frequencies we had available for operational communications. The test of the new radio-phones quietly faded off the radar.

Modern Mobility

Our radio-phone experiment didn't quite work out for two reasons: The technology was complex beyond most people's ability to use it, and there were simpler, less costly ways to get the same thing done. We are faced with a similar situation with cellular telephones. They are becoming more functional, but more complex. While a cell phone can include a lot of functions in one portable unit, it is second-best at most of them when compared to more traditional technologies. Here's a quick list of some of that functionality with my opinion of its usefulness.

Text Messaging: This feature was originally added to cell phones in Japan; allegedly so that teenagers on trains could chat with each other when it was too noisy to use their phones. Other uses are for short, quick alerts, much like a pager. It can be a pricey feature when used for sending messages.

Web Browsing: You can access any Web service from anywhere you have cell phone access. Viewing most Web pages on a cell phone screen is often like looking at something through the wrong end of a telescope. But as more people access the Web from cell phones, more sites should move to a more readable format.

E-Mail: While screen size is still a constraint, text-only e-mail works fairly well on devices designed for it like the RIM (Research in Motion) Blackberry or Handspring Treo.

Video Games: Cell phones have view screens and buttons. It is inevitable that games could become a favorite way to drain the battery.

Digital Cameras/Video: This is handy if you need to snap and send something quickly, but the picture resolution is not great, and most cell phones will only send directly to another cell phone on the same service. There are also cellular telephone vendors trying to incorporate television into cell phones. If we have cell phones so we can talk to each other, do we really want to drain the battery watching a television rerun?

Voice Recognition: There are phones that can recognize rudimentary voice commands, like: "Call Chad," but voice recognition is still fairly crude. There are companies working on telephones that will allow you to navigate through menus using voice commands, but they aren't ready for market yet.

Internet Protocol (IP): As I mentioned in the last issue, I think IP will eventually become the dominant technology in voice telephony, and combined with cell phones, it may completely transform the telephony landscape in the next 10 years. First we'll have to overcome a huge legacy artifact: The plain old phone dialing system with it's reliance on geographically-based area codes and strict numbering systems. Maybe someday you will be able to get one portable phone number that will follow you wherever you go, much like a Web-based e-mail address, but it will take a commitment from the telecommunications industry and regulators to change how we dial calls. VoIP may provide the needed lift.

Built-in Personal Digital Assistants: I'm going to test this one personally. When my Kyocera 7135 arrives, I will finally be able to share one personal contact database between my cell phone PDA, Microsoft Outlook on my PC and my Nortel Meridian telephone, and I will have achieved one of my ultimate personal convergence goals.

There are a few off-the-wall things I've heard reported in cellular telephone research and development. One vendor offers foreign language flash cards, Scholastic Aptitude Test practice drills, a metronome, an Etch-A-Sketch and a tide clock. In Korea, SK Telecom offers ring tones that it claims can repel mosquitoes. Two Romanian inventors are reportedly working on a handset that will include a built-in sensor to detect smoke or toxic gases. Last summer Japanese inventors unveiled a tiny ultraviolet light sensor for cell phone users concerned about sunburn.

The main limiting factor in cell phone technology today is the battery. The more you add to the unit, the more power it requires. Soon I expect to see phones with solar panels that can recharge or prolong usage. As more surface area means more power gathered, perhaps there will even be clothing made with solar power collectors that we can plug our telephones into. I suppose anything is possible in a world that is rapidly becoming accustomed to instantaneous, direct personal communications with anyone, anywhere, anytime.

Until next time: Happy Networking!

Long is a retired Air Force communications officer who has written regularly for CHIPS since 1993. He holds a Master of Science degree in information resource management from the Air Force Institute of Technology. He is currently serving as a telecommunications manager in the U.S. Department of Homeland Security.

Enterprise Software Agreements Listed Below

The **Enterprise Software Initiative (ESI)** is a Department of Defense (DoD) initiative to streamline the acquisition process and provide best-priced, standards-compliant information technology (IT). The ESI is a business discipline used to coordinate multiple IT investments and leverage the buying power of the government for commercial IT products and services. By consolidating IT requirements and negotiating Enterprise Agreements with software vendors, the DoD realizes significant Total Cost of Ownership (TCO) savings in IT acquisition and maintenance. The goal is to develop and implement a process to identify, acquire, distribute and manage IT from the enterprise level.

In September 2001, the ESI was approved as a "quick hit" initiative under the DoD Business Initiative Council (BIC). Under the BIC, the ESI will become the benchmark acquisition strategy for the licensing of commercial software and will extend a Software Asset Management Framework across the DoD. Additionally, the ESI was incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74 on Oct. 25, 2002, and DoD Instruction 500.2 in May 2003.

Unless otherwise stated authorized ESI users include all DoD components, and their employees including Reserve component (Guard and Reserve) and the U.S. Coast Guard mobilized or attached to DoD; other government employees assigned to and working with DoD; nonappropriated funds instrumentalities such as NAFI employees; Intelligence Community (IC) covered organizations to include all DoD Intel System member organizations and employees, but not the CIA nor other IC employees unless they are assigned to and working with DoD organizations; DoD contractors authorized in accordance with the FAR; and authorized Foreign Military Sales.

For more information on the ESI or to obtain product information, visit the ESI Web site at http://www.don-imit.navy.mil/esi.

Software Categories for ESI:

Business and Modeling Tools

BPWin/ERWin

BPWin/ERWin - Provides products, upgrades and warranty for ERWin, a data modeling solution that creates and maintains databases, data warehouses and enterprise data resource models. It also provides BPWin, a modeling tool used to analyze, document and improve complex business processes.

Contractor: ***Computer Associates International, Inc.*** (DAAB15-01-A-0001)

Ordering Expires: 30 Mar 06

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Collaborative Tools

Envoke Software (CESM-E)

Envoke Software - A collaboration integration platform that provides global awareness and secure instant messaging, integration and interoperability between disparate collaboration applications in support of the DoD's Enterprise Collaboration Initiatives.

Contractor: ***Structure Wise*** (DABL01-03-A-1007)

Ordering Expires: 4 Sep 05

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Click to Meet Software (CT-CTM)

Click to Meet Software - Provides software license and support for Click to Meet collaboration software (previously known as CUSeeMe and MeetingPoint), in support of the DoD's Enterprise Collaboration Initiatives. Discounts range from 6 to 11 percent off GSA Schedule prices.

Contractor: ***First Virtual Communications, Inc.*** (W91QUZ-04-A-1001)

Ordering Expires: 05 Nov 08

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Database Management Tools

IBM Informix (DEAL-I/D)

IBM Informix - Provides IBM/Informix database software licenses and maintenance support at prices discounted 2 to 27 percent off GSA Schedule prices. The products included in the enterprise portion are: IBM Informix Dynamic Server Enterprise Edition (version 9), IBM Informix SQL Development, IBM Informix SQL Runtime, IBM Informix ESQL/C Development, IBM Informix ESQL/C Runtime, IBM Informix 4GL Interactive Debugger Development, IBM Informix 4GL Compiler Development, IBM Informix 4GL Compiler Runtime, IBM Informix 4GL RDS Development, IBM Informix 4GL RDS Runtime, IBM Informix Client SDK, IBM Informix Dynamic Server Enterprise Edition (version 7 and 9), and IBM Informix D.M. Gold Transaction Processing Bundle.

Contractor: ***IBM Global Services*** (DABL01-03-A-0002)

Ordering Expires: 30 Sep 04

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Microsoft Products

Microsoft Database Products - See information provided under Office Systems below.

Oracle (DEAL-O)

Oracle Products - Provides Oracle database and application software licenses, support, training and consulting services. Inventory exists for Navy customers, contact Navy Project Managers below for further details.

Contractors: ***Oracle Corp.*** (DAAB15-99-A-1002)
Northrop Grumman – authorized reseller
DLT Solutions – authorized reseller
Mythics, Inc. – authorized reseller

Ordering Expires: 30 Nov 04

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Special Note for Navy users:

Nov. 28, 2003, the Department of the Navy Chief Information Officer (DON CIO) executed an order for an Oracle Database Enterprise License for Ashore Navy programs and offices. This agreement provides significantly reduced pricing to programs and organizations for new products, reduced logistics costs by consolidation and management of maintenance and no escalation in maintenance costs for the next 10 years.

The Oracle Navy Shore Based Enterprise License will provide all U.S. Navy shore-based employees (including all full-time or part-time active duty, reserve or civilian U.S. Navy shore-based employees, not assigned to a ship) and U.S. Navy shore-based contractors (on-site contractors or off-site contractors accessing U.S. Navy owned or leased hardware for the purposes of supporting U.S. Navy shore-based operations) the ability to use Oracle Database Licenses without the requirement of individual programs or offices having to count users. The number of licenses required by the U.S. Navy will be managed at the DON CIO level. In accordance with the DFAR Supplement Subpart 208.74, if an inventory exists, new requirements must be purchased through

the DoD Enterprise Software Initiative following the related procurement process.

We are currently in the consolidation phase of this enterprise license agreement scheduled to be effective Oct. 1, 2004. Until that date, organizations should continue to operate in accordance with their current Oracle license agreement. If an organization's scheduled renewal is prior to Sept. 30, 2004, they will receive a prorated quote for maintenance support for the remainder of FY 2004. The intent of this prorating is to have all Navy shore-based Oracle maintenance contracts begin concurrently Oct. 1, 2004. Excess funds which result from this prorating should be reserved pending further guidance.

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/deal/oracle/oracle.shtml

Sybase (DEAL-S)

Sybase Products - Offers a full suite of software solutions designed to assist customers in achieving Information Liquidity. These solutions are focused on data management and integration, application integration, Anywhere integration, and vertical process integration, development and management. Specific products include but are not limited to Sybase's Enterprise Application Server, Mobile and Embedded databases, m-Business Studio, HIPAA (Health Insurance Portability and Accountability Act) and Patriot Act Compliance, PowerBuilder and a wide range of application adaptors. In addition, a Golden Disk for the Adaptive Server Enterprise (ASE) product is part of the agreement. The Enterprise portion of the BPA offers NT servers, NT seats, Unix servers, Unix seats, Linux servers and Linux seats. Software purchased under this BPA has a perpetual software license. The BPA also has exceptional pricing for other Sybase options. The savings to the government is 64 percent off GSA prices.

Contractor: ***Sybase, Inc.*** (DAAB15-99-A-1003); (800) 879-2273; (301) 896-1661

Ordering Expires: 15 Jan 08

Authorized Users: Authorized users include personnel and employees of the DoD, Reserve components (Guard and Reserve), U.S. Coast Guard when mobilized with, or attached to the DoD and nonappropriated funds instrumentalities. Also included are Intelligence Communities, including all DoD Intel Information Systems (DoDIIS) member organizations and employees. Contractors of the DoD may use this agreement to license software for performance of work on DoD projects.

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Architecture Tools

Rational Software (AVMS-R)

Rational Software - Provides IBM Rational software licenses and maintenance support for suites and point products to include IBM Rational RequisitePro, IBM Rational Rose, IBM Rational ClearCase, IBM Rational ClearQuest and IBM Rational Unified Process.

Contractor: ***immixTechnology,*** (DABL01-03-A-1006); (800) 433-5444

Ordering Expires: 25 Aug 05

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Popkin (AMS-P)

Popkin Products and Services - Includes the System Architect software license for Enterprise Modeling and add-on products including the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Extension, which provides specific support for the U.S. Department of Defense Architecture Framework (DoDAF), Envision XML, Doors Interface and SA Simulator as well as license support, training and consulting services. Products vary from 3 to 15 percent off GSA pricing depending on dollar threshold ordered.

Contractor: ***Popkin Software & Systems, Inc.*** (DABL01-03-A-0001); (800) 732-5227, ext. 244

Ordering Expires: 13 Apr 05

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Management

CA Enterprise Management Software (C-EMS)

Computer Associates Unicenter Enterprise Management Software - Includes Security Management, Network Management, Event Management, Output Management, Storage Management, Performance Management, Problem Management, Software Delivery and Asset Management. In addition to these products there are many optional products, services and training available.

Contractor: ***Computer Associates International, Inc.*** (DAAB15-99-A-0018); (800) 645-3042

Ordering Expires: 30 Mar 06

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Merant Products

Merant Products - Includes PVCS Change Management Software used to manage change processes in common development environments, release procedures and practices across the enterprise. All software assets can be accessed from anywhere in the enterprise. All changes can be entered, managed and tracked across mainframes, Unix or Windows platforms. The PVCS family also includes products to speed Web site development and deployment, manage enterprise content, extend PVCS to geographically dispersed teams and integrate PVCS capabilities into custom development workbenches.

Contractor: ***Northrop Grumman*** (N00104-03-A-ZE78); (703) 312-2543

Ordering Expires: 15 Jan 06

Web Link: http://www.feddata.com/schedules/navy.merant.asp

Microsoft Premier Support Services (MPS-1)

Microsoft Premier Support Services - Provides premier support packages to small and large-size organizations. The products include Technical Account Managers, Alliance Support Teams, Reactive Incidents, on-site support, Technet and MSDN subscriptions.

Contractor: ***Microsoft*** (DAAB15-02-D-1002); (960) 776-8283

Ordering Expires: 30 Jun 04 (Extension in progress)

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Resource Planning

Oracle

Oracle - See information provided under Database Management Tools on the first page of contracts.

PeopleSoft

PeopleSoft - Provides software license, maintenance, training and installation and implementation technical support.

Contractor: ***PeopleSoft USA, Inc.*** (N00104-03-A-ZE89); (800) 380-SOFT (7638)

Ordering Expires: Effective for term of the GSA FSS Schedule

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/peoplesoft/peoplesoft.shtml

SAP

SAP Software - Provides software license, installation, implementation technical support, maintenance and training services.

Contractor: ***SAP Public Sector & Education, Inc.*** (N00104-02-A-ZE77); (202) 312-3571

Ordering Expires: Effective for term of the GSA FSS Schedule

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/sap/sap.shtml

ERP Systems Integration Services

ERP Systems Integration Services - Provides the procurement of configuration, integration, installation, data conversion, training, testing, object development, interface development, business process reengineering, project management, risk management, quality assurance and other professional services for COTS software implementations. Ordering under the BPAs is decentralized and is open to all DoD activities. The BPAs offer GSA discounts from 10 percent to 20 percent. Firm fixed prices and performance-based contracting approaches are provided to facilitate more efficient buying of systems integration services. Five BPAs were competitively established against the GSA Schedule. Task orders must be competed among the five BPA holders in accordance with DFARS 208.404-70 and Section C.1.1 of the BPA. Acquisition strategies at the task order level should consider that Section 803 of the National Defense Authorization Act for 2002 requirements were satisfied by the BPA competition.

Contractors:

Accenture LLP (N00104-04-A-ZF12); (703) 947-1698

BearingPoint (N00104-04-A-ZF15); (757) 616-7162

Computer Sciences Corp. (N00104-04-A-ZF16); (856) 252-5583

Deloitte Consulting LLP (N00104-04-A-ZF17); (703) 885-6020

IBM Corp. (N00104-04-A-ZF18); (301) 803-6625

Ordering Expires: 03 May 09

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_services/erp-esi.shtml

Information Assurance Tools

Network Associates, Inc.

Network Associates, Inc. (NAI) - This protection encompasses the following NAI products: VirusScan, Virex for Macintosh, VirusScan Thin Client, NetShield, NetShield for NetApp, ePolicy Orchestrator, VirusScan for Wireless, GroupShield, WebShield (software only for Solaris and SMTP for NT), and McAfee Desktop Firewall for home use only.

Contractor: ***Network Associates, Inc.*** (DCA100-02-C-4046)

Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.

Web Link: http://www.don-imit.navy.mil/esi/

Antivirus Web Links: Antivirus software available for no cost download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: http://www.cert.mil/antivirus/antivirus_index.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/antivirus_index.htm

Symantec

Symantec - This protection encompasses the following Symantec products: Symantec Client Security, Norton Antivirus for Macintosh, Symantec System Center, Symantec AntiVirus/Filtering for Domino, Symantec AntiVirus/Filtering for MS Exchange, Symantec AntiVirus Scan Engine, Symantec AntiVirus Command Line Scanner, Symantec for Personal Electronic Devices, Symantec AntiVirus for SMTP Gateway, Symantec Web Security (AV only) and support.

Contractor: ***Northrop Grumman Information Technology*** (DCA100-02-C-4049)

Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.

Web Link: http://www.don-imit.navy.mil/esi/

Antivirus Web Links: Antivirus software available for no cost download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: http://www.cert.mil/antivirus/antivirus_index.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/antivirus_index.htm

Trend Micro

Trend Micro - This protection encompasses the following Trend Micro products: InterScan Virus Wall (NT/2000, Solaris, Linux), ScanMail for Exchange (NT, Exchange 2000), TMCM/TVCS (Management Console - TMCM W/OPP srv.), PC-Cillin for Wireless, Gold Premium support contract/year (PSP), which includes six POCs.

Contractor: ***Government Technology Solutions*** (DCA100-02-C-045)

Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.

Web Link: http://www.don-imit.navy.mil/esi/

Antivirus Web Links: Antivirus software available for no cost download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: http://www.cert.mil/antivirus/antivirus_index.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/antivirus_index.htm

Xacta

Xacta - Provides Xacta Web Certification and Accreditation (C&A) software products and consulting support. Xacta Web C&A is the first commercially available application to automate the security C&A process. The software simplifies C&A and reduces its costs by guiding users through a step-by-step process to determine risk posture and assess system and network configuration compliance with applicable regulations, standards and industry best practices, in accordance with the DITSCAP, NIACAP, NIST or DCID processes.

Contractor: ***Telos Corp.*** (F01620-03-A-8003); (703) 724-4555

Ordering Expires: 31 Jul 08

Web Link: http://esi.telos.com/contract/overview/

SecureInfo

SecureInfo - Enterprise Vulnerability Remediation (EVR) software allows IT managers the ability to automatically identify, track and correct vulnerability-related IT security material weaknesses. EVR distributes intelligence to the devices attached to the network to easily and quickly identify machines that require security fixes. With a single click of the mouse, administrators can confidently deploy patches that have been tested and approved to only the machines that need them.

Risk Management System (RMS) software offers organizations a highly automated certification and accreditation process that is customizable to meet the security requirements of enterprise networks. By utilizing extensive questionnaires, integrating specific requirements to exact standards and providing a straightforward

intuitive user environment, RMS addresses the challenges experienced by C&A specialists throughout each individual phase including: security policies; test plans; security procedures; system posture and reports; and management documentation.

Contractor: ***SecureInfo Corp.*** (FA8771-04-A-0301); (210) 403-5610

Ordering Expires: 19 Mar 09

Web Link: http://www.don-imit.navy.mil/esi/

Office Systems

Adobe

Adobe Products - Provides software licenses (new and upgrade) and maintenance for numerous Adobe products, including Acrobat (Standard and Professional), Approval, Capture, Distiller, Elements, After Effects, Design Collection, Digital Video Collection, Dimensions, Frame Maker, GoLive, Illustrator, PageMaker, Photoshop and other Adobe products.

Contractors:

ASAP (N00104-03-A-ZE88); Small Business; (800) 248-2727, ext. 5303

CDW-G (N00104-03-A-ZE90); (877) 890-1330

GTSI (N00104-03-A-ZE92); (800) 999-4874, ext. 2578

Ordering Expires: 30 Sep 05

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/adobe/adobe-ela.shtml

CAC Middleware

CAC Middleware - Provides Common Access Card middleware.

Contractors:

Datakey, Inc. (N00104-02-D-Q666) IDIQ Contract for DATAKEY products; (301) 261-9150

Schlumberger (N00104-02-D-Q668) IDIQ Contract for CACTUS products; (410) 723-2428

Spyrus, Inc. (N00104-02-D-Q669) IDIQ Contract for ROSETTA products; (408) 953-0700, ext. 155

SSP-Litronic, Inc. (N00104-02-D-Q667) IDIQ Contract for NETSIGN products; (703) 905-9700

Ordering Expires: 6 Aug 05

Web Link: http://www.it-umbrella.navy.mil/contract/middleware-esa/index-cac.shtml

Microsoft Products

Microsoft Products - Provides licenses and software assurance for desktop configurations, servers and other products. In addition, any Microsoft product available on the GSA Schedule can be added to the BPA.

Contractors:

ASAP (N00104-02-A-ZE78); Small Business; (800) 248-2727, ext. 5303

CDW-G (N00104-02-A-ZE85); (847) 968-9429

Hewlett-Packard (formerly Compaq) (N00104-02-A-ZE80); (800) 535-2563 pin 6246

Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 37010 or (512) 723-7010

GTSI (N00104-02-A-ZE79); Small Business; (800) 999-GTSI or (703) 502-2073

Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638 or (703) 469-3899

Softmart (N00104-02-A-ZE84); (610) 518-4000, ext. 6492 or (800) 628-9091 ext. 6928

Software House International (N00104-02-A-ZE86); Small Business Disadvantaged; (800) 477-6479 ext. 7130 or (703) 404-0484

Software Spectrum, Inc. (N00104-02-A-ZE82); (800) 862-8758 or (509) 742-2308 (OCONUS)

Ordering Expires: 30 Jun 05

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.shtml

Netscape Products

Netscape Products - Netscape Communicator Client and a number of the Netscape Server products for use across DoD are available for download at no cost. Customers must choose between the commercial version and the Defense Information Infrastructure Common Operating Environment (DII COE) Segmented Versions.

Licensed software products available from the Defense Information Systems Agency (DISA) are commercial versions of the software, not the segmented versions that are compliant with the DII COE standards. The segmented versions of the software are required for development and operation of applications associated with the DII COE, the Global Command and Control System (GCCS) or the Global Combat Support System (GCSS).

If your intent is to use a licensed product available for download from the DoD Download site to support development or operation of an application associated with the DII COE, GCCS or GCSS, you must go to one of the Web sites listed below to obtain the DII COE segmented version of the software. You may not use the commercial version available from the DoD Download site.

If you are not sure which version (commercial or segmented) to use, we strongly encourage you to refer to the Web sites listed below for additional information to help you to make this determination before you obtain the software from the DoD Download site.

DII COE or GCCS users: Common Operating Environment Home Page
http://disa.dtic.mil/coe

GCSS users: Global Combat Support System
http://www.disa.mil/main/prodsol/gcss.html

Contractor: ***Netscape***

Ordering Expires: Mar 05 – Download provided at no cost.

Web Link: http://dii-sw.ncr.disa.mil/Del/netlic.html

Operating Systems

Novell

Novell Products - Provides master license agreement for all Novell products, including NetWare, GroupWise and ZenWorks.

Contractor: ***ASAP Software*** (N00039-98-A-9002); Small business; (800) 883-7413

Ordering Expires: 31 Mar 07

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/novell/novell.shtml

Sun (SSTEW)

SUN Support - Sun Support Total Enterprise Warranty (SSTEW) offers extended warranty, maintenance, education and professional services for all Sun Microsystems products. The maintenance covered in this contract includes flexible and comprehensive hardware and software support ranging from basic to mission critical services. Maintenance covered includes Sun Spectrum Platinum, Gold, Silver, Bronze, hardware only and software only support programs.

Contractor: ***Dynamic Systems*** (DCA200-02-A-5011)

Ordering Expires: Dependent on GSA Schedule until 2011

Web Link: http://www.ditco.disa.mil/hq/contracts/sstewchar.asp

Section 508 Tools

HiSoftware 508 Tools

HiSoftware Section 508 Web Developer Correction Tools - Includes AccRepair (StandAlone Edition), AccRepair for Microsoft FrontPage, AccVerify for Microsoft FrontPage and AccVerify Server. Also includes consulting and training support services.

Contractor: ***HiSoftware, DLT Solutions, Inc.*** (N00104-01-A-Q570); Small Business; (888) 223-7083 or (703) 773-1194

Ordering Expires: 16 Aug 04 (Renewal pending)

Web Link: http://www.it-umbrella.navy.mil/contract/508/dlt/dlt.shtml

Warranty: IAW GSA Schedule. Additional warranty and maintenance options available. Acquisition, Contracting and Technical fee included in all BLINS.

ViViD Contracts

N68939-97-D-0040

Contractor: Avaya Incorporated

N68939-97-D-0041

Contractor: General Dynamics

ViViD provides digital switching systems, cable plant components, communications and telecommunications equipment and services required to engineer, maintain, operate and modernize base level and ships afloat information infrastructure. This includes pier side connectivity and afloat infrastructure with purchase, lease and lease-to-own options. Outsourcing is also available. Awarded to:

Avaya Incorporated (N68939-97-D-0040); (888) VIVID4U or (888) 848-4348. Avaya also provides local access and local usage services

General Dynamics (N68939-97-D-0041); (888) 483-8831

Modifications

Latest contract modifications are available at http://www.it-umbrella.navy.mil

Ordering Information

Ordering Expires:
26 Jul 05 for all CLINs/SCLINs
26 Jul 07 for Support Services and Spare Parts

Authorized users: DoD and U.S. Coast Guard

Warranty: Four years after government acceptance. Exceptions are original equipment manufacturer (OEM) warranties on catalog items.

Acquisition, Contracting & Technical Fee: Included in all CLINs/SCLINs

Web Link

http://www.it-umbrella.navy.mil/contract/vivid/vivid.shtml

TAC Solutions BPAs Listed Below

TAC Solutions provides PCs, notebooks, workstations, servers, networking equipment and all related equipment and services necessary to provide a completely integrated solution. BPAs have been awarded to the following:

Control Concepts (N68939-97-A-0001); (800) 922-9259

Dell (N68939-97-A-0011); (800) 727-1100, ext. 61973

GTSI (N68939-96-A-0006); (800) 999-4874, ext. 2104

Hewlett-Packard (formerly Compaq) (N68939-96-A-0005); (800) 727-5472, ext. 15515

Hewlett-Packard (N68939-97-A-0006); (800) 352-3276, ext. 8288

Sun (N68939-97-A-0005); (800) 786-0404

Ordering Expires:
Control Concepts: 03 May 07 (includes two one-year options)
Dell: 31 Mar 05 (includes two one-year options)
GTSI: 1 Apr 05 (includes two one-year options)
Hewlett-Packard (formerly Compaq): 8 Oct 05 (includes two one-year options)
Hewlett-Packard: 28 Oct 05 (includes two one-year options)
Sun: 22 Aug 04

Authorized Users: DON, U.S. Coast Guard, DoD and other federal agencies with prior approval.

Warranty: IAW GSA Schedule. Additional warranty options available.

Web Links

Control Concepts
http://www.it-umbrella.navy.mil/contract/tac-solutions/cc/cc.shtml

Dell
http://www.it-umbrella.navy.mil/contract/tac-solutions/dell/dell.shtml

GTSI
http://www.it-umbrella.navy.mil/contract/tac-solutions/gtsi/gtsi.shtml

Hewlett-Packard (formerly Compaq)
http://www.it-umbrella.navy.mil/contract/tac-solutions/compaq/compaq.shtml

Hewlett-Packard
http://www.it-umbrella.navy.mil/contract/tac-solutions/hp/hp.shtml

Sun
http://www.it-umbrella.navy.mil/contract/tac-solutions/sun/sun.shtml

Department of the Navy Enterprise Solutions BPA

Navy Contract: N68939-97-A-0008

The Department of the Navy Enterprise Solutions (DON ES) BPA provides a wide range of technical services, specially structured to meet tactical requirements, including worldwide logistical support, integration and engineering services (including rugged solutions), hardware, software and network communications solutions. DON ES has one BPA.

Computer Sciences Corp. (N68939-97-A-0008); (619) 225-2412; Awarded 7 May 97; Ordering expires 31 Mar 06, with two one year options

Authorized Users: All DoD, federal agencies and U.S. Coast Guard.

Web Link

http://www.it-umbrella.navy.mil/contract/don-es/csc.shtml

Information Technology Support Services BPAs

Listed Below

The Information Technology Support Services (ITSS) BPAs provide a wide range of IT support services such as networks, Web development, communications, training, systems engineering, integration, consultant services, programming, analysis and planning. ITSS has four BPAs. They have been awarded to:

Lockheed Martin (N68939-97-A-0017); (240) 725-5950; Awarded 1 Jul 97; Ordering expires 30 Jun 05, with two one-year options

Northrop Grumman Information Technology (N68939-97-A-0018); (703) 413-1084; Awarded 1 Jul 97; Ordering expires 11 Feb 05, with two one-year options

SAIC (N68939-97-A-0020); (703) 676-2388; Awarded 1 Jul 97; Ordering expires 30 Jun 05, with two one-year options

TDS (Small Business) (N00039-98-A-3008); (619) 224-1100; Awarded 15 Jul 98; Ordering expires 14 Jul 05, with two one-year options

Authorized Users: All DoD, federal agencies and U.S. Coast Guard

Web Links

Lockheed Martin
http://www.it-umbrella.navy.mil/contract/itss/lockheed/itss-lockheed.shtml

Northrop Grumman IT
http://www.it-umbrella.navy.mil/contract/itss/northrop/itss-northrop.shtml

SAIC
http://www.it-umbrella.navy.mil/contract/itss/saic/itss-saic.shtml

TDS
http://www.it-umbrella.navy.mil/contract/itss/tds/itss-tds.shtml

Research and Advisory BPAs

Listed Below

Research and Advisory Services BPAs provide unlimited access to telephone inquiry support, access to research via Web sites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. BPAs listed below.

Gartner Group (N00104-03-A-ZE77); (703) 226-4815; Awarded Nov 02; one-year base period with three one-year options.

Acquisition Solutions (N00104-00-A-Q150); (703) 378-3226; Awarded 14 Jan 00; one-year base period with three one-year options.

Ordering Expires:
Gartner Group: Nov 06
Acquisition Solutions: 30 Sep 04

Authorized Users:
Gartner Group: This Navy BPA is open for ordering by all DoD components and their employees, including Reserve Components (Guard and Reserve); the U.S. Coast Guard; other government employees assigned to and working with DoD; nonappropriated funds instrumentalities of the DoD; DoD contractors authorized in accordance with the FAR and authorized Foreign Military Sales (FMS).

Acquisition Solutions: All DoD. For purposes of this agreement, DoD is defined as: all DoD Components and their employees, including Reserve Component (Guard and Reserve) and the U.S. Coast Guard mobilized or attached to DoD; other government employees assigned to and working with DoD; nonappropriated funds instrumentalities such as NAFI employees; Intelligence Community (IC) covered organizations to include all DoD Intel System member organizations and employees, but not the CIA nor other IC employees unless they are assigned to and working with DoD organizations; DoD contractors authorized in accordance with the FAR; and authorized Foreign Military Sales.

Web Links

Gartner Group
http://www.it-umbrella.navy.mil/contract/r&a/gartner/gartner.shtml

Acquisition Solutions
http://www.it-umbrella.navy.mil/contract/r&a/acq-sol/acq-sol.shtml

The U.S. Army Maxi-Mini and Database (MMAD) Program

Listed Below

The MMAD Program is supported by two fully competed Indefinite Delivery Indefinite Quantity (IDIQ) contracts with IBM Global Services and GTSI Corp. The program is designed to fulfill high and medium level IT product and service requirements of DoD and other federal users by providing items to establish, modernize, upgrade, refresh and consolidate system environments. Products and manufacturers include:

	IBM Global Services	GTSI
Servers (64-bit & Itanium)	IBM, HP, Sun	Compaq, HP
Workstations	HP, Sun	Compaq, HP
Storage Systems	IBM, Sun, EMC, McData, System Upgrade, Network Appliances	HP, Compaq, EMC, RMSI, Dot Hill, Network Appliances
Networking	Cisco	Cisco, 3COM, HP, Enterasys, Foundry, Segovia

Ancillaries include network hardware items, upgrades, peripherals and software.

Services include consultants, managers, analysts, engineers, programmers, administrators and trainers.

MMAD is designed to ensure the latest products and services are available in a flexible manner to meet the various requirements identified by DoD and other agencies. This flexibility includes special solution CLINs, technology insertion provisions, ODC (Other Direct Cost) provisions for ordering related non-contract items, and no dollar/ratio limitation for ordering services and hardware.

Latest product additions include Fortress Technologies, HP Overview, Remedy Websphere and DB2 Tools.

Awarded to:

GTSI Corp. (DAAB07-00-D-H251); (800) 999-GTSI

IBM Global Services-Federal (DAAB07-00-D-H252); CONUS: (866) IBM-MMAD (1-866-426-6623) OCONUS: (703) 724-3660 (Collect)

Ordering Information

Ordering: Decentralized. Any federal contracting officer may issue delivery orders directly to the contractor.

Ordering Expires:
GTSI: 25 May 06 (includes three option periods)
IBM: 19 Feb 06 (includes three option periods)

Authorized Users: DoD and other federal agencies including FMS

Warranty: 5 years or OEM options

Delivery: 35 days from date of order (50 days during surge period, August and September)

No separate acquisition, contracting and technical fees.

Web Link

GTSI and IBM: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

New ERP
Systems Integration Services
BPAs!

Celebrating 16 years of Delivering Huge Savings to DON and DoD customers

The Umbrella Program provides easy-to-use, pre-competed acquisition vehicles that give you better life-cycle prices, higher quality, timely delivery, and guaranteed integration and interoperability with the standards-based technology you already have in place. We offer tens of thousands of IT products, as well as an entire range of IT services to help you meet your mission needs. We leverage DoD and DON buying power and commercial best practices with a focus on industry trends to bring you the easiest acquisition solution and best savings available — anywhere! Visit us online.

www.it-umbrella.navy.mil

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN CHARLESTON
CHIPS MAGAZINE
9456 FOURTH AVE
NORFOLK VA 23511-2130
OFFICIAL BUSINESS

PERIODICAL
POSTAGE AND FEES PAID
SSC CHARLESTON
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988