Sharing Information ▭ Technology ▭ Experience

January - March 2007

CHIPS Magazine

The Standing Joint Force Headquarters - Core Element

On the Job Around the World

CHIPS January - March 2007

Volume XXV Issue I

Department of the Navy
Chief Information Officer
Mr. Robert J. Carey
Mr. John J. Lussier (Acting)

Space & Naval Warfare Systems Command
Commander
Rear Admiral Michael C. Bachmann

Space & Naval Warfare Systems Center Charleston
Commanding Officer
Captain Red Hoover

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Web support: Tony Virata 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 and Naval Warfare Systems Center, San Diego, Calif.

CHIPS is published quarterly by the Space and Naval Warfare Systems Center Charleston. USPS 757-910 Periodical postage paid at Norfolk, VA and at an 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: http://www.chips.navy.mil/.

Disclaimer. The views and opinions contained in CHIPS are not necessarily those of the Department of Defense nor do they constitute endorsement or approval by the DON CIO, DON IT Umbrella Program or SPAWAR Systems Center Charleston. The facts as presented in each article are verified insofar as possible, but the opinions are strictly those of the individual authors.

Don't miss a single issue of CHIPS! To request extra copies or send address changes, contact CHIPS editors at chips@navy.mil or phone (757) 444-8704, DSN 564.

Contents

4 **Editor's Notebook**

5 **From the Acting DON CIO John J. Lussier**

6 **Letter from the desert** - From the recently selected DON CIO Rob Carey

8 **Interview with Dr. Michael F. McGrath**
Deputy Assistant Secretary of the Navy RDT&E

12 **Interview with Vice Adm. Mark J. Edwards**
Deputy Chief of Naval Operations for Communication Networks (N6)

16 **Interview with Rear Adm. Donald K. Bullard**
Commander, Navy Expeditionary Combat Command

20 **Standing Joint Force Headquarters-Core Element**

24 **Subnet Relay – Enhancing Multinational Connectivity**

27 **Priority to Deliver Network Interoperability Solutions Affirmed**

29 **Electromagnetic Spectrum: Critical to Our Nation's Security …**

30 **Don't Fall for the "Phisher's Bait"**

32 **Joint Integration and Interoperability of Special Operations**

33 **Department of the Navy INFO Alert**

34 **Innovation Delivered to the Warfighter by the OX**

35 **DON IT Umbrella Program Update**

36 **Interview with Joe Camacho -** USFCOM JKDDC Program Manager

38 **USJFCOM's New Supercomputer**

39 **Developing the Information Technology Professionals of Tomorrow …**

40 **Electromagnetic Railgun – a "Navy After Next" Game Changer**

42 **Navy "COOL" Web Site …**
Credentialing the DON IA/CND Workforce

43 **Enabling Warfighter Mission Assurance …**

44 **Coalition Interoperability Reaches New Heights in RIMPAC 2006**

45 **CHIPS 25th Anniversary**

47 **QuABO - An Interview with Cmdr. John Ingersoll**

50 **The Lazy Person's Guide to Silver Bullets**

52 **"Big T" Hosts PEO EIS Working Group**

53 **Under the Contract**

Norfolk, Va. (Aug. 24, 2006) - Navy Expeditionary Combat Command members perform High Value Asset (HVA) escort training between Inshore Boat Units (IBU) 41 and 42 assigned to Naval Coastal Warfare Squadron Four. This exercise provides the final test for Level II Combat Coxswains and Gunners' qualification to handle small boats with weapons capability in defense of multiple-size U.S. Navy vessels transiting narrow waterways. U.S. Navy photo by Mass Communication Specialist 2nd Class Justin K. Thomas.

Cover: Joint Task Force Lebanon with U.S. Joint Forces Command Standing Joint Force Headquarters-Core Element and the U.S. European Command Joint Enabling Team. Photos illustrate the various missions of the SJFHQ-Core Element. Cover story on page 20.

Features

6
Recently selected Department of the Navy Chief Information Officer Rob Carey talks about what it is like to serve in Iraq as a civil engineer assigned to a construction regiment (Seabees) in Iraq

8
Deputy Assistant Secretary of the Navy - Research, Development, Test & Evaluation Dr. Michael F. McGrath discusses transitioning new capabilities into programs of record and into the hands of warfighters

12
Deputy Chief of Naval Operations for Communication Networks (N6) Vice Adm. Mark J. Edwards discusses N6 mission areas and successes six months after the N6 standup

16
Commander Navy Expeditionary Combat Command Rear Adm. Donald K. Bullard talks about the NECC mission one year after its standup

Editor's Notebook

Of course, the most important thing on my mind is that 2007 marks the 25th anniversary of CHIPS. As you can imagine, we are pretty excited about attaining this milestone since not many publications reach this venerable age.

We couldn't have done it without the support of the many contributors to CHIPS who have made this possible: The Department of the Navy Chief Information Officer (DON CIO), the DON Information Technology Umbrella Program team, the Space and Naval Warfare Systems Command and systems centers, our authors, technical experts, and DON and Defense Department program managers and senior leadership, who are always gracious and willing to talk to the CHIPS staff.

I've saved the best for last — you — our loyal readers! Thank you for your continuing support of CHIPS. Please join us in our year of celebration by contributing your ideas and articles to CHIPS via e-mail to chips@navy.mil. Look for a special anniversary issue coming up this year!

In the last few months, I have had the privilege to interview Deputy Assistant Secretary RDT&E, Dr. Michael McGrath; U.S. Joint Forces Command Standing Joint Force Headquarters-Core Element (our cover story); Commander, Navy Expeditionary Combat Command, Rear Adm. Donald Bullard; and the new N6, Vice Adm. Mark Edwards.

The 11th annual Naval NETWAR FORCEnet Enterprise and Industry Conference was a highlight in November. The conference, held in San Diego, featured top-notch speakers and opportunities to engage with DON and DoD program managers and senior officials.

November 28, 2006, we attended the stirring Second Fleet change of command ceremony on Naval Base Norfolk. Vice Adm. Evan M. Chanik relieved Vice Adm. Mark P. Fitzgerald. Fitzgerald departed 2nd Fleet to become the Director, Navy Staff in the Office of the Chief of Naval Operations.

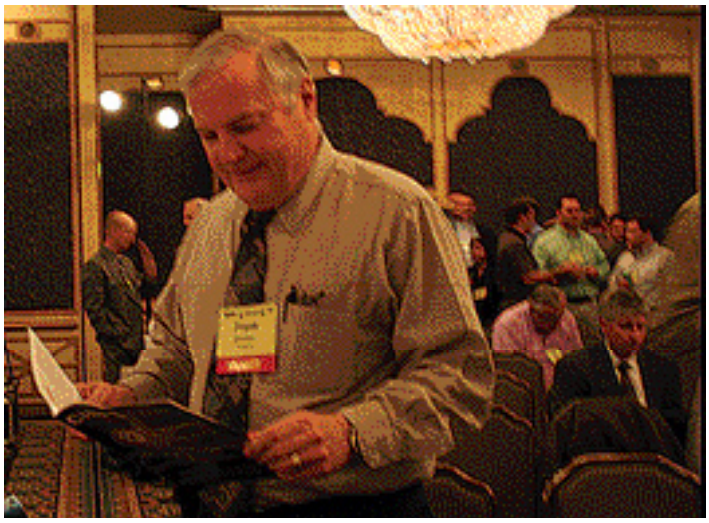
Perhaps the most moving experience I had was communicating by e-mail with the recently selected DON CIO, Rob Carey, who is currently serving as plans officer for a construction regiment in Iraq. It was just before the holidays and the poignant reminder of so many of our Sailors, Marines, Soldiers and Airmen serving America so far from home during this happy time evoked renewed feelings of humbleness and appreciation in the face of their bravery and self-sacrifice. I know they are always uppermost in your mind too.

Welcome new subscribers!

Sharon Anderson

On the road again in Washington, D.C., June 2007 with CHIPS webmaster Tony Virata. DON IT Umbrella Program teammates often assist the CHIPS staff at conferences and events.

The Second Fleet change of command ceremony onboard Naval Base Norfolk, Nov. 28, 2006. At the podium, guest speaker, Commander Fleet Forces Command Adm. John B. Nathman. Vice Adm. Mark P. Fitzgerald, left, was relieved by Vice Adm. Evan M. Chanik, second from right. Fitzgerald departed 2nd Fleet to become the Director, Navy Staff in the Office of the Chief of Naval Operations. Navy chaplain Capt. Olric R. Wilkins gave the benediction.



Dr. Frank E. Gordon, head of the Navigation & Applied Sciences Department, Space and Naval Warfare Systems Center, San Diego, reading CHIPS at the Naval NETWAR FORCEnet Enterprise and Industry Conference November 2006 in San Diego at the Bahia Hotel on Mission Bay.

DON CIO

Putting information to work for our people

Happy New Year!

The end of calendar year 2006 and the beginning of 2007 have been a period of transition but also one of continued accomplishment here at the DON CIO. As you are probably aware, after 26 years of service to the Department of the Navy, four as the DON CIO, Dave Wennergren has moved on to become the Department of Defense Deputy CIO as of Nov. 26, 2006.

Under Mr. Wennergren's tenure, the DON has made significant progress toward using information technology (IT) to transform our business and warfighting support processes. A few of the Department's many transformation successes include the full deployment of the Common Access Card with Public Key Infrastructure digital certificates on all NMCI computers, enabling secure cryptographic logon and Web site access; the elimination of outdated and duplicative software and the establishment of a single authoritative database for IT systems, applications and databases; and the development of a comprehensive strategy for transitioning the Department to an enterprise telecommunications management structure.

Secretary Winter has selected Rob Carey, the former deputy CIO for policy and integration, for the position of DON CIO. Mr. Carey is looking forward to taking the helm when he returns from his deployment with a Navy reserve unit in Iraq (see related articles on pages 6 and 33).

In the meantime, our successes continued in December with the signing of Secretary of the Navy Instruction 2075.1, Department of the Navy Use of Commercial Wireless Local Area Network (WLAN) Devices, Services, and Technologies; and the release of the DON EA-2006, a compendium of ongoing enterprise architecture efforts across the Department, which has been posted on the DON CIO Web site at http://www.doncio.navy.mil. We have also released a request for quotations (RFQ) for a Department-wide telecommunications recovery audit, which is expected, based on the results of a pilot project, to recover many millions of dollars for the Department.

In the coming months, we will be implementing Lean Six Sigma initiatives to optimize the certification and accreditation of IT systems, expedite the introduction of spectrally dependent innovative technology into theater in Iraq, and minimize and mitigate privacy spillages. Additionally, a core team was formed to aggressively pursue the Next Generation Enterprise Network, the follow-on to the Navy Marine Corps Intranet.

As we look back over the accomplishments of the last few months and plans for the upcoming months, it is evident that our efforts to provide the leadership necessary to align information technology and information management in support of the warfighter are moving full steam ahead. We look forward to continued successes as we move into the new year.

John J. Lussier
Department of the Navy Chief Information Officer (Acting)

Letter from the desert

By Cmdr. Rob Carey

I received an e-mail in late October from the *CHIPS* editor, Sharon Anderson, who asked me if I would write about my experiences here and what I am doing.

So what is the recently selected Department of the Navy Chief Information Officer doing as an engineer assigned to a construction regiment (Seabees) in Iraq? Well, many things! Then I realized, heck, there's really not much that I can say about what I do because nearly everything (and for good reasons) I read or hear is classified because of OPSEC (operational security) rules!

What I thought I could do is talk about what it is like to serve in Iraq to help you understand a little about serving the nation and Navy in Iraq. I am the plans officer for a construction regiment. We provide engineering support to I Marine Expeditionary Force (IMEF) (Fwd)/Multi-National Force West. I work very closely with superb officers on the IMEF (Fwd) staff to work engineering aspects of large strategic projects, as well as to assist the interests of the Seabees so that as operations are executed, engineering facets are supportive of the goals of each mission.

I have been in theater about two months, and have settled into a routine that is very different from one inside the Beltway. In short, life in a coalition operating base is filled with visions of the movie "Groundhog Day," interrupted by unnatural sounds and occasionally earth-shaking thunder. It's quite a dramatic shift from life in Virginia, but overall, my teammates and I are doing well.

We arrived to temperatures around 120 F, and as of this writing, daytime highs remain in the upper 80s. Dust storms are a thing to behold, and they generally precede the rainstorms which have recently just started. After the rain, mud is everywhere, and I mean everywhere! I am not sure which environment I prefer: heat or mud. The heat is so intense that the breeze is hot on your exposed skin, and the mud can make your boots weigh 5 pounds more — or so it seems.

The sunsets here are cool to watch if you happen to be out there and looking west at that time. Probably, the "moon dust" helps with the atmospherics.

The sounds and smells of this place permeate one's senses. Whether it be the startling thunder of our artillery being delivered (as has happened to me more than once at night walking home), or the foul smell of the garbage pits burning — glowing on the horizon at night rather eerily. My walk home at night could serve as a backdrop to film many a horror movie!

We have it much easier than the ground troops at smaller forward operating bases and combat outposts. They are out every day in a bizarre, yet deadly cat and mouse game with the insurgents.

The Seabees here help to build most of those facilities — often in the middle of very dangerous places. There are many "Fort Apaches" here in Iraq. Watching these young Marines, Soldiers and Sailors go out the gate on convoys, armed to the teeth (some have yet to shave) is truly amazing — a sight to behold.

There are many 18 and 19-year-olds who hold the decision of life in their hands every day — and they perform magnificently.

Navy Commander and recently selected DON CIO Rob Carey in Iraq.

Some seem numb to conditions here. Convoys often operate at night, so they present hard targets; we call them "vampires."

You will all be glad to know that the power of information technology here at the tip of the spear is enormous. The use of the Web is standard. VOIP [voice-over-IP] is used as a mainstream phone system. Most everyone has a personal computer on their desk.

And while things here perform very well, we must not take for granted that we are working to support the team at the tip of the spear. My being here shows me firsthand that there is much work to be done to realize the vision of the GIG [Global Information Grid] connecting the battlefield to the wealth of information that exists in the United States. The vision of seamless "reachback" must accommodate the reality of the operating forces' architecture and equipment.

I work in a Southwest Asia (SWA) hut, a 16 by 32-foot wooden structure, which is basically a big shed with a plywood floor and walls. We have air conditioning — if we didn't — the computers would not operate. I am convinced the A/C is for them — not for us. Of course, we expanded the SWA hut (because we could) and built a 16 by 16-foot addition. There are 11 Seabees who work here in the building. I have a master chief and a chief who help keep me out of trouble. A tall order I know, but they are both bigger than I am and that helps.

The Marines have been super to work with here. From the generals to the lance corporals, they are professional and friendly.

"I have traveled a bit and by far the worst place that I've seen is Ar Ramadi — hands down. The guys who live and serve there are very special. Everyday, life outside the wire is pure combat with no holds barred."

– Cmdr. Rob Carey

They definitely like and respect Seabees, probably because we have men who patrol the roads at night ready for trouble like they do. Not to mention, we build most of their combat outposts and forward operating bases.

The Seabees are focused and driven to deliver whatever is needed by the Marines, Sailors and Soldiers in the area of operations to get the mission accomplished.

I have traveled a bit and by far the worst place that I've seen is Ar Ramadi — hands down. The guys who live and serve there are very special. Every day, life outside the wire is pure combat with no holds barred.

Inside the wire, it is dirty, dry and grimy. The insurgents attack our convoys with IEDs (improvised explosive devices) in the road, snipers, mortars and small arms. We counter them with tanks, attack helicopters, fixed-wing close air support, artillery, crew-served weapons — and our snipers —who are ***FAR*** better than theirs.

The Al Anbar province is the most violent place I have ever visited in my life. Quite a change of pace from inside the Beltway and soccer games in the suburbs of Washington, D.C. Outside the walls, we are all targets.

The surgical team sent an e-mail requesting blood donors, and there seemed to be many. Just like on the television show "MASH" — wounded were in. I had to get ready for my helo flight or would have donated on the spot. Surgical is on my way home each night. When we see helos on its landing pads we know that the surgical team is working to save lives …

There have been some humorous moments here, like the time one of my fellow officers was stopped at the galley for trying to take a cookie with him as he left — unbelievable. It's amazing what can make you laugh here.

Speaking of the galley, it's like being in grammar school: you come in with four or five folks and want to sit with each other. After getting your tray and food, you look up — and there is a sea of tan uniforms — your friends are lost in the ocean of uniformity. Watching the young kids eat! Yikes! They deserve the best!

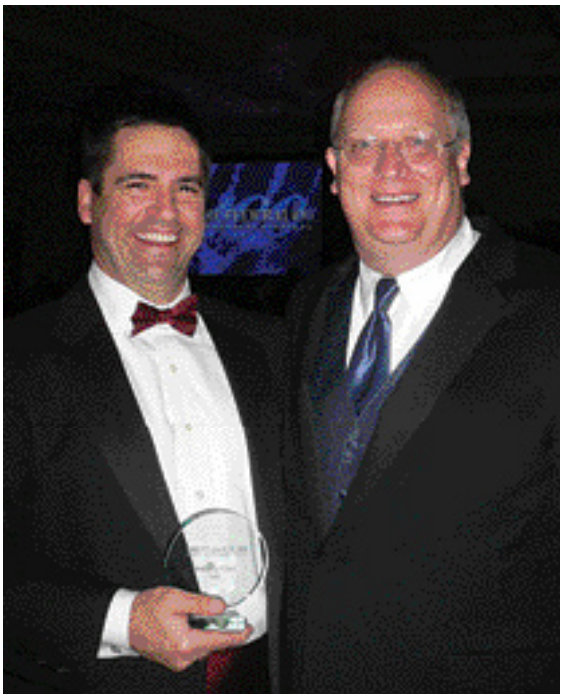
Getting caught unaware by our outbound artillery when you're walking in the dark, minding your own business, a bit tired, thinking of home, is quite an experience — BOOM — at 100 meters away! It's sort of like someone shooting a shotgun off next to your head when you aren't paying attention. It's a bit disturbing, but it's nice that it is outbound and not landing in camp! The howitzers are pretty close to where I work. Generally, the shooting makes the dust re-settle in the SWA hut I work in! Still, the artillery gunfire is welcome when it is directed toward the enemy.

Being here and serving the nation in this "away game" definitely makes me appreciate all that we have in the United States of America. This tour makes me pause and think a great deal, and to reflect on what we take for granted: liberty, freedom and equality.

While we all complain about traffic, the heat, the humidity, the price of gas, why Congress isn't doing what we think is right, the snow, a wet newspaper, a grocery store not having the steaks we wanted, just remember that having that right to complain is pretty damn cool.

So while I have worked for the Army and Navy for 24 years, and have been in uniform as a Reserve officer for more than 17, I am once again amazed at the strength of this nation, and the talented men and women of the armed forces. I am nothing but proud to serve.

So are we making a difference? I think so. We all are.



Robert Carey and then DON CIO Dave Wennergren at the Federal 100 Awards 2006 black-tie gala March 20, 2006. Carey was recognized with a Federal 100 award for leading information assurance strategy and policy development and implementation efforts that significantly improved the security of DON systems and networks.

"So while I have worked for the Army and Navy for 24 years, and have been in uniform as a Reserve officer for more than 17, I am once again amazed at the strength of this nation, and the talented men and women of the armed forces. I am nothing but proud to serve."

– Cmdr. Rob Carey

Mr. Robert J. Carey was designated as the Department of the Navy Chief Information Officer (DON CIO) effective Nov. 26, 2006. Reporting directly to the Secretary of the Navy, he is the principal adviser to the Secretary in all matters related to the mandates of the Clinger-Cohen Act; Chapter 35 of Title 44, United States Code; Section 2223 of Title 10. In his position as DON CIO, Mr. Carey is also designated as the DON Critical Infrastructure Assurance Officer.

Until his return from his deployment in Iraq, Mr. John J. Lussier is designated as the acting DON CIO.

Mr. Carey is also a Commander, Civil Engineer Corps in a U.S. Navy Reserve unit. He serves as plans officer for a construction regiment in Iraq. He is expected to return to his civilian life early 2007. CHIPS

Interview with Dr. Michael F. McGrath

Deputy Assistant Secretary of the Navy

Research, Development, Test and Evaluation

Dr. Michael McGrath is the deputy assistant Secretary of the Navy for research, development, test and evaluation. His role is to aggressively drive new technologies from all sources across Navy and Marine Corps platforms and systems, and to develop programs to bridge the gap in transitioning new capabilities from science and technology (S&T) to acquisition. CHIPS spoke with Dr. McGrath in August 2006.

Dr. Michael F. McGrath

CHIPS: Can you talk about your role as the commercial technology transition officer for the Department of the Navy?

Dr. McGrath: My official title is the DASN for RDT&E. A major function that I have is to be an advocate for technology transition. That means having one foot in the world of science and technology and the other foot in acquisition in order to move new technologies across the valley of death to a program of record. That transition is a difficult thing to achieve.

On one side is a technology source ready to launch new ideas into full scale development and production. On the other side is the acquisition community, which is risk-averse and will, only as a last resort, pull something that is immature into their system.

It is a process in which many players must agree on the criteria for handing something from S&T into an acquisition program. We have a number of ways designed to get at various aspects of that problem.

CHIPS: Do you transition programs through the Advanced Concept Technology Demonstration program?

Dr. McGrath: ACTD is one of the programs that I would consider to be in the portfolio of tools for tech transition. ACTDs are run by OSD (Office of the Secretary of Defense) and all of the services play in them. Each ACTD is managed by a lead service or agency developer and driven by the principal user sponsor. As a general rule, the user sponsor is usually a unified commander.

The ACTD is designed to deliver a prototype into the field with a transition agreement so that in a three- to five-year period, a capability is developed and fielded in response to a user need. In some cases you are co-developing the concept of operations and the need along with the technology.

Many of the ACTDs are based on advanced technologies which demand a new concept of operations, tactics and doctrine in order to realize their maximum potential.

The ACTD provides a means to develop, refine and optimize these warfighting concepts to achieve maximum utility and effectiveness.

With the ACTD team is a transition manager whose job is to transition the prototype into a program of record.

A key goal of the program is to move an ACTD into the appropriate phase of formal acquisition without loss of momentum, assuming the user makes a positive determination of military utility.

Each ACTD has a clear acquisition goal for the post-ACTD phases. Additionally, there must be provisions for the development of formal operational requirements; documents addressing interoperability, life cycle cost, manning, and training; and preparations for supportability.

CHIPS: Do you work with industry, the universities and the naval research centers to transition ACTDs?

Dr. McGrath: Yes, I transition technology from all sources. ACTDs and other programs become part of the portfolio of transition tools depending upon the source of technology. ACTDs often start with ideas that come from industry or the naval warfare centers or other government activities. The priorities are set largely by the combatant commanders.

At the back end of that process, there is a program of record, and if it is a Navy program of record, we want to have a resource sponsor and acquisition manager in on the decision to launch the ACTD. (See Figure 1, Deal Components.)

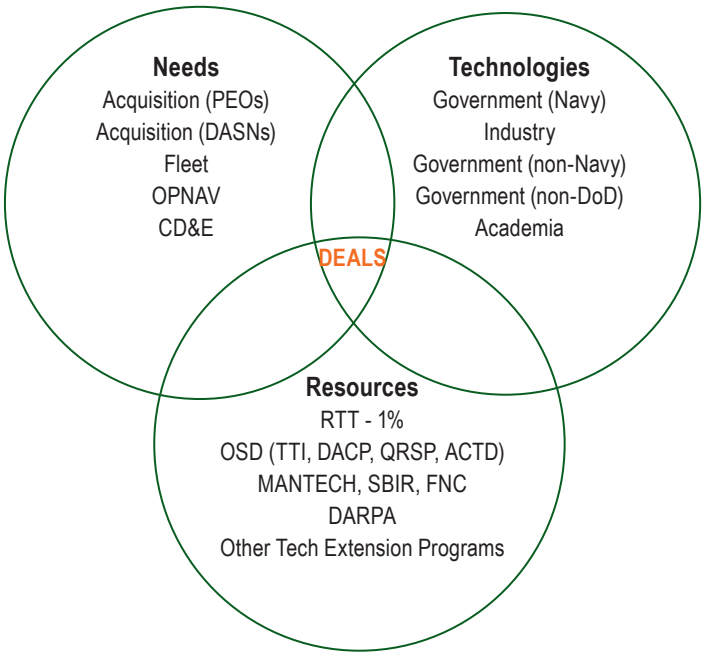
An ACTD will not be approved unless there is a commitment by a lead service or agency to accept the responsibility for preparing for transition at the end of the ACTD, and the risks are understood and accepted.

Even with the use of sufficiently mature technology, there can be technical risks associated with engineering and integration work to be performed. The more complex the capability, the greater these risks tend to be.

There can also be programmatic risks (e.g., cost and schedule), as well as operational risks related to the acceptability of the operational concepts necessary to realize the full benefit of the proposed capability.

These risks must be identified and accepted by the primary stakeholders in the ACTD prior to its initiation.

Figure 1. Deal Components.



"I would have to say the most exciting technologies for me are the ones that are saving lives on the battlefield and helping our warfighters accomplish their missions in harsh real-world conditions."

Dr. Michael McGrath
DASN RDT&E

CHIPS: What about advanced technologies that come from industry or the universities? How are they transitioned?

Dr. McGrath: If you are talking about other sources of technology that are commercial or university-based, then other tools come into play.

One tool is a Navy program called Rapid Technology Transition, or RTT. The RTT program provides current-year funding for emerging capabilities. The RTT program office tries to broker a deal that matches an interesting technology with a user who has a need.

A resource sponsor must agree that this will be funded as a program of record, and then usually the problem is the budget.

If Navy did not budget for the technology this year, the best we can do is to try to find funding next year or put it in the POM (Program Objective Memorandum) for funding in two years. In the intervening time the deal often unravels.

The RTT program can step in with bridge funding to keep the deal alive until the program of record money can kick in. That bridge funding is used to do testing and evaluation to flight-certify an item so it can go into an aircraft or ship.

A little bit of money can keep a deal alive until more substantial funding becomes available.

The largest Navy transition-oriented program is at the Office of Naval Research, and it is called the Future Naval Capabilities or FNCs. The FNCs have about one-third of the Navy's S&T money. This is the part of ONR's portfolio that is directly related to requirements — capability gaps defined by OPNAV (Office of the Chief of Naval Operations).

The FNCs have tech transition agreements with acquisition programs of record built-in early in the life of an FNC.

CHIPS: Do the FNCs use mature technology?

Dr. McGrath: Yes. We measure technology maturity with technology readiness levels (TRL). Typically, an FNC would start with TRL 5 and an FNC would transition at TRL 6 or maybe TRL 7. (See Figure 2, Technology Readiness Levels below.)

CHIPS: Is there an average time span between when technology would move up between levels?

Dr. McGrath: FNCs are designed to take three to five years to deliver, similar to ACTDs. Information technology tends to mature more rapidly than, for example, a new structural material. You can do spiral development of information systems and allow the user to experiment with the system.

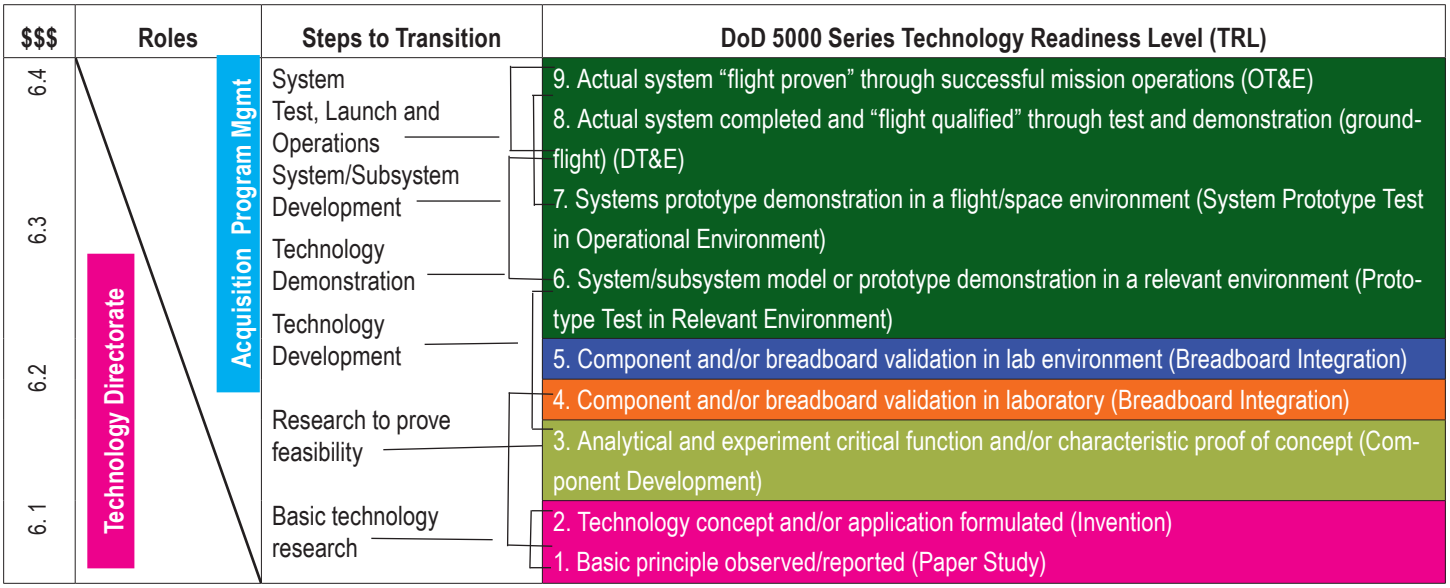
The TRL levels have to do with the scale at which you have done demonstrations and the environment in which you are doing those tests and demonstrations.

Often in information systems we can get a representative environment in a spiral development fashion and expand to a reasonable scale of operations so that the user has confidence that this is at a maturity level that will not add undue risk to the acquisition program.

We manage FNCs with IPTs, an integrated process team structure, which brings together the requirements community (that is the fleet), the resource sponsor from OPNAV, the acquisition community, and the science and technology community. The current portfolio of FNC projects is managed by five IPTs, each led by a member of the Senior Executive Service or flag officer.

That means that we are developing new FNCs and overseeing the execution of the ongoing FNCs with teams that have all the

Figure 2. Technology Readiness Levels (TRL).



Deal Name	PEO	Operational Impact
Virginia-Class Multi-Level Security (MLS)	PEO(Subs)/PMS-401/PMS-450	Integrates commercial security software and provides onboard MLS for data routing, network transmissions, and information storage avoiding burdensome procedural security measures and costly redesign efforts for the onboard network on the Virginia-class attack submarines and USS Los Angeles SSN 688 backfit; an estimated $76.8 million in integration and redesign cost can be avoided.
Commercial Emulator for E-2C Hawkeye Mission Computer	PEO(T)/PMA-231	Solves obsolescence problems in the E-2C Hawkeye by introducing a form, fit and function emulation technology combined with commercial-off-the-shelf (COTS) technology. Provides for the expansion of capabilities in response to new fleet requirements.
USMC Universal Communications Interface Module (UCIM)	MARCORSYSCOM	Allows integration of legacy radios and future Joint Tactical Radio System (JTRS) sets with C2 systems and antenna arrangements in a common environment across multiple platforms. The UCIM will decrease C2 platform costs, improve C2 platform capabilities, and provide tractable transition path from legacy radios to JTRS.
C2 On-The-Move Network Digital Over-the-Horizon Relay (CONDOR)	MARCORSYSCOM	Provides for a 12-month acceleration of the Ku-band capability for the Command and Control CONDOR program. The solution consists of a COTS-based Ku satellite communications system integrated into the CONDOR gateway and Jump Command and Control Vehicle (JC2-V). The current solution is the International Maritime Satellite (Inmarsat) system which costs $11 per minute and provides for 65 kbps. The Ku systems are expected to cost $1 per minute and provide 256 kbps.

Figure 3. Transitioned FORCEnet Capabilities.

players necessary for success of the project and for successful transition at the end.

We have brought together the stakeholders from the outset of the S&T project to make sure we have built a bridge across the valley of death instead of having a scientist or engineer invent something and try to throw it over the wall to somebody who is going to receive it in the acquisition community.

I want to make sure we give plenty of credit to OPNAV, the fleet and the acquisition community, in addition to ONR, for all being stakeholders in that FNC process.

CHIPS: When you refer to the acquisition community, are you talking about the program executive offices?

Dr. McGrath: Yes, we have PEOs on each of the five FNC IPTs. Four of the IPTs are aligned with the Sea Power 21 pillars, which are Sea Strike, Sea Shield, FORCEnet and Sea Basing.

There is a fifth IPT called Enterprise and Platform Enablers. This is where you would find corrosion control technologies that would have life cycle savings that would not fit into the warfighting pillars.

Those IPTs have PEOs on them who represent the acquisition community. They have senior representation from the fleet or from the Marine Corps, and they have resource sponsor representation from both OPNAV and Marine Corps. They also have S&T representation from ONR.

There is an oversight group called the Technology Oversight Group (TOG), co-chaired at the three-star level by OPNAV N8 (resources, requirements and assessments) and the Marine Corps Combat Development Command.

The TOG brings all stakeholders together. They approve FNC new starts, they review transition progress, and they intervene and fix things if transitions start to get off track.

This group is working problems that are important to the whole naval enterprise.

CHIPS: Have any FORCEnet-type technologies transitioned to the acquisition community?

Dr. McGrath: A lot of the systems that I am transitioning are FORCEnet-related systems. Earlier you mentioned the commercial technology transition office. That has been renamed. It is now called the Rapid Technology Transition office, or RTT office, that I talked about earlier. It is located at ONR.

The RTT office has done a number of transitions into systems that provide situational awareness or enhanced networking capabilities. One example is a multilevel secure coalition architecture transitioned to PEO C4I (command, control, communications, computers and intelligence).

The solution transitioned by RTT provides accredited multilevel secure (MLS) servers, chat services and information sharing in a single enclave, rather than a highly segmented solution for each coalition partner.

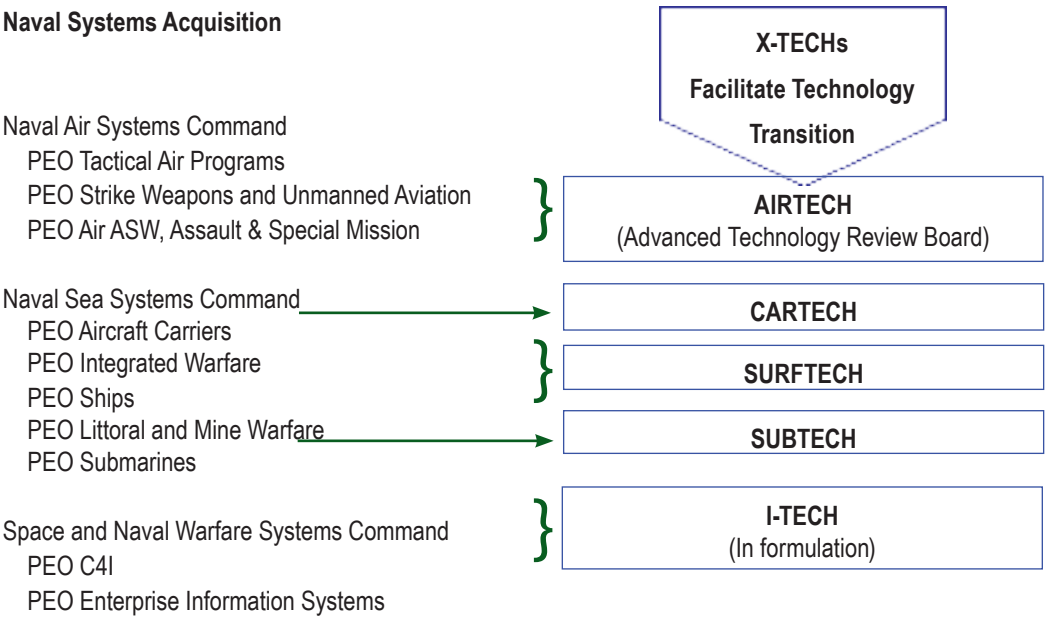
This advance in sharing critical information with allies and coalition partners supports collaboration that is critical to joint and coalition operations. There are other RTT examples that have transitioned FORCEnet enablers to aviation platforms, submarines and Marine Corps systems. (See Figure 3, Transitioned FORCEnet Capabilities.)

CHIPS: Do you look globally for new technologies?

Dr. McGrath: Each of these programs in the transition portfolio, ACTDs, FNCs and RTTs has its own mechanisms for inviting new project proposals.

CHIPS: So your office does not investigate new technologies?

Dr. McGrath: The RTT office does try to stay aware of new technologies. Sometimes it encourages programs to respond. They get help from groups in the systems commands that we refer to



Each of these programs in the transition portfolio — Advanced Concept Technology Demonstration, Future Naval Capabilities and Rapid Technology Transfer — has its own mechanisms for inviting new project proposals.

Each of the X-TECHs constantly reviews science and technology innovations and looks for insertion opportunities into Navy programs of record and acquisition programs.

The acquisition and S&T communities work closely together to identify technology approaches and solutions.

Figure 4.The X-TECHs work closely with the S&T community and the DASN RDT&E looking for innovative solutions to rapidly respond to warfighter needs.

as the 'X-TECHs.' Each domain has an organization that works to identify the technologies desired and to either find a commercial solution or have a solution developed.

There is a group at Naval Air Systems Command for aircraft called AIRTECH. For ships there is SURFTECH. At Naval Sea Systems Command, there is SUBTECH for submarine technology.

There is a group being formed at the Space and Naval Warfare Systems Command (with a lot of input from OPNAV N6) called I-TECH which works on FORCEnet.

There are also carrier technologies called CARTECH. (See Figure 4, X-TECHs.)

Each of these X-TECH groups is constantly reviewing technology and looking for insertion opportunities. They are involved in responding to these programs — the ACTDs, FNCs and the RTTs.

CHIPS: The groups that you just mentioned would stay abreast of emerging technologies to prevent technological surprises being used against the Navy and, ultimately, the United States?

Dr. McGrath: There are different levels for that. The groups I mentioned, the X-TECHs, are looking for mature technologies that are candidates for transition. The ONR, the Navy, and the broader S&T community try to stay plugged into scientific developments around the world.

ONR has an office called ONR Global with several international locations and a staff that tries to stay plugged into emerging scientific developments. They attend conferences and visit universities and industry on an international basis to stay aware of new developments and prevent technological surprise.

A lot of the work that goes on in government laboratories and our university-affiliated research centers involves taking scientific discoveries and turning them into technologies and applications that have military importance. They are making sure that we are not surprised by somebody developing a military application from a scientific breakthrough.

CHIPS: Are you excited about any new technologies that you think might have military application?

Dr. McGrath: One of the great things about this job is the opportunity to look across the broad horizon of technology and see something new every month. At the basic research level, you hear a lot about new fields like nanotechnology, where there are breakthroughs seemingly on a monthly basis. It is the job of our S&T community to see the possibilities for naval relevance of those things.

Nanotechnology can lead to advanced coatings that will give us better corrosion resistance in the maritime environment, better wear characteristics, or lightweight armor and power systems for dismounted Marines.

At the system level, advances in power control, power electronics, power systems and power storage make it possible for us to build systems like the electromagnetic launch system for CVN 21, the future aircraft carrier replacement program, or the electromagnetic railgun that is in development at ONR.

I would have to say the most exciting technologies for me are the ones that are saving lives on the battlefield and helping our warfighters accomplish their missions in harsh real-world conditions.

Often these warfighter solutions trace their roots to S&T programs started 20 years earlier. Your readers can find lots of examples of new technologies at the ONR Web site at http://www.onr.navy.mil, that are making a difference for today's Navy, tomorrow's Navy — and the Navy after next.

For more information about the work of the deputy assistant Secretary of the Navy for research, development, test and evaluaton and to view Dr. McGrath's biography, go to http://acquisition.navy.mil/organizations/dasns/dasn_rdt_e.

For information about the electromagnetic railgun, the next generation of naval gun, go to page 40. CHIPS

Interview with Vice Admiral Mark J. Edwards Deputy Chief of Naval Operations for Communication Networks (N6)

Vice Adm. Mark J. Edwards

In January 2006, the Chief of Naval Operations (CNO) announced the standup of a separate N6 Directorate for Navy as part of the greater realignment effort of his Navy staff in Washington.

The fast pace of change in technology and the ever-increasing importance of networks to modern warfare prompted the CNO to ensure the Navy has clarity, stability and discipline in managing warfare technology assets. N6 is responsible for centralized coordination of net-centric policy, planning, governance, requirements integration and investment direction to provide a competitive information advantage to combat-ready Navy forces.

N6 serves as the principal adviser to the CNO for all communication networks and is matrixed with N2 for ISR and N3/5 for IO and C2, and also performs as Navy's Chief Information Officer (CIO) ensuring optimum use of Navy information technology/information management (IT/IM) resources.

N6 includes N6F – Warfare Integration, N60/62 – Programming and Fiscal Management and N61 – Capability Analysis and Assessment.

CHIPS talked to Vice Adm. Edwards in December about six months since N6's standup.

CHIPS: Is it correct to say that some of the N6 mission areas were once held by other Navy commands or Navy staff? If so, what led to the consolidation of these particular functional areas?

Vice Adm. Edwards: The short answer to your question is, yes. Significant command, control, communications and computers (C4) changes within the Department of Defense are impacting all of the military departments. The DoD C4 paradigm shift from platform-based systems to network-centric warfare or NCW has prompted all the service chiefs to rethink their C4 investment strategies.

Under the concept of NCW, all services contribute information to the Global Information Grid, or GIG, for exploitation by all services and the combatant commanders. Services must now look at C4 functions across service lines. Networking the naval warrior through communication networks has become a linchpin in effective leadership for the 21st century.

Adm. Mullen's realignment of the OPNAV staff to stand up the N6 directorate is an inclusive step for the Navy to operate in the net-centric battlespace, and this means looking at C4 functions across the OPNAV staff and fleet commands. Getting the greatest return on the Navy's C4 investments requires a unified information technology (IT) strategy that is carried out by Navy leaders from the Pentagon down to the deck plates.

As we seek to better understand and capture where our business IT resources are, and how they are being used, one of the areas that I'm very interested in is having better visibility into how our IT money is being spent across the Navy. It's my sense that many of our legacy IT systems are in a sustainment mode and, in some cases, duplicative across the enterprise. Opportunities to redirect our investment dollars to other warfighting systems may exist as we collapse and sunset those legacy systems.

CHIPS: You have an enormous responsibility in planning the Navy investment and integration of warfare technology resources. How have you approached the coordination of all these functions?

Vice Adm. Edwards: As we work Program Review (PR)-09, the staff has done a lot of discovery into where we should focus our investments. We have a new generation ("Millennium" or "Gen Y") of Sailor entering the Navy that grew up with the Internet, who is collaborative and technologically savvy. One of our challenges is the lack of robust connectivity to our smaller warships. It is hard for our new Sailors not to be discouraged when they find out that our cruisers, destroyers and frigates have less bandwidth than they typically have at home or on their cell phone.

It is my intent to find IT investments that not only meet our warfighting requirements, but also provide our Sailors with the access they need to advance their careers and conduct their personal lives. In fact, our Sea Warrior program will require reach-back connectivity for our Sailors in order to get promoted and compete for their next job assignments. We also need to encourage more collaboration.

There is no reason the Navy should not embrace more chat or instant messaging capabilities across the fleet. Bandwidth and reliable network connectivity are key tenants of my PR-09 and Program Objective Memorandum (POM)-10 strategies.

We are also working toward aligning our IT functional areas with the correct resource sponsors. Currently, the Navy's IT portfolio is managed by 16 functional area managers. Our goal is to ensure the IT systems and applications within those functional areas are managed by the same OPNAV resource sponsor thus aligning our systems and applications with our warfighting requirements.

CHIPS: Do you have an eye on long and short-term investment? For example, the need for the Navy Expeditionary Combat Command was not forecasted even five years ago. How do you balance requirements in terms of fiscal responsibility and the larger question of national defense?

Vice Adm. Edwards: There is probably no need to remind your readers that we are a nation at war, and that the Navy has always

responded to the need to stay ahead of our adversaries. Our future C4 capabilities are being rewritten to meet the demands of conducting net-centric warfare with a joint and coalition maritime force in numerous mission areas, including major combat operations, global war on terror, homeland defense and stability operations. Today's enemies are dynamic, unpredictable, diverse and networked.

"I have directed my staff to use greater scrutiny in approving expenditures based on the capability return for the operating force. In-service legacy IT systems can be a tremendous drain on our limited resources, and they prevent us from being more agile in the IT arena. "
– Vice Adm. Mark Edwards
OPNAV N6

That being said, the Navy has to remain flexible to the changes in the battlespace. I have engaged my staff to improve the return on Navy C4 investments. Part of my initial efforts is to focus on finding the resources to fund C4 capabilities that the *fleet* is telling me *they* need — namely more bandwidth — and the ability to rapidly develop and field new capabilities.

I have directed my staff to use greater scrutiny in approving expenditures based on the capability return for the operating force. In-service legacy IT systems can be a tremendous drain on our limited resources, and they prevent us from being more agile in the IT arena. The fleet must be provided with the most effective C4/IT capability to safely execute its missions.

CHIPS: Can you discuss some of the successes that N6 has had since standup?

Vice Adm. Edwards: The most important success we've had since standing up is getting everyone pulling in the same direction. We developed a 100 Day Plan that I promulgated on my first day as N6. It directed specific actions in the following areas:

- Governance
- Legacy network reduction
- Capturing the money the Navy is investing in IT
- Maritime Headquarters/Maritime Operations Center (MHQ/MOC) comms and C2
- Maritime Domain Awareness (MDA)
- Sea Warrior IT
- Rapid capability development
- Open architecture
- Next generation enterprise networks
- Increasing effective bandwidth to tactical users
- Low cost operationally responsive space
- Tactical network realignment
- Field programs under cost and on schedule
- Strengthen Navy C4/IT community management and support

We have also put together a strategy for PR-09 that is focusing our efforts in three areas: warfighting, manpower and business. With warfighting, our demand for Web service capabilities to support warfighting continues to explode. The MHQ/MOC mirrors commercial trends in connectivity and information management capabilities. Our acquisition process is not agile, and we need to instill a rapid capabilities development process across the Navy enterprise.

My staff also recently completed a MDA connectivity workshop which brought together allied and fleet N6 officers to identify technical and procedural requirements for greater allied interoperability. Adm. Mullen has identified our allies and coalition partners as important components of his naval strategy.

My experience working with foreign navies has been that it takes practice, patience and persistence to become an efficient multinational maritime force. C4 technology is meant to facilitate operational evolution. This MDA connectivity workshop has been a great success in bringing naval players together to identify critical future C4 and interoperability capabilities.

On a more technical side, my staff is upgrading the high frequency (HF) radio capability across the fleet in order to enable better interoperability with other nations, many of whom use HF for long-range communications. Advances in HF radio technology now allow low rates of data to be exchanged which helps coordination among coalition partners.

Internet Protocol over HF radio is gaining increasing interest with our allies following technology demonstrations during the recent Trident Warrior exercise series.

"Our junior Sailors are dissatisfied with current Internet connectivity and our ability to provide distance learning through programs like Navy Knowledge Online, Sea Warrior and Distance Support while at sea. We are working with N1, the systems commands and the fleet to rapidly field these capabilities."
– Vice Adm. Mark Edwards
OPNAV N6

The Navy Combat Identification Capabilities Organization (CIDCO) was established by OPNAV N6 to function as the Navy's Office of Primary Responsibility for combat identification (CID). CID is a process used for force posturing, command and control, situational awareness as well as shoot, no-shoot employment decisions.

CID provides, through net-centric CID platforms, the capability for joint and coalition interoperability through accurate characterization of detected objects in the battlespace. CID is a fundamental requirement in increasing combat effectiveness in long-range, highly accurate weapons.

Manpower will always be a challenge. Our junior Sailors are dissatisfied with current Internet connectivity and our ability to provide distance learning through programs like Navy Knowledge

Online, Sea Warrior and Distance Support while at sea. We are working with N1, the systems commands and the fleet to rapidly field these capabilities.

The business side of the Navy is hamstrung with our legacy IT systems that make our networks vulnerable to hackers and intrusions from our adversaries. We need to move to more distributed network operations and implement a data strategy that supports our information requirements.

We are working with the Department of the Navy Chief Information Officer (DON CIO), Commander, Fleet Forces Command, Commander, Pacific Fleet and the type commanders to identify, train and certify the Information Assurance (IA) Workforce. In 2005, the Department of Defense promulgated an Information Assurance Improvement Program to develop an IA Workforce who possesses a common knowledge base in order to protect and maintain information, information systems and networks.

Over the next year, Information System Technicians, Information Professionals and the civilian workforce, with privileged access to the network, should look forward to seeing new and expanded opportunities for IA training and free vouchers to obtain commercial certifications in information assurance.

We are also earnestly working with DON CIO to develop a cogent strategy for our people in the Information Management/ Information Technology (IM/IT) Workforce. As a starting point, I have talked with the Information Professional and Information Warfare communities to ensure I have situational awareness of the communities, their needs, and an appreciation of the vast talents they bring to bear in support of the Naval NETWAR FORCEnet Enterprise.

CHIPS: How has the war on terror affected how the Navy is looking at its C4ISR networking capabilities?

Vice Adm. Edwards: The war on terror has highlighted the need to provide robust, reliable, high speed unclassified and classified data exchanges for hosted applications and with coalition forces. The Navy is investing in network infrastructures such as Combined Enterprise Regional Information Exchange System–Maritime (CENTRIXS-M) and Integrated Shipboard Network System (ISNS).

N6 is making sure that ISNS and CENTRIX-M networks provide increased capability to meet documented warfighter requirements such as the Automatic Information System and the Global Command and Control System-Maritime. This will foster a net-centric operational environment across the enterprise that allows improved fleet sufficiency in information sharing for the warfighter. It will also facilitate tactical and operational information sharing with our coalition partners.

CENTRIXS-M grew from an operational need for information sharing with allies and coalition partners during Operation Iraqi Freedom. The Navy has made rapid advancements with CENTRIXS-M to improve the free flow of actionable intelligence between the Navy and our allied and coalition partners.

The Navy's Space and Naval Warfare Systems Command has added some significant enhancements recently with the addition of multilevel thin clients (MLTC) to the CENTRIXS-M architecture. MLTC significantly improves our ability to share information simultaneously with our partners in the global war on terror, and it was fielded with relatively little expense.

MLTC allows Sailors to access several enclaves from the same terminal. This reduces the number of workstations required onboard and the expense to maintain them. This is a great example of the agility we need in our IT capability procurement.

"IO is a perfect example of why Adm. Mullen reestablished the N6 Directorate. It is a key warfighting area for the Navy in the post 9/11 security environment, where we are placing increased emphasis on non-traditional mission areas and asymmetric warfare."

– Vice Adm. Mark Edwards
OPNAV N6

CHIPS: Can you talk about the information operations mission area?

Vice Adm. Edwards: I'm glad you asked about information operations, or IO — it is a really important area of our portfolio. N6 has the responsibility for IO in a matrixed role with N3/N5. For me, IO is the perfect complement to all my other N6 mission areas.

Over the last four months, we've studied technology trends and have an appreciation for how these can accelerate C2, not only for us, but for our adversaries as well. By applying these trends to our C2, we can generate our force capability more quickly and, at the same time, use IO to slow the generation of our adversaries force capability. This particularly applies to the manner in which we will conduct major combat operations in the future.

The conflict against transnational terrorism is an information-rich fight that challenges the existing way we do IO. We can't expect to jam a terrorist radar or spoof its missile seeker. The techniques we use in GWOT will be much more subtle and directed at individuals vice opposing naval forces. The forward operating posture of U.S. Naval Forces is well-suited for these kinds of effects.

In a world that is globally connected, the ability to employ the elements of IO is critical to achieving and maintaining information superiority. As we continue to operate today and prepare for the future, using computer network defense to protect our IT investments and providing the fleet with unique electronic or digital attack capabilities is essential for operating around the globe in the information-laden 21st century.

There are other Navy players that work capabilities for specific platforms that can perform IO missions, but we at N6 focus on cross-platform or platform independent weapons and tools.

In the coming year I am particularly interested in examining high-payoff efforts to exploit, influence, deny, degrade, deceive and/or delay adversary efforts using computer network attack as well as electronic attack.

In summary, IO is a perfect example of why Adm. Mullen reestablished the N6 Directorate. It is a key warfighting area for

the Navy in the post 9/11 security environment, where we are placing increased emphasis on non-traditional mission areas and asymmetric warfare. It is imperative that we stay ahead of our adversaries and be able to exploit, influence, deny, degrade and/or deceive inside their decision loop while maintaining the integrity of our own.

CHIPS: As part of your job, do you work with Vice Adm. Nancy Brown, the J6 on the Joint Staff, and your counterparts in the other services?

Vice Adm. Edwards: My team and I work very closely with the Joint Staff and the other service 6s. The transformation to a network-centric battlespace means the services must interact more closely then ever before. The key to net-centric interoperability is the GIG. My staff works closely with our sister services through participation on several joint requirements boards.

Closest to home, the Blue in Support of Green, or BISOG, is a standing three-star level requirements board focusing on Navy's commitment to supporting the Marines. The long-standing relationship between Navy and the Marines has been cemented by the need to provide seamless connectivity whether our maritime force is in transit, conducting ship to objective maneuver operations, or providing logistics support.

I've just sent a liaison officer to Headquarters Marine Corps C4 to complement the Marine communications officer on my staff. We work very closely with Brig. Gen. George Allen, Director C4, Headquarters Marine Corps, on such projects as installing secure wireless network access aboard amphibious ships to support embarked forces.

My staff represents me on the U.S. Joint Forces Command-led CID Working Group (CID WG) that also has representatives from the services, combatant commands, Joint Staff and agencies that report to the C2 Functional Capabilities Board. This CID WG develops and helps coordinate CID, blue force tracking, and Joint Blue Force Situational Awareness tasks, as well as maintains accountability in a formalized action plan that could influence the Navy investment and integration of warfare technology resources.

Going a step further, my staff has been engaged in developing the systems and procedures that support interoperability with our closest allies. The reality of Adm. Mullen's MDA concept means our Navy operating with long-standing allies and ad hoc coalition partners in a myriad of wartime and peacetime humanitarian missions.

The recent Pakistan flood relief and Joint Task Force Lebanon missions demonstrated how effective naval command and control is exercised through C4 circuits across the joint and coalition environment.

OPNAV N6 is also the Navy Major Area Sponsor for the JC4I Curriculum that is taught at the Naval Postgraduate School and participates in all curriculum reviews for the JC4I course taught at the Joint Forces Staff College. N6 works very closely with the J6 staff personnel to identify Joint Officer and Enlisted Manpower, Personnel, Training and Education requirements.

The Navy's IT portfolio reduction and standardization efforts are closely aligned with DoD and the Marine Corps. We both use the Department of Navy Applications and Database Management System to capture detailed information on our investments in networks, servers, devices, applications and databases. The functional area managers in both services work together with the overall goal of developing standard processes and solutions.

"The Navy's IT portfolio reduction and standardization efforts are closely aligned with DoD and the Marine Corps. We both use the Department of Navy Applications and Database Management System to capture detailed information on our investments…"

– Vice Adm. Mark Edwards
OPNAV N6

CHIPS: Can you talk about N6's role in space communications?

Vice Adm. Edwards: It is a naval tradition for Navy commanding officers to operate with relative independence from higher headquarters. The net-centric battlespace, however, requires greater connectivity than ever before. For the Navy, that means greater dependence on satellite communications (SATCOM). The majority of Navy's space-related capabilities are provided by either the Air Force or the National Reconnaissance Office.

My staff pursues space-delivered services through robust participation in joint and national security space decision-making processes. My directives are to focus on smart investments in space technology and exploit space technology developed by other services and national sources.

The Navy Tactical Exploitation of National Capabilities Program, or TENCAP, leverages a modest research and development budget to develop innovative solutions for emerging fleet requirements and mission capability gaps in this area.

The Navy is also the acquisition agent for narrowband, unprotected SATCOM, and is responsible for the joint Mobile User Objective System (MUOS) development and acquisition, which will replenish our narrow-band communications satellite system. MUOS will provide 'communications on the move' from the high-seas to jungles — to urban environments for disadvantaged users.

MUOS is the common denominator for command and control capability from tactical to theater levels, to allies and coalition partners, and between DoD and non-DoD agencies.

In addition to its SATCOM responsibilities, Navy acquires the applicable user equipment to enable use of space capabilities, such as the Global Positioning System. In the arena of rapid technology deployment, the Naval Research Laboratory's Center for Space Technology has taken a key role in the Tactical Satellite (TacSat) series of small satellite experiments, starting with the development of TacSat-1 funded by the Office of Force Transformation.

To view Vice Adm. Edwards' biography, go to Navy NewsStand's Biographies page at http://www.navy.mil/navydata/bios/navybio.asp?bioID=102.

CHIPS

Rear Adm. Donald K. Bullard
Commander, Navy Expeditionary Combat Command

Rear Adm. Donald K. Bullard

The Navy Expeditionary Combat Command (NECC) is a vital new element in the Navy's role in the global war on terror. The establishment of NECC in January brought the manning, training and equipping of Explosive Ordnance Disposal (EOD); Naval Coastal Warfare; Riverine; Combat Camera Atlantic; the Expeditionary Combat Readiness Center; Navy Expeditionary Logistics Support functions; the Maritime Civil Affairs Group and the Seabees under one umbrella. NECC integrates all warfighting requirements for expeditionary combat and combat support elements. This transformation allows for standardized training, manning and equipping of Sailors who will participate in maritime security operations as part of the joint force.

Rear Adm. Bullard has been the NECC commander since its establishment in January 2006. Just months away from the command's first anniversary, CHIPS asked the admiral to discuss NECC capabilities.

CHIPS: In May, the Navy reestablished its riverine forces which were last used during the Vietnam War, has the 40-year gap been difficult to overcome in terms of training and fusing forces?

Rear Adm. Bullard: Our riverine forces are just one part of the NECC puzzle which includes the Navy's expeditionary forces. Having a commander overseeing the manning, training and equipping of all these forces is new but the majority of the capability has been here within the Navy COCOMS, or combatant commands, for a long time. We have had Seabees for a long time. Underwater demolition has been here for a long time. We have been doing expeditionary logistics from the sea base for a long time.

Riverine forces establish and maintain control of rivers and waterways. They provide a continuum of capability from the green water to the brown water areas. Riverine forces balance our efforts to combat sea-based terrorism and other illegal activities, such as transporting weapons of mass destruction, hijacking, piracy and human trafficking. While many may think that is new, it really is an expansion of our current naval coastal warfare capability.

In addition to riverine, the Maritime Civil Affairs Group is a new structure in our organization, but the Navy has been doing civil military operations around the world since we came into existence. We do port visits; we do community relations projects like Project Handclasp; we have done tsunami relief, and we have assisted in Bangladesh. Those are civil military operations.

In the civil affairs group, we will formally train people on how to do civil affairs because we have been doing it ad hoc until now. This is to make sure that we have people that are well-trained to plan and assist the naval component commanders to do civil affairs.

This is a new organization, but it is not a new Navy core capability that we are building. Another new organization within NECC is the Expeditionary Training Command because we recognize the need to focus on our partners' ability to help with maritime security operations. But the Navy has been training with foreign militaries around the world for many years. Many countries do not have a big navy, but they do have small navies. They have small boats, and they do have maritime security concerns in their territorial waters, in their ports and harbors.

The Expeditionary Training Command will deliver timely, focused and customized training to host nations. This supports critical regional stability by helping improve the recipient nation's capabilities in exercising maritime sovereignty.

None of this is new, it is simply adapting to what the maritime environment looks like today. It is balancing the Navy's capability across the full spectrum to be able to make sure that the sea lines of communication in blue water are secure — and that the harbors, ports and littorals are secure. It's extending our reach, doing maritime security operations on inland waterways whether it is on the Euphrates in Iraq or elsewhere.

This is ensuring that the Navy has capability across the full spectrum over the blue water, the green water and the brown water, and that is what NECC is doing.

A lot of people focused just on riverine because it's the 'Gucci' thing. Even though it is important that we be able to operate in that environment, so we deny sanctuary, freedom of movement of terrorists, and interdict arms and human trafficking, piracy — all of those things — it is just part of the continuum that we are building. It does not stand alone — nor can it stand alone.

NECC is all about closing any gaps or seams that may exist. It is not to duplicate or take away from what another service might be doing. It is to be sure there is seamless transition from what the Marine Corps does to what we do.

As we see in riverine, we are supporting the Marine Corps with its mission coming up after the first of the year. There has been a lot of supposition that we were building the 'naval infantry' — the naval infantry is the U.S. Marine Corps. We are better organizing and improving our warfighting effectiveness in these core maritime expeditionary areas.

CHIPS: You had to start from scratch as far as organizing the groups that are now under NECC. How did that come together?

Rear Adm. Bullard: We have force commanders that are charged to man, train, equip, organize and resource. We have had those for a long time — for AIRFOR (air forces), SURFOR (surface forces) and SUBFOR (submarine forces) — they are called type commanders (TYCOMS).

About 18 months ago, we saw that we had other forces that did not have a coherent force commander, and they had been below the threshold until 9/11 — Seabees, EOD, and naval coastal warfare. They have been around for a long time and are now in high demand by a lot of the geographical naval component commanders.

In the past, they had some challenges, whether it was resources or training support. They did not have anyone with the oversight to help them get the visibility they needed. They needed to be properly organized to respond more effectively to the demand signal and request for forces by the naval component commanders or by the COCOMS, and they needed visibility in the budget.

We needed to establish, just like we did for AIRFOR, SURFOR and SUBFOR, a command that brings this all together, that better organizes them, capitalizes on the synergy in training and equipment, gives them visibility in the budget and can better package them in their mission for the naval component commanders — and provides a better command and control structure for them. They need a commander that can do all that.

About 18 months ago, the decision was made to stand up another type commander, and we went to CNO, the Chief of Naval Operations, with our proposal. Also about that time, the Navy recognized that it needed to expand and balance these capabilities and better organize them, and soon after that Navy decided it needed to expand into the inland waterways. Even though we had naval coastal warfare, we felt the need to expand that.

We need to better organize civil military operations and have teams of regional experts so that when we do tsunami relief, for example, we better connect to the combatant commander's theater security operational plan.

As the CNO expressed his vision of the 1,000-ship Navy, a global architecture of allies and coalition partners and friends that can act together globally to create maritime security — whether it be counterterrorism or piracy or human trafficking that also has an interactive full-time global force, the realization was that many countries do not have a large, traditional navy. They have small boats. We need to train to them, and that's how the idea for the Expeditionary Training Command came up.

We recognized that we needed a type commander for existing expeditionary forces. They all operate in about the same battlespace — near coast, near inland, inland waterway so it made sense to bring them under this commander also.

They were already organized as Seabees, EODs and naval coastal warfare forces. Riverine, Maritime Civil Affairs Group and the Expeditionary Training Command are in the same area too — in this maritime expeditionary environment. It made sense to bring them under NECC. There are lots of synergies in training and equipment that we can capitalize on.

Last October it was approved by the CNO to bring all of these capabilities under a new type commander, and January 13, 2006, we stood up. For 10 months we have been bringing this all together. Our focus is on properly organizing these forces, increasing the warfighting effectiveness for our naval component commanders, making sure they are properly equipped and trained, making sure they see the right resources and visibility in the budget and providing a more coherent command and control structure for the warfare commander of these forces. It has been a challenge.

CHIPS: Is the intent to deploy with the strike group and the Marine Expeditionary Force? Or are your forces deployed on the request of the COCOMs and component commanders?

Rear Adm. Bullard: NECC is not a warfare commander. We are a TYCOM. We are charged with manning, training, equiping, organizing and resourcing the Navy's expeditionary forces. We are a force provider. We get a mission request from one of the fleet commanders, and we make sure to build an adaptive force that meets that capability, and then we will deploy a force to that fleet commander.

Santa Rita, Guam (Dec. 15, 2006) – Commander, Navy Expeditionary Combat Command, Rear Adm. Donald K. Bullard, displays the Navy's first Expeditionary Warfare pin, awarded to Master-at-Arms 2nd Class Carl Hurtt, assigned to Mobile Security Squadron Seven (MSS-7), during a ceremony onboard U.S. Naval Base Guam. The Expeditionary pin, the Navy's first new warfare device issued in the last six years, is the latest in a series of milestones implemented by the Navy to acknowledge the service's need to have Sailors with core expeditionary capabilities. U.S. Navy photo by Mass Communication Specialist 2nd Class Edward N. Vasquez.

In conjunction with our two training fleets, 2nd Fleet and 3rd Fleet — they are the ones that deploy the forces around the world — we are in charge of making sure these adaptive forces meet the mission capability. We are not a warfare commander; we are a type commander, or force provider.

CHIPS: The forces that are under NECC, for example, the EOD capability that you have and the riverine forces, will they become a regular part of the strike group?

Rear Adm. Bullard: Some of our forces are integrated into strike groups and expeditionary strike groups, like the EOD, but the Seabees are not. Seabees are deployed on a rotating basis around the world to the different naval component commanders — 6th Fleet, 5th Fleet and 7th Fleet.

EOD is also deployed to those fleet commanders and the naval component commanders as are the maritime security forces. Some maritime security forces are integrated.

Our objective here is to take the mission requirement — whether it be an integration into another force, with the Marines, Army or carrier strike groups or on their own — and assure that the deployed unit can meet its mission. As a force provider, our forces could be integrated into the joint force, into the Marine force, into other naval forces or they can act independently depending on the mission requirements.

Whidbey Island, Wash. (Dec. 12, 2006) – Commander, Navy Expeditionary Combat Command, Rear Adm. Donald Bullard, speaks to members of Explosive Ordnance Disposal Mobile Unit Eleven during his visit to the unit. U.S. Navy photo by Mass Communication Specialist 1st Class Bruce McVicar.

Riverine is not a permanent part of the strike group, but riverine could operate in an environment where it reports to the strike group commander. We are not going to deploy a bunch of small boats in a strike group.

CHIPS: Can you talk about the coastal warfare mission?

Rear Adm. Bullard: Naval coastal warfare has been done for many years, but the current genesis came out of Vietnam. In Vietnam, naval coastal warfare went into riverine and when it came out of Vietnam, it was split into two areas: one was special boat teams that went to the SEALs, and naval coastal warfare, which was mainly all Reservists until recently. Their mission is coastal surveillance and maritime security operations.

Today, we do surveillance and small boat security operations in three or four different ports in U.S. Central Command. We provide high-visibility or high-value unit protection, procure needed small boats to protect them and provide force protection teams for transit of noncombatant vessels for the Maritime Sealift Command, for example.

We have security teams. Naval coastal warfare is about security in harbors and bays in the near shore to be able to do surveillance and interdiction and maritime security.

CHIPS: Does maritime civil affairs fill a diplomatic role?

Rear Adm. Bullard: We are not in charge of diplomatic engagement with countries. The State Department does that. We are there to support those objectives with certain civil military operations. Are we training diplomats? No. We are training individuals to be regionally focused, who are able to coordinate civil military operations into a coherent plan that connects into the naval component commander's engagement objectives. The COCOMS are connected with the State Department. We are down the chain quite a bit.

The purpose of Maritime Civil Affairs Group teams is to gain expertise and knowledge of how to work with the interagency process and how to work with the NGOs (nongovernmental organizations) in disaster situations. It is about the Navy having a trained set of individuals who can plug into the humanitarian disaster relief organizations.

"We have made leaps and bounds in the last year. All of the capabilities that we have talked about will be deployed in the next six months. Riverine will deploy sometime after the first of the year. It took 10 months from the word go to stand it up with fully trained Sailors and equipment capability."

– Rear Adm. Donald K. Bullard
Commander, Navy Expeditionary Combat Command

As we saw with Katrina, the main thrust of the first responders came from the Navy. No one could get in there. We did an amazing job. We had quite a few of our forces down there. We want to have people professionally trained to be able to run civil military operations from the sea and better connect with the Federal Emergency Management Agency or the U.S. Agency for International Development if needed.

Do we support the State Department and the country teams diplomatically? Sure we do.

CHIPS: I've read news reports about the enthusiasm of the brown water Sailors. Why do you think they have this level of enthusiasm?

Rear Adm. Bullard: It is not just the brown water Sailors; everybody connects brown water Sailors with riverine because that is what everybody thinks it is. But there are other people doing brown water stuff. It is really about expeditionary Sailors. I have people doing customs and cargo handling in Kuwait, who are just as excited as the Sailors on those boats.

I have good Sailors, who are teaching Iraqis security procedures and how to guard oil platforms in the North Arabian Gulf, who are just as excited as the people on those boats. It is about expeditionary Sailors; it is about all of them.

Why are they excited? It is the small unit camaraderie in most cases. It is personal involvement when you talk about four people on a boat. They rely on each other. It is up close and personal with the environment. Even though our Navy mission out at sea is just as important, I would not trade one of my boats for an aircraft carrier. It is the full spectrum that we need.

The Sailors see that we, the Navy, need to be in this environment because this is a maritime environment. It's challenging both mentally and physically.

CHIPS: Do expeditionary Sailors exploit technology or would you say that their work is more hands-on?

Rear Adm. Bullard: That is part of NECC's charter, to see where we can bring in technology to improve warfighting effectiveness, to provide better force protection and to reduce the manpower load.

We have tactical unmanned air vehicles and unmanned surface vehicles. We are bringing in sensors and data technology to the boats. By having that technology, we can expand maritime domain awareness from near inland harbors and all the way out

China Lake, Calif. (Nov. 6, 2006) – Sailors from Naval Coastal Warfare Squadron Five and Explosive Ordnance Disposal (EOD) Group One shoot an M-16 at a target 25 yards away for a weapons qualification course during a joint task force exercise. U.S. Navy photo by Mass Communication Specialist Seaman Jose R. Rolun.

to the blue water with the carriers so you have an integrated picture.

Bringing technology into this area will allow us to have that common operating picture that spans the blue, green and brown water.

CHIPS: Is there a group doing experimentation for NECC's mission areas?

Rear Adm. Bullard: We are capitalizing on the normal Navy process as well as the joint process. The Office of Naval Research is looking into some things for us. We are capitalizing on some of the things that DARPA, the Defense Advanced Research Projects Agency, is doing for the other services. We are working with the Marine Corps Warfighting Laboratory.

Do we have a science and technology entity that specifically supports us? No, but I do have a technology strategy directorate that is leveraging all the other things that go on. We need to bring in today's technology.

We are leveraging off all the other efforts that are going on. It can be Army, Air Force or industry. When we talk about security, which is our main function here, there are a lot of things that are commercially available or that research is doing about security issues that can apply here.

CHIPS: Can you talk about the gaps that you are filling for the Special Operating Forces and Marines.

Rear Adm. Bullard: We are trying to see what our interdependencies are with the Marine Corps, the Special Forces and the Coast Guard. We are still doing that analysis. There are interdependencies.

There may be times where there is a maritime security mission that is just Navy. There may be a maritime security mission supporting the Marines on the ground, or there could be a maritime security mission where the Marines need to support us.

We are developing the concept of operations and trying to see where there are gaps. The Coast Guard owns many small boats. We are working to where we have the right commonality and techniques, tactics and procedures. The Coast Guard has officers embedded in our naval coastal warfare, and they deploy with us. We have Coast Guard boats around the oil platforms and harbors working with us overseas.

We have lots of small boats too. Since the Coast Guard is in charge of homeland security, if need be, we're looking at how could we add to their capacity. We are looking at that interdependency.

Where can we support the Special Forces mission? We are helping Special Forces in a couple of places to do some of their security. We're asking, what do we need to do to build capability that better enhances their mission?

CHIPS: Can you talk about what you would like NECC to look like in five years?

Rear Adm. Bullard: In five years we want to see it as a mature TYCOM, such as AIRFOR and SURFOR. We want to have a mature structure that provides the best warfighter effectiveness of these forces and the best effectiveness and efficiency in responding to the mission requirements from the naval component commanders.

We want to ensure that we have the process that gives us the best command and control and force protection for our Sailors. We want to be an established pillar within the Navy. There is surface, there is sub-surface, there is air and there is medical, and we want expeditionary to be that pillar across the full spectrum of the supportable community in detailing, resources and equipment.

We have made leaps and bounds in the last year. All of the capabilities that we have talked about will be deployed in the next six months. Civil affairs and riverine will deploy sometime after the first of the year [2007]. It took 10 months from the word go to stand these up with fully trained Sailors and equipment.

All of these capabilities will be deployed and will be operating in the maritime environment whether it is in blue water or green or brown water. Will it be fully mature? No, but we will have initial operating capability. We will be maturing and building the processes and learning more about how we can get more effective warfighting out of these capabilities and how we can get better efficiency in providing and resourcing them.

In five years we will have an established force that has all the support and processes within the Navy to man, train, equip, organize and resource to support this expeditionary mission. I can see it today. By the end of next summer, we will really be able to see it because it will be there in a small portion.

The Navy is pushing for it and adapting to this new environment — understanding where they need to be, understanding what capabilities they need to have, understanding that these are Navy core competencies and going full speed ahead to make this happen. I think we are going to get there.

For more information about the Navy Expeditionary Combat Command, go to http://www.necc.navy.mil or contact the NECC public affairs office at (757) 462-7400 ext. 137 or ext. 177.

To view Rear Adm. Bullard's biography, go to Navy NewsStand's Biographies page at http://www.navy.mil/navydata/bios/navybio.asp?bioID=58.

CHIPS

Standing Joint Force Headquarters - Core Element

The mission of the U.S. Joint Forces Command Standing Joint Force Headquarters-Core Element is to provide the warfighter with a trained, standing core element to enable the joint task force commander to command and control joint and multinational assigned forces. The SJFHQ-CE is a team of operational planners and command and control specialists. This team of planning, operations, information management and information superiority experts form the backbone of the JTF command structure.

During day-to-day operations, the SJFHQ-CE is assigned to a theater commander. When a crisis develops in a theater, the SJFHQ-CE can be assigned to a JTF headquarters where it brings the knowledge base, collaborative tools and contacts from the centers of excellence to the JTF. This enables more proactive and coherent advanced planning and quicker use of capabilities than can be accomplished by ad hoc stand up of a JTF headquarters.

The SJFHQ stood up in summer 2003 under Air Force Brig. Gen. Marc E. Rogers. CHIPS interviewed Rogers during the launching of the SJFHQ and revisited the SJFHQ-CE to ask the current staff to assess its effectiveness three years after it was developed. (Rogers' interview can be found at http://www.chips.navy.mil/archives/03_summer/web%20pages/SJFHQ.htm.) CHIPS spoke with Chief, Standards and Readiness Division, Army Col. Paul Haveles; Navy captains Jeffrey Hood and Alan Hollingsworth; and Navy Cmdr. Kevin Robinson in November 2006 onboard Naval Station Norfolk.

CHIPS: Has the vision for SJFHQ been met?

Col. Haveles: As we fielded the organization under Brig. Gen. Rogers, we realized that our name carried a misconception. The SJFHQ name gave a perception to some people that we were a headquarters. Based on Adm. Giambastiani's (former commander of Joint Forces Command) guidance in January 2004, we have added the term or identifier 'core element.' SJFHQ's 58 people are what we call a core element.

The true term for the group that deploys is Standing Joint Force Headquarters-Core Element. They are not a headquarters, but they are the foundation upon which to build the headquarters or to help someone else build a headquarters.

The initial guidance was that all combatant commands would have a SJFHQ-CE by the end of fiscal year 2005.

That is a true statement; SJFHQ-CEs exist in some form or another at U.S. Northern Command, U.S. Southern Command, U.S. Pacific Command and U.S. European Command. As with any organization in the Department of Defense, now the struggle is over manpower because the global war on terror and the wars in Iraq and Afghanistan are taking a lot of manpower. There are not available personnel, and the SJFHQ-CEs may not get 100 percent of their manning.

They are meeting the intent of the design to get a core element fielded for each combatant command so each commander has the ability to facilitate the standup of a joint task force headquarters within his area of responsibility.

Since that guidance and your interview with Brig. Gen. Rogers, JFCOM has received guidance to stand up two operational core elements. Captains Jeffrey Hood and Alan Hollingsworth and Cmdr. Kevin Robinson are members of the operational core elements here at JFCOM.

One of the core elements has been tasked to support U.S. Central Command because it does not have its own core element. Now each geographic combatant command has a core element to facilitate the rapid stand up of a service component headquarters to a joint task force headquarters, which was the original intent of the guidance. Three years later, we are getting there.

U.S. European Command Joint Enabling Team and USJFCOM SJFHQ-CE personnel onboard USS Mount Whitney during Joint Task Force Lebanon in August 2006.

Are we at the total end state of where we wanted to be or the original documents wanted us to be? No. We have adjusted based on command guidance, leadership, environments and manpower.

CHIPS: Brig. Gen. Rogers compared the SJFHQ-CE to another weapon system in the U.S. military arsenal. Is this still a good comparison?

Col. Haveles: The analogy that Gen. Rogers used is in terms of its management — how the Department of Defense manages a weapon system from its conception, revision, fielding and program management. The SJFHQ needs to be managed in that same manner. The SJFHQ-CE was conceptualized in the late 1990s. It was tested during Millennium Challenge 2002, and it was fielded from 2003 to 2005.

Capt. Hood: The weapons system that he used refers to how the Air Force made its Air Operations Centers, the centers that control all the aviation assets that operate in theater. The Air Force termed this as a weapon system for the reasons the colonel was talking about — the whole life cycle of a weapons system including training students through the Air Force Command and Control Warrior School — and all the way to making them an integral part of the AOC. Even though the SJFHQ-CE is on a smaller scale, it is still a weapons system with a command and control team aligned with tools, trained personnel, and it has a life cycle.

CHIPS: What is the most important capability that you bring to an operational commander?

Capt. Hood: The most important capability that we bring is the personnel that are trained in joint processes of command and control. Having worked together we are

familiar with each other, we know the processes, we know our strengths and weaknesses, and we can be put into another organization, or we can have another organization come in on top of us.

We bring the initial capability of a trained staff able to speed the establishment of a joint task headquarters and the training, joint processes, and command and control systems that we would use in the various headquarters — that is our strongest capability.

Cmdr. Robinson: When the SJFHQ-CE for a combatant commander goes into theater what it brings is a combination of subject matter experts who are trained in joint operations across all spectrums of the military. The SJFHQ-CE knows how the combatant commander thinks, and this is part of how we enable that rapid stand up of those joint task forces and their headquarter elements.

CHIPS: Is there any problem in applying doctrine in a multi-service environment?

Cmdr. Robinson: You will always have service tendencies. The thing we typically see, for example, is Army Soldiers think as land-centric folks, Navy personnel think as sea-centric folks, and so on, but the joint doctrine is universal. What we bring is knowledge of how the other services work because we are continuously working with them in a headquarters environment. This allows us to learn how the other services think so proceeding with their service planning is not foreign to me as a naval officer.

Those seams between the services get reduced significantly because we are continuously working in that joint environment from a common doctrine.

CHIPS: How is the SJFHQ-CE different from the commander's staff? Doesn't he have the same skill sets and tools on his staff?

Col. Haveles: You have service component headquarters that exist – Army, Navy, Air Force, Marines. They have service-specific capabilities, and they focus on the tactical fight because that is what each service does. The transition is to a joint task force commander, who now has to think at the operational level of war with the integration of all the services capabilities, other agencies of the U.S. government and the integration of coalition partners.

The services don't normally think in these terms. The people of our core elements bring that perspective of the operational level of war with the integration of interagency and coalition partners to help him and his staff come up from that tactical fight to the operational level fight.

Service component headquarters personnel have those skills inherently in their military training, but they do not use them all the time because they are focused on their service area. Core element people help build the ability to think, work and function in the joint multinational interagency environment that they normally don't do on a day-to-day basis.

The JTF functions in a slightly different battle rhythm and thought process that has to know the combatant commander's intent. They bring that perspective, so that it gets spread through more of the staff as opposed to just commander to commander.

CHIPS: Does the SJFHQ-CE work with interagency organizations?

Col. Haveles: Yes. At the operational level of war, at the joint task force level, that is a normal operating event — to work in the multinational interagency environment. That is why the people of the core element must have that skill set and understanding of the interagency environment.

Cmdr. Robinson: Each core element here at JFCOM, for example, has a planner who is regularly developing interagency relationships by participating in discussions with a government agency. In my job as a maritime planner only a small portion of those I work with are U.S. Navy. I have to think about how we can utilize multinational navies as well as what other instruments of national power can be brought to bear in a situation.

We are continuously thinking how the multinational or the interagency piece fits into what we are doing. We are working on this on a daily basis depending on the operation we are planning. Two years ago I was thinking about driving ships, and now I am thinking about how I interface with the Department of State.

CHIPS: Can you talk about the collaborative information environment that you help the combatant commander establish?

Col. Haveles: The collaborative information environment is not a network or an application. It is a combination of four pillars: people, process, tools and the environment. It is a perspective on the workplace and how to get things done. By using a collaborative information environment, as people from the JTF headquarters build a plan, components of the subordinate units, the higher units, the combatant commander's staff and the Joint Staff are also participating.

You can have higher, parallel and subordinate organizations all participating in the building of your operational plan at the same time. It's coordinated, it's synchronized, it's smoother, and participants can agree to what capabilities they are required to provide.

During operations, rather than a stovepipe small element participating, there is a broader environment that reaches throughout the JTF headquarters and its components participating in the command and control of operations. It spreads out the knowledge base; it spreads out the information. It allows us to streamline our operations and make them more efficient.

The SJFHQ-CE personnel bring an understanding of the collaborative information environment with them. They can sit down at a workstation and reach out through collaborative tools and processes to other combatant commands to centers of influence, to other U.S. agency players and learn how to work with other people outside of their own level of expertise.

The core element, which is made up of 58 people does not have to have experts in every single field of endeavor. These 58 people can reach out to the expertise they need. It also means that everybody does not have to go into the theater of operations.

You can reach back through the collaborative information environment to people who are working in an operations center in Norfolk. You can still provide the required support, information and capability to the JTF commander. That is part of the value of the collaborative information environment.

I will not get into countries or specifics, but we collaborate with folks all around the world from here in Norfolk on a regular basis. We use multiple tools to do that — conference calls, video teleconferencing or voice-over-Internet Protocol headsets over a computer.

"The people on our teams could do their job with zero electricity — if they had to. They have been in austere environments in other countries — in Afghanistan and Pakistan — with limited technology capabilities and been able to do their job just fine. We exploit the technology; we use it to its maximum potential."

– Army Col. Paul Haveles
U.S. Joint Forces Command SJFHQ-CE

Years ago people did not think like that. They did not think about reaching out to other centers of excellence. They tried to work with whatever expertise they had on hand and their view of the world. Their view of their capabilities was limited to the expertise that was in the room. The collaborative information environment says that I can reach out to whatever experts I need to get the best answer or solution.

CHIPS: How heavily do you rely on technology?

Col. Haveles: Reliance? I am not sure that I would say reliance. Every one of us (if we needed to) could probably pull out a butcher block and a board and do what we need to do. We exploit the technological capabilities of today to use them to further our capabilities and our ability to conduct operations. I resist the term 'rely on' technology because I believe that the implication is that if it was not there I could not do operations.

The people on our teams could do their job with zero electricity — if they had to. They have been in austere environments in other countries — in Afghanistan and Pakistan — with limited technology capabilities and been able to do their job just fine. We exploit the technology; we use it to its maximum potential.

Capt. Hollingsworth: Technology is an enabler. Specific technologies are enablers, and we can use various pathways depending upon which systems are available and functioning for us. If a specific system that is our preferred method is not working, we might have two or three other redundant systems or methods that we can use. If there is none available, it will affect how we do what we do, but we still would have the ability to function.

CHIPS: Does the SJFHQ-CE help with the enormous amounts of data and intelligence the commander receives?

Capt. Hood: With the advent of technology, the commander has more opportunities to receive more critical information. In that aspect, technology is critical to what we do. It gives us that advantage with all that extra information. It speeds his ability to make decisions and affects his decision cycle, assuming that the information is handled properly. Information overload is very easy.

Within the SJFHQ-CE are knowledge managers whose focus is to make meaning out of that information and make it such that it is sorted, displayed and provided in usable bits to the different elements of the staff, so that the commander can make decisions and speed his decision process. Within our information superiority cells we have people with intelligence backgrounds who do traditional analysis.

Cmdr. Robinson: Besides the information superiority section, the SJFHQ-CE is cross-functionally organized. You do not have the old Napoleonic organization of J1, J2 and J3. In the planning cell or planning portion of SJFHQ we have intelligence planners. What they bring to the table is that as the plans group is making a plan or the operations group is executing an operation, those cross-functional members are already there.

When analysis is being done by the information superiority team, someone from the plans team is regularly interfacing with them, integrally involved in the planning process. This provides the combination of moving people with cross-functional areas into various teams and gives you a synergistic affect across the core element.

Capt. Hollingsworth: Beyond the core element members and the groups that have already been discussed, we also have systems of systems analysts, who provide information processing and mining that assists the core element teams and the supported combatant commanders.

Col. Haveles: The only piece of clarity that I want to give you is that the SJFHQ-CE is not doing data analysis and intelligence preparation. The JTF headquarters that the SJFHQ-CE is plugging into and augmenting is doing this. We are helping them with their process on how to analyze data.

CHIPS: What else would a SJFHQ-CE provide?

Capt. Hollingsworth: I deployed in August for Joint Task Force Lebanon. The core of the JTF was the 6th Fleet staff led by Commander, Sixth Fleet and Deputy Commander, Naval Forces Europe Vice Adm. John Stufflebeem. Personnel from other parts of EUCOM – Army, Air Force and Marine Corps forces manned the rest of the JTF headquarters.

The SJFHQ-CE equivalent from EUCOM — the Joint Enabling Team (JET) — provided people with certain skill sets that they were short on in the JTF staff. Joint Forces Command provided nine people, two from other elements and seven from SJFHQ, with additional JTF skill sets that the JET needed. The JET helped JTF Lebanon stand up in a couple of days and accept the responsibility for the evacuation of American citizens from Lebanon as well as the support and potential evacuation of the American Embassy in Lebanon, a mission the JTF had not been trained for.

As a joint task force headquarters they had been trained to fight an air campaign, something similar to what was done in Kosovo and Bosnia in the 1990s. By bringing a SJFHQ-CE equivalent from EUCOM, supplemented with skills from JFCOM, we were able to take a JTF oriented around an air mission — refocus it — and give it the capability to conduct land and sea-focused missions.

It would have taken three to four weeks for the JTF to be able to prepare for that same mission without the specialists that were brought in. In that deployment we were able to reach back from onboard the USS Mount Whitney (LCC/JCC 20) in the Mediterranean Sea to our building in Norfolk and draw on the special skills and analysis of our people back here. They would not have been accessible to the JTF had we not been participating in the JTF standup.

This was a good demonstration of the capability the standing

core group of JTF experts can bring to an environment when something unexpected occurs, and the JTF is not prepared.

We had to coordinate getting Army land-based helicopters from Germany to Cypress where they could support the U.S. Embassy. We had to look at the qualification of those helicopters to operate off our ships — if they needed to land on our deck in between the two land masses. We were bringing in Air Force helicopters to provide armed escort and support if needed. We learned that the Army helicopters were not outfitted and trained to pick people out of the water.

There were a lot of complicated issues that a group of people within the headquarters staff of 6th Fleet and even the European Command may not have been aware of and noted without bringing in people with cross-functional skills and expertise.

Capt. Hood: Since your last interview we have had a couple of opportunities to employ SJFHQ-CE. The captain just alluded to JTF Lebanon. One thing that you may have noticed is that none of them have used the entire textbook construct of the SJFHQ-CE deploying as an entire group. We have chosen to tailor it, which is one of the benefits of a tailorable package, to be able to give combatant commanders exactly what they need.

We supported the Department of Homeland Security during Katrina in the planning cell. We sent about 40 people down to Baton Rouge at the joint field office to provide planning support. This was the initial deployment for Core Element – Alpha.

After that we supported the Expeditionary Strike Group 1 and Rear Adm. Michael LeFever in Islamabad, Pakistan. We sent a team to become an integral part of his staff in Islamabad coordinating the humanitarian relief effort following the earthquake.

After that we sent a core element team into Afghanistan to Combined Joint Task Force 76 to stand up a new task force. We provided planners, intelligence and operations personnel to speed that task force for CJTF 76. That mission lasted about six months with varying levels of support personnel. It is now finishing off with support to ISAF, the International Security Assistance Force in Afghanistan.

Our most current effort is to provide an augmentation to U.S. Central Command Air Forces. CENTAF was charged with standing up a headquarters to provide support for Internal Look '07, which is an exercise with follow-on operations. We have a team deployed providing support as an augment to CENTAF providing the full spectrum of capabilities that we bring as a JTF.

CHIPS: Can you talk about the stand up of the SJFHQ-CE for CENTCOM?

Capt. Hood: Central Command (being occupied with two major combat operations in Iraq and Afghanistan) did not have the personnel available to stand up its own core element. JFCOM has two core elements and has opted to dedicate one of our core elements to CENTCOM for planning purposes. If CENTCOM needs one — we will be there.

Air Force Gen. Lance Smith, commander of JFCOM (and NATO Supreme Allied Commander Transformation) dedicated one of his core elements for planning purposes. A relationship is forming between the Central Command staff and the Central Command component headquarters, like its CENTAF and U.S. Central Command Naval Forces, or NAVCENT, to understand what this core element does and what its capabilities are.

CHIPS: When you deploy is there an average length of time that you can assist?

Capt. Hood: I think that the length of time we are deployed is dependent on the supported commander and what he needs. Since we are not aligned with a geographic combatant commander, if CENTCOM needs us, we will go as long as it needs us.

There are planning factors that we would like to adhere to, but we will provide the support that the commander needs for the duration that he needs it.

CHIPS: Is it part of your mission to train the commander's staff?

Cmdr. Robinson: Within Joint Forces Command, J7 is responsible for training. But any person who brings expertise to a staff has, in typical military fashion, the duty to train others. If we come as people who have a skill set and extra training in joint procedures, processes and tools we will share that training, but we do not roll in as the trainers. That is not a mission of the SJFHQ-CE. But we will, if we are turning over the mission, do 'left seat, right seat' type training where we train our reliefs and then let them take the seat.

Capt. Hollingsworth: When we went over for JTF Lebanon, the bulk of the task force had already been through more than a year of training and preparation to be certified as a joint task force. However, there were a lot of people who had turned over and had not been through all of that training. The guy on our team who had the most experience and expertise took aside several members of the JTF headquarters and went through the same training material that we received when we were training here at SJFHQ-CE.

Another thing that we were able to do was to help the effects-based cell team members to integrate what they were doing with the joint planning group of the JTF headquarters. The guys who were analyzing the effects of our actions were also integrated with the guys making plans — instead of having two separate functions without a connection.

CHIPS: Have you helped the Combined Joint Task Force Horn of Africa?

Capt. Hollingsworth: My core element, Core Element B, went through the mission rehearsal exercise which was one of the last major training steps for the task force headquarters that is over there now. We did that in February 2006, and when they deployed and assumed the Horn of Africa mission we sent a small group of people with certain skill sets that they needed. We have had three to seven people from our core element, at any one time, in the Horn of Africa.

They have had some interesting experiences helping to engage with the national militaries and also with the other government agencies and non-government organizations that are working in that part of the world.

For more information about the Standing Joint Force Headquarters-Core Element, go to the U.S. Joint Forces Command Web site at http://www.jfcom.mil/about/fact_sjfhq.htm. Or you may contact the SJFHQ strategic communications specialist at (757) 836-9730 or DSN 836.

CHIPS

Subnet Relay - Enhancing Multinational Connectivity

By Canadian Navy Lt. Cmdr. Robert Sibbald, U.S. Navy Lt. Joe Zuliani and Dr. Stephan Lapic

To many members of the multinational naval communications community, SNR means signal-to-noise-ratio. But to a growing number of communicators this acronym has a new definition: Subnet Relay. Subnet Relay is a true masterless, ad-hoc, self-organizing data networking technology with inherent relay capabilities that employs tactical line-of-sight (LOS) bearers to carry Internet Protocol (IP) data between groups of ships within a task group.

As a result of multinational collaboration, SNR has been developed over the past few years, matured through successful demonstrations in sea trials, and is in the process of transitioning to the U.S. Navy fleet.

Coalition communications has been identified by the numbered fleet commanders as their number one command, control, communications, computers and intelligence (C4I) warfighting priority.

For nearly half a century, the AUSCANNZUKUS organization has worked to enhance maritime C4 interoperability between the navies of its member nations — Australia, Canada, New Zealand, United Kingdom and United States — and also with the larger coalition community.

In the late 1990s, as a result of increasing satellite congestion, mounting costs and a desire to improve communications availability, AUSCANNZUKUS articulated a requirement to use LOS bearers to carry IP data traffic ship-to-ship within a coalition task group, much like a tactical intranet at sea.

In 1999, work on what became the SNR system, began in earnest when representatives of the five nations met at the Defense Establishment Research Agency (DERA) facility in Portsmouth, U.K., to consider technical approaches.

Three years later in 2003, a prototype was featured as part of the AUSCANNZUKUS contributions to Joint Warrior Interoperability Demonstration (JWID) '03. Later that same year, SNR saw its first at-sea demonstration in a U.S.-Canada joint trial when a four-ship Canadian task group transited from Victoria, British Columbia, to San Diego, Calif. (See Figure 1.)

The trial proved to be a success, transferring data up to 64 kbps and achieving 24/7 network connectivity for four ships with only three satellite connections.

Previously, a task group would have to "time-share" the connections via a predetermined schedule, with a maximum of three ships being connected to the network at any one time.

National, binational and multinational sea trials continued over the next three years, including experimentation within Trident Warrior 2005 and 2006.

What sets SNR apart from many comparable systems is that it makes use of the existing shipboard radio and cryptographic infrastructure by bringing a new controller to use legacy equipment in new ways.

"Subnet Relay is the warfighter's version of what the dial-up telephone modem does to a phone line," said AUSCANNZUKUS C4 Interoperability Project Officer, Canadian Navy Lt. Cmdr. Rob Sibbald.

"Radio equipment that was originally designed for different types of voice communications can, with minimal investment, now be used for text chat, e-mail, Web browsing and other Internet-type applications."

LOS radio assets, primarily in the very high frequency (VHF) and ultra high frequency (UHF) bands, can be used to give tactical commanders an intra-task group data networking system under their local control — without having to rely on strategic reachback through satellite connections.

In addition, units with strategic satellite network connectivity can provide seamless bridging of the LOS subnet back into the global Wide Area Network (WAN).

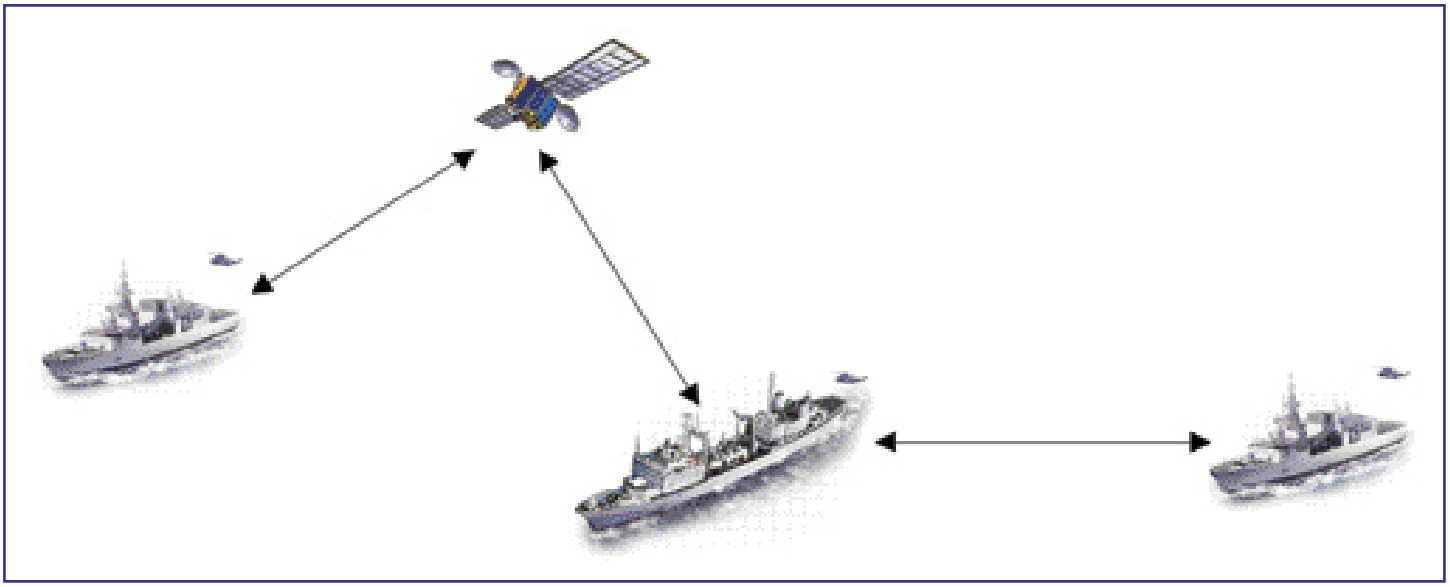


Figure 1. Ships sharing a satellite connection over SNR.

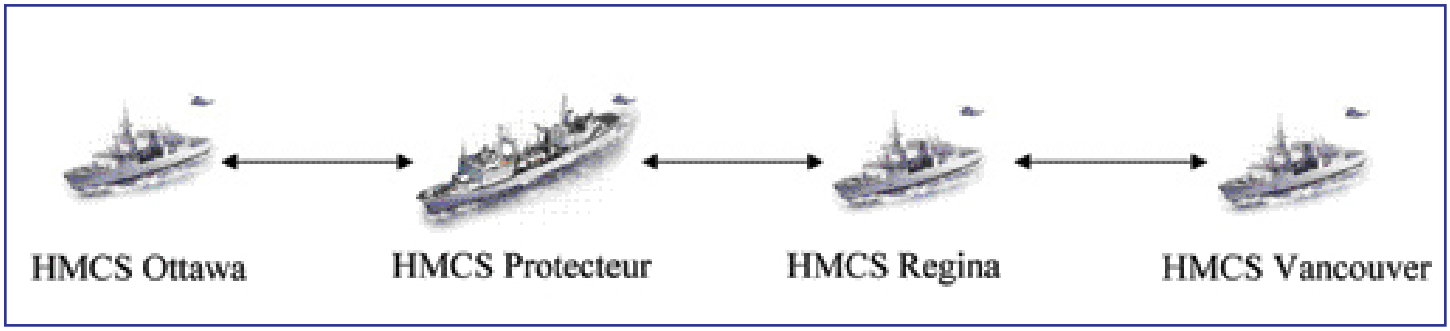


Figure 2. Ships connected in a three-hop SNR configuration.

"Coalition partners, who previously had limited or no shipboard satellite connectivity into tactical networks, such as the Combined Enterprise Regional Information Exchange System (CENTRIXS), can use this technology to increase their connectivity time by sharing another nation's link over SNR," Sibbald said.

This is all done without operator intervention. The system "discovers" other nodes in range, organizes transmissions without a master and relays traffic — automatically.

Sibbald calls this capability "Fire and Forget."

Another key feature of SNR is its ability to automatically relay IP traffic between participating units (or nodes), providing the capability of extending the network between ships that are outside of point-to-point radio range as other ships provide the automatic bridging.

Figure 2 shows IP data being sent from HMCS Ottawa (FFH 341) to HMCS Vancouver (FFH 331) automatically relayed (retransmitted) within the SNR technology through HMCS Protecteur (AOR 509) and HMCS Regina (FFH 334) to Vancouver.

The SNR solution requires two new pieces of equipment to be integrated into the legacy communications system: a self-configuring relay network (SCRN) control node and a high data rate (HDR) modem.

The SCRN control node uses a synchronous time division multiple access (TDMA) protocol to control channel access among multiple platforms, provides relay functionality to support data transfer in multi-hop topologies and provides interfaces to standard shipboard routers and cryptographic gear.

The HDR modem provides advanced coding to increase the data rate with interfaces to standard crypto and shipboard tactical radios. Figure 3 shows how the SNR node and modem fit into a ship's communications architecture.

Rockwell Collins, Inc. (formerly IP Unwired, Inc.) is the AUSCANNZUKUS commercial development partner for SNR. A SNR solution is available for acquisition by coalition members.

The SNR technology solution is in the process of being published as a NATO Standardization Agreement (STANAG) to allow nations to locally manufacture SNR communication products that would be fully interoperable throughout the coalition.

A similar process was used for Battle Force E-mail, an HF point-to-point communication system, published as STANAG 5066.

All AUSCANNZUKUS navies now have capital projects in place to field SNR in the 2007–2010 time frame.

A number of other NATO nations, including France, Germany and the Nether-

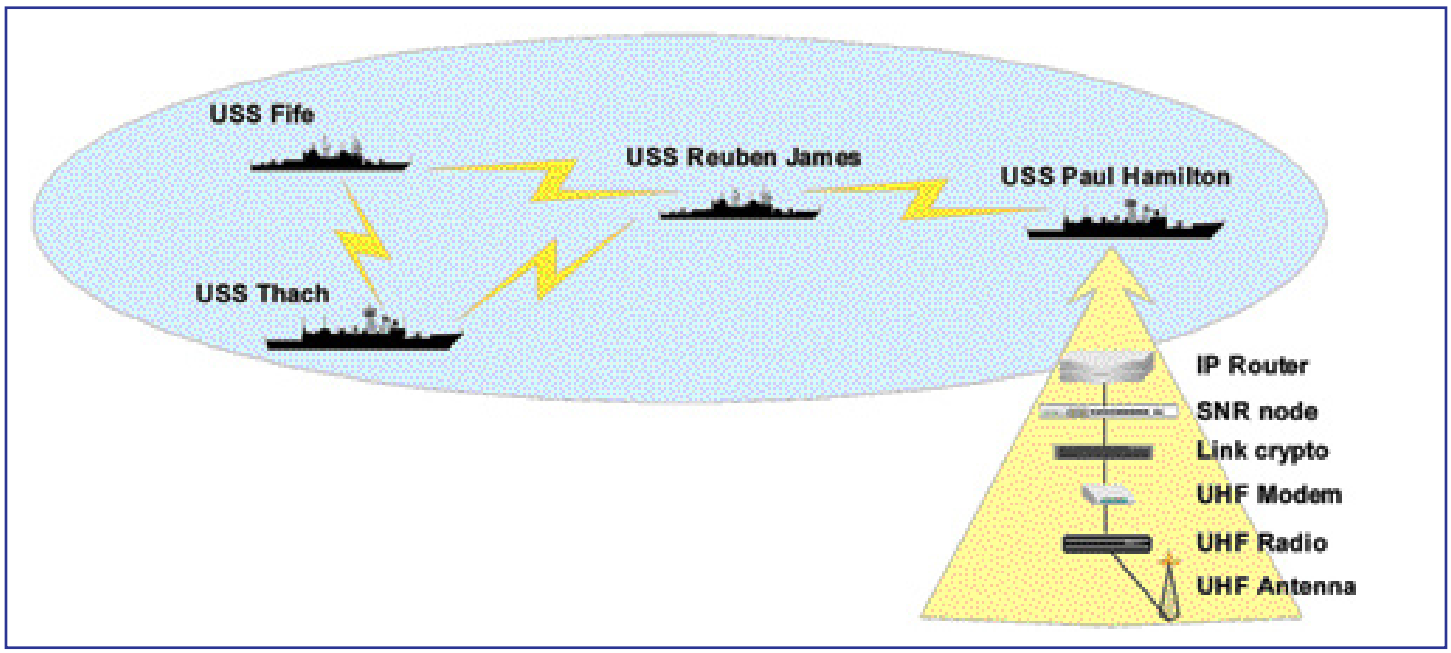


Figure 3. SNR equipment and basic topology.

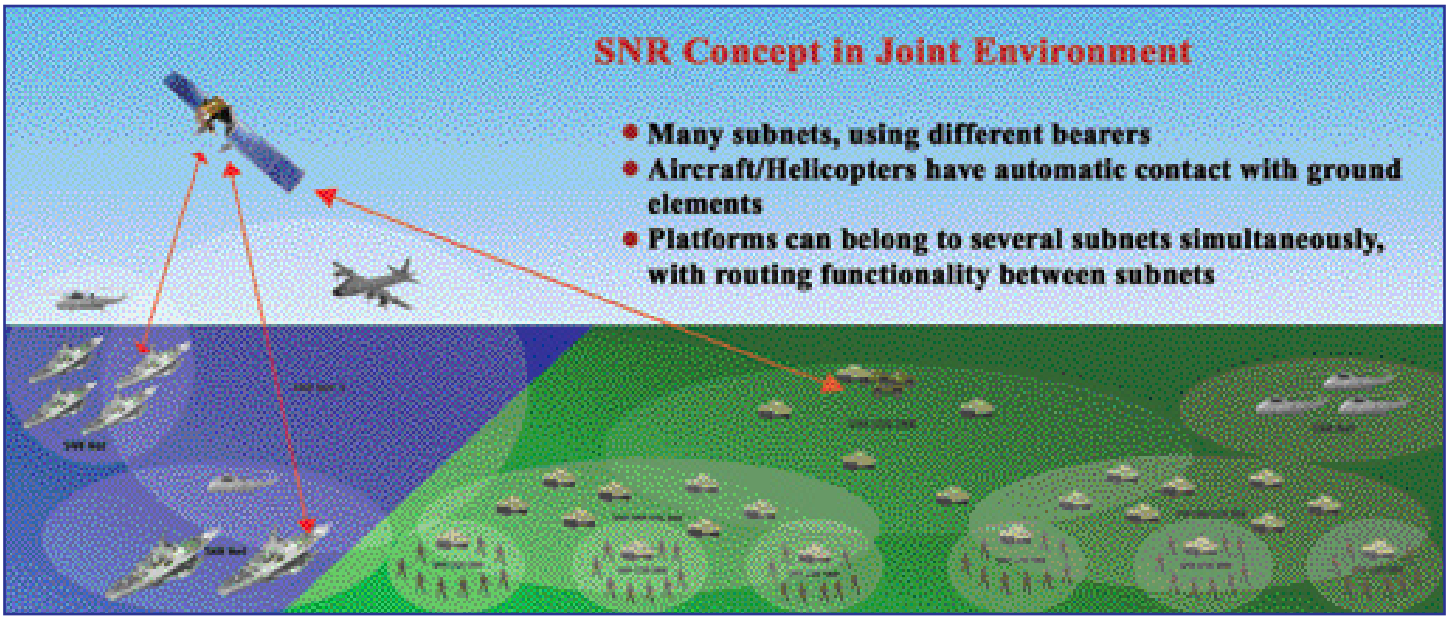


Figure 4. SNR Joint Concept.

SNR Technology Advantages

√ Self-organization of participating platforms into networks using line-of-sight (LOS) and extended line-of-sight (ELOS) UHF, VHF and HF bearers.

√ Automatic admission of properly configured new members into existing networks.

√ Automatic adaptation to topological changes as existing links fail and new links are discovered, including mechanisms for merging multiple SNR networks.

√ Traffic relay to extend connectivity to provide beyond line-of-sight (BLOS) connectivity in multi-hop topologies.

√ Distributed channel access to support contention-free transmission.

√ Adaptive allocation of bandwidth that adjusts transmissions to meet platform requirements.

√ A standard interface to a shipboard IP router.

√ Interfaces for legacy radios and cryptographic equipment.

"Subnet Relay is the warfighter's version of what the dial-up telephone modem does to a phone line. Radio equipment that was originally designed for different types of communications can, with minimal investment, now be used for text chat, e-mail, Web browsing and other Internet-type applications."

– Canadian Navy Lt. Cmdr. Rob Sibbald
OPNAV N6F422 Allied AUSCANNZUKUS C4 Interoperability Project Officer

lands, are preparing or conducting at-sea trials of the SNR technology. In addition, NATO is moving to adopt SNR as a requirement for maritime networking.

In preparation for SNR becoming a Navy program of record in fiscal year 2008, SNR will be fielded in March 2007 within the Harry S. Truman (HST) Carrier Strike Group as part of a Rapid Technology Transition operational demonstration.

HST will experiment with the SNR capability during Trident Warrior 2007 and will be able to take advantage of this communications enhancement during her next deployment.

Future efforts will involve increasing efficiency and data throughput in addition to investigating how SNR could be used in the joint environment.

SNR is not a replacement for the next generation of high data rate networking radio systems, such as the Joint Tactical Radio System (JTRS). Rather, Subnet Relay provides a transitional technology; repurposing fitted communications equipment to help support the FORCEnet objectives of today and develop the tactical LOS networking concepts and procedures needed to prepare us for the solutions of tomorrow.

As we move forward through the new millennium, innovative multinational development solutions, such as SNR, will help bring affordable connectivity to the Global Maritime Partnership Initiative; enabling enhanced information sharing and interoperability for all coalition members.

Lt. Cmdr. Rob Sibbald is the OPNAV N6F422 Allied AUSCANNZUKUS C4 interoperability project officer.

Lt. Joe Zuliani is the OPNAV N6F421 Allied interoperability officer.

Dr. Stephan Lapic is with the SPAWAR Systems Center San Diego, Network Centric Warfare Analysis Branch.

CHIPS

Priority to Deliver Network Interoperability Solutions Affirmed

By Andrea V. Houck

Speakers at the 11th annual Naval NETWAR FORCEnet Enterprise and Industry Conference unveiled plans to tackle current readiness issues and to provide coalition interoperability capabilities to the joint warfighter.

The conference, held Nov. 14-16, 2006, in San Diego at the Bahia Hotel on Mission Bay, attracted nearly 600 military, government and industry attendees and focused around a wide range of perspectives on "Evolving the Network: Meeting the Warfighter's Critical Information Needs."

"This has been an exciting first year for the Naval NETWAR FORCEnet Enterprise, and we are already beginning see the benefits of this collaborative effort," said Vice Adm. James McArthur, Commander Naval Network Warfare Command (NETWARCOM), who also serves as the NNFE's chief executive officer (CEO).

"While we are still shaping alignment, we are looking at resources, funding technology in the future and how we can meet fleet requirements. We are on the cusp of dramatic changes in C4I [command, control, communications, computers and intelligence] and making huge leaps in capabilities to support the warfighter," McArthur explained.

In an effort to produce and deliver the most effective network capabilities to combatant commanders while efficiently allocating the Navy's resources, the Navy's acquisition organizations that support the air, surface, submarine, expeditionary and network communities have realigned under an enterprise model to increase efficiency, decrease costs and improve speed to capability for the fleet.

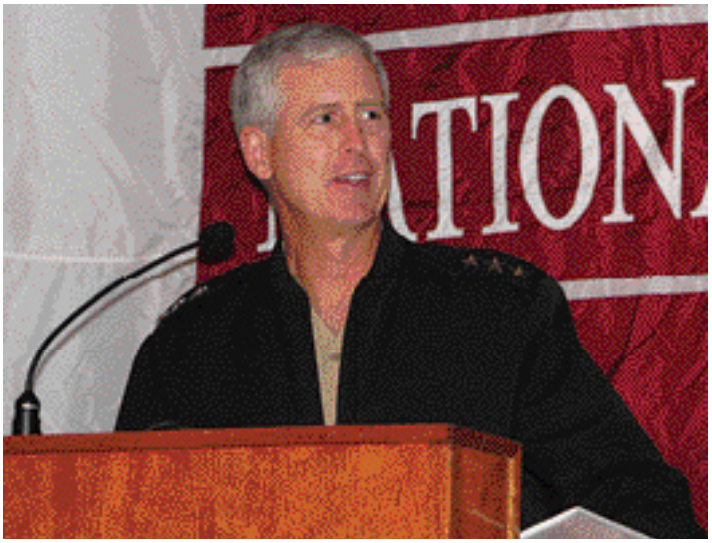
The NNFE is an enterprise approach to implementing FORCEnet and delivering network-centric capabilities to the warfighter. This is a collaborative effort between NETWARCOM, the Office of the Chief of Naval Operations (OPNAV N6), the Space and Naval Warfare Systems Command (SPAWAR) and a host of additional stakeholder organizations, including the Navy's Program Executive Offices (PEO) for C4I, Space Systems and Enterprise Information Systems.

"We are marching down the path to fully support the NNFE," said Rear Adm. Michael Bachmann, Commander SPAWAR. "As the chief operating officer (COO), I am committed to ensuring we effectively deliver FORCEnet capabilities, such as interoperable platforms, to the fleet," he said.

The NNFE's Board of Directors is led by top admirals who meet monthly to assess the enterprise's progress in delivering its products and services. The NETWARCOM Commander is the CEO, the SPAWAR Commander is the COO and OPNAV N6, Vice Adm. Mark Edwards, is the chief financial officer.

By leveraging the power of networks and the information they provide to a wide range of users, the FORCEnet operational construct and architectural framework are expected to improve the fleet's lethality and quicken the pace of decision-making. FORCEnet is the core of Navy and Marine Corps transformation and is the means by which naval forces will make network-centric warfare an operational reality.

For the second consecutive year, NETWARCOM and PEO C4I joined SPAWAR and the San Diego Chapter of the National Defense Industrial Association (NDIA) in sponsorship. The conference served as a major symposium for senior military, government and industry officials to share their perspectives on acquisition strategies and business opportunities for large and small businesses.



Nearly 600 military, industry and civilian employees listened to Vice Adm. James McArthur, Commander NETWARCOM, deliver his address at the Naval NETWAR FORCEnet Enterprise and Industry Conference, held Nov. 14-16, 2006, in San Diego.

"I believe in coalition interoperability, and I am committed to industry to find the solution to provide the systems and products to connect all the fleet together."

– Vice Adm. Barry Costello
Commander Third Fleet

The conference was designed to explore multiple facets of the NNFE. The Assistant Secretary of the Navy for Research, Development and Acquisition chief engineer, Carl Siel, was the keynote speaker who opened the conference by defining the Navy Acquisition Enterprise framework as a behavioral model. Siel said that the model operates within the Navy's command structure to clarify accountability for Navy-wide efficient use of resources and to promote enhanced coordination and collaboration among all stakeholders in mission effectiveness and decision-making.

The discussion progressed into a dialogue on the NNFE's requirements and results, followed by presentations highlighting service initiatives from Marine Corps, Coast Guard and Air Force representatives.

The final day featured perspectives from the acquisition providers — PEOs from C4I, Space Systems and Enterprise Information Systems — and concluded with the "Voice from the Customer" segment. Vice Adm. Barry Costello, Commander Third Fleet, and Vice Adm. Mark Fitzgerald, Commander Second Fleet, discussed their requirements and how network-centric capabilities can assist joint warfighters. (Vice Adm. Evan M. Chanik relieved Vice Adm. Fitzgerald Nov. 28, 2006. Fitzgerald

Vice Adm. Mark Fitzgerald, Commander Second Fleet, discusses the concept of standing up Maritime Headquarters with Mission Operation Centers and how the concept fits into the Chief of Naval Operations' 1,000-ship Navy concept. Vice Adm. Evan M. Chanik relieved Fitzgerald Nov. 28, 2006. Fitzgerald departed 2nd Fleet to become the Director, Navy Staff in the Office of the Chief of Naval Operations.

departed 2nd Fleet to become the Director, Navy Staff in the Office of the Chief of Naval Operations.)

"For the past few years, coalition interoperability has been a top priority and requirement not only for Third Fleet but for all the numbered fleets," said Costello. "I believe in coalition interoperability, and I am committed to industry to find the solution to provide the systems and products to connect all the fleet together."

Other featured speakers included FORCEnet Director, Capt. Richard Simon; Senior Adviser for Command and Control Modeling and Simulation Office of the Chief of Warfighting Integration and Chief Information Officer, Secretary of the Air Force, Keith Seaman; Coast Guard Research and Development Program Manager, Navy Capt. John Macaluso; and other senior military and government officials.

"We have to remember we're a nation at war, and we must be able to adjust to our changing environment in order to have a clearer focus on our mission as premier C4I providers and provide compatible interoperability to the warfighter."

– Acting PEO C4I Chris Miller

As part of the network-centric warfare acquisition portion of the conference, Chris Miller, acting PEO C4I, discussed the organization's realignment to better deliver valuable, cost-effective C4I capabilities without compromising safety or acquisition integrity. He also provided an update on a new contracting strategy called Efficient Contract Requirements and Use (ECRU), which was formerly known as Transition to Industry Primes. ECRU is designed to maintain a competitive landscape in order for industry to focus on engineering efforts and to allow PEO C4I to focus on acquisition and interoperability efforts.

"We have to remember we're a nation at war," said Miller, "and we must be able to adjust to our changing environment in order to have a clearer focus on our mission as premier C4I providers and provide compatible interoperability to the warfighter."

The conference concluded with the presentation of the A. Bryan Lasswell Awards at the sixth annual NDIA Fleet Support Awards Banquet. The event recognized technical and management personnel who made significant contributions to fleet readiness and support.

Fitzgerald was featured as the banquet's keynote speaker, and the evening was highlighted by a poignant moment when Jim Lasswell, former NDIA San Diego Chapter president and son of the award's namesake, spoke of his father's accomplishments in the Marine Corps. This was the inaugural year in which the awards were presented in honor of the senior Lasswell.

"Particularly impressive was the lineup of superb speakers, presenters and panel members that provided two-and-a-half days worth of perspective from the key players of our government, military and civilian sectors," said Dwayne Junker, NDIA San Diego Chapter president.

"It was very encouraging to observe the rapt attention each received during their time on the podium and the spirited question and answer sessions that followed. The result was a significant amount of substantial information provided — and received," Junker said.

Ruth Fox, the NNFE development deputy lead, discusses government - industry partnership at the NNFE and Industry Conference.

Presentations from the conference may be found on the SPAWAR Web site at http://enterprise.spawar.navy.mil/. Additional information on NDIA co-sponsored events can be found at http://ndia-sd.org/.

Andrea V. Houck is with the SPAWAR corporate communications team.

CHIPS

CAN YOU HEAR ME NOW?

ELECTROMAGNETIC SPECTRUM: CRITICAL TO OUR NATION'S SECURITY AND ECONOMY

By the DON CIO Telecom/RF Spectrum/Wireless Team

New innovative technologies to improve wireless efficiency will be needed to ensure America's future security and economic strength ...

Increasingly, our lives, lifestyles, culture and economy depend on wireless devices. Wireless devices enable us to remotely monitor our sleeping children, turn on the television without leaving the couch, make phone calls whenever and wherever, pass through toll booths without stopping, and use our laptops and personal digital assistants virtually anywhere. These devices, and many others in our modern world, work because of the electromagnetic spectrum.

Electromagnetic spectrum — usually referred to as "spectrum" — encompasses radio waves, infrared, visible light, ultraviolet light, x-rays, gamma rays and cosmic rays. Radio waves are an incredibly versatile area of the spectrum and make much of our modern communication possible, including television, AM and FM radio bands and satellite radio broadcasting. While spectrum makes our lives more enjoyable, it is, in fact, critical to our modern quality of life.

Modern health care depends on spectrum to operate medical monitoring systems. Public utilities use spectrum to remotely control pipeline valves that direct the flow of our water, electricity and gas. Transportation systems rely on spectrum for cargo tracking, air traffic control and security sensors.

Firefighters, police and emergency service personnel require spectrum for rapid communication, location positioning and other services. Additionally, spectrum allows manufacturers, shippers and merchants to monitor the location of products using advanced identification technologies, such as radio frequency identification (RFID).

Warfighter Reliance on Spectrum

Our Naval forces are especially reliant on spectrum. Using RFID technology, the Navy and Marine Corps track shipments of critical supplies and confirm patient identity and enter diagnosis and treatment information. In addition to implementing commercial technologies, our Naval forces have unique spectrum requirements. Communications; radar; air and fleet defense; weapons guidance; command and control; and many other systems rely on spectrum to function. In fact, conducting network-centric warfare is impossible without spectrum.

Marine Expeditionary Forces, with integrated aircraft and combat service support, along with Navy SEAL teams, submarines and carrier strike groups are often the first to arrive in theater and must rely on spectrum to remain highly maneuverable, flexible and tactically effective.

An example of complex spectrum demand is found in a typical naval aircraft — voice communications and digital data links require many wireless devices. Weapons systems with associated fire control radar rely on spectrum for guidance to find and destroy their targets. Such demands have both expanded our military's need for, and increased its dependency on, spectrum.

The Challenge

A critical challenge is that spectrum is a finite resource, and it is in great demand. Without careful planning and implementation, spectrum-dependent systems may unintentionally, yet adversely interfere with each other. For example, a test flight at a naval air station was delayed because of interference to an important ground-based test measurement instrument. The source of the interference was a malfunctioning baby monitor in nearby military housing.

Providing balance between spectrum-dependent devices that make our lives more convenient and those that are critical to our national defense is a growing challenge. New technologies to improve wireless efficiency will be needed to maintain a balance between national defense and economic strength.

In the Department of the Navy (DON), we are constantly exploring technologies that allow us to utilize spectrum in innovative ways. Some of these technologies include:

- Frequency agile technologies that can sense a competing device on the same frequency and instantly switch to available spectrum;
- Software defined radios that can set or alter almost any characteristic of a device, including frequency ranges and power and modulation, simply by loading new software;
- Ultra-wide band devices that can "see through walls" to detect combat threats without entering a building.

In addition to implementing new technology, we must all collaborate in the efficient use of current assets to guarantee dependable spectrum access for everyone.

Coordination of Spectrum Use

The complexity of spectrum coordination is enormous, and it is a global challenge because the DON deploys Marine Corps forces and Navy assets worldwide. Careful and constant coordination is required to guarantee that the Department meets it mission.

Through international negotiations, the DON ensures that

Marine Expeditionary Forces, with integrated aircraft and combat service support, along with Navy SEAL teams, submarines and battle groups are often the first to arrive in theater and must rely on spectrum to remain highly maneuverable, flexible and tactically effective.

the spectrum-dependent capabilities of the Navy and Marine Corps are preserved. Because the radio frequency spectrum must be shared among nations, a United Nations agency, the International Telecommunication Union, convenes the World Radiocommunication Conference to modify spectrum allocation as technology and services require.

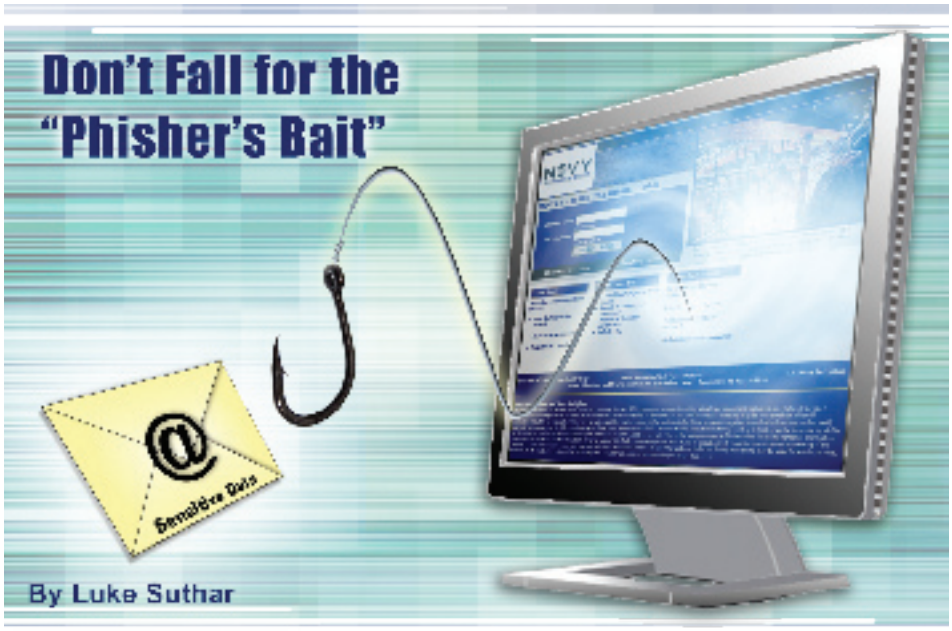
All members of the United Nations are invited to these conferences and the Department of the Navy Chief Information Officer participates as the Department's national and international representative to these forums.

To achieve its goals, the DON strives to improve efficient use of spectrum through collaborative efforts among business, industry, government and other nations.

In order to maintain America's advantage and secure our country's future, we must continue to work to meet our growing national spectrum challenges because electromagnetic spectrum is critical to both our nation's security and economy.

For more information, please contact the DON Spectrum Team at DONSpectrumTeam@navy.mil. CHIPS

Can You Hear Me Now is a regularly featured column in CHIPS magazine. Please go to the CHIPS Web site at http://www.chips.navy.mil/ and click on the Archives link at the top of the page to view past columns.



Department of the Navy (DON) networks are under continuous attack by an invasion of "spam on steroids." There has been a significant and widespread trend of using bogus e-mails to steal personal information and access critical DON information systems.

The ultimate objective of these Internet intruders is to trick unsuspecting users to open an attachment or click a Web link that will download specialized malicious software onto the computer. This process circumvents existing security measures and allows access to DON data.

The Naval Criminal Investigative Service (NCIS) has observed a growing trend of thousands of malicious e-mails targeting Sailors, Marines, Navy civilian workers and DON contractors, with the potential to compromise a significant number of computers across the Department.

Web Tricks

"Phishing" is a criminal activity in which an adversary attempts to fraudulently acquire sensitive information by impersonating a trustworthy person or organization using, for example, manipulated e-mails that appear to represent the DON, Navy Federal Credit Union, Navy Knowledge Online (NKO) or other familiar institutions.

The ultimate goal of a phishing attempt is to extract information through the contact in order to evade existing security measures and allow access to DON secure information and data. Phishing is typically carried out using two techniques: "spoofing" and "social engineering."

Spoofing an e-mail creates a fraudulent message with an e-mail address and page content that appear to be from a valid source. Often the e-mails contain malicious attachments and links to deceptive Web sites that appear to be an exact duplicate of the authentic Web sites.

Social engineering involves multiple correspondences to potential victims in order to get them to divulge critical and confidential information through trickery. Correspondence includes, but is not limited to, the use of e-mails, telephone calls and personal contact.

Victims are manipulated or tricked into providing personally identifiable information, such as credit card numbers, bank information, Social Security numbers, user IDs and passwords — and possible critical information that could harm the DON network that would not be otherwise easily disclosed.

When spoofing and social engineering are concatenated, the outcome is a new technique, known as "spear phishing" — a mass of manipulative e-mails to unsuspecting recipients who believe the message is authentic and from a trusted sender.

When using spear phishing, offenders adapt to security measures that would otherwise block a majority of these menacing e-mails. This type of attack uses targeted e-mails that are manipulated to

specifically fit the potential victims, providing them with a false sense of trust.

Spear phishing is similar to phishing; however, the audience is a targeted group of individuals. The sophistication of this technique is reflected in the attacker's ability to obtain legitimate DON documents, use enticing subject lines relating to genuine operations, exercises or military topics, and exploit the trust of users across the Department.

The following are the steps attackers use to complete a spear-phishing scheme:

(1) The attacker obtains e-mail addresses for the intended victims and generates an e-mail that appears genuine and which requests the recipients to perform a certain task or action.

(2) The attacker sends the e-mail to the intended victims in a way that appears legitimate and obscures the true source.

(3) Depending on the content of the e-mail, the recipients open a malicious attachment, complete a form or visit a deceptive Web site.

(4) The attacker collects the victim's sensitive information for future exploitation.

Tips for Prevention

Be aware that providing personal information to an unverified source may lead to information compromise, identity theft and a great deal of stress. By taking the following few simple precautions you can help avoid this costly mistake:

Digital Signatures – The DON CIO issued naval message 061525Z of October 2004, Public Key Infrastructure (PKI) Implementation Guidance, which required DON network users to digitally sign any e-mail requiring message integrity and non-repudiation. Any message that tasks or requests a DON user to provide personal or otherwise sensitive information should be digitally signed. (Go to http://www.doncio.navy.mil and type 061525Z in the Search block to download a copy of the guidance.)

If a digital signature is not present and the sender is unknown, recipients should verify the authenticity through other methods, such as a phone call to verify and request a digital signature.

If the sender's identity still cannot be verified, the message should not be opened and the incident should be reported to the user's information assurance (IA) manager and/or the NMCI help desk immediately by phoning 1-866-THE-NMCI (1-866-843-6624).

User Education – Users should not answer any e-mail that attempts to collect personal identifiers and other critical information unless the e-mail has been verified to be authentic.

Opening e-mail attachments or clicking on hyperlinks from unknown or unexpected sources, including but not limited to e-mail from dot-mil and dot-gov sources, could cause a system malfunction, slow computer performance and ultimately disrupt network service.

Mandatory Training – To combat the growing threat of spear-phishing, the Navy Cyber Defense Operations Command issued Task Order 06-17 (INFOCON 4), which makes "DoD Spear-Phishing Awareness" training mandatory for all military, civilian and contractor employees of the Defense Department.

This training is available on the Joint Task Force Global Network Operations (JTF-GNO) Web site at: https://www.jtfgno.mil/. You will need to use your Common Access Card to log in.

Some commands are offering in house training. Employees should check with their command IA manager or security manager for guidance.

Information assurance training offered on NKO provides additional details and preventive tips. To access the IA training, go to http://www.nko.navy.mil. If you are not a registered user, you must register first, then select the following options:

- Launch Navy E-Learning
- Browse Categories
- U.S. Department of the Navy (DON)
- Information Assurance (IA)
- Select DoD Information Assurance Awareness

User Reporting – NMCI users are encouraged to perform one of the two following directions upon receipt of spam or unwanted e-mail:

1. Highlight the spam e-mail in your Inbox, but do no open it.
2. Go to Edit > Copy.
3. Paste the entire e-mail into a new message, and ensure the word SPAM is in the subject line.
4. Forward it to GNOC_GL-IAM. The message will be forwarded to spam filter managers for action.

Laukik "Luke" Suthar is an NCIS special agent supporting the DON CIO.

CHIPS

The Joint Task Force Global Network Operations (JTF-GNO) offers DoD Spear-Phishing Awareness training at: https://www.jtfgno.mil/.

You will need to use your Common Access Card to log in.

Tips from the JTF GNO presentation of the DoD Spear-Phishing Awareness Training

Discovered "spear-phishing" messages within the DoD can be very convincing.

How to recognize a spear-phishing attempt

-"From" field of an e-mail can be easily faked (spoofed). It might appear completely correct, or have a similar variation. For example: account_security@mypay.com

-On the other hand, the message may come from a legitimate e-mail account, because that account has been compromised. For example: john.smith.yourboss@yourbase.mil. This can occur when the attackers obtain someone's login credentials and e-mail contacts.

How can I be sure?
Is the message digitally signed?

Other recognition factors of phishing attempts:
1) Generic Greeting
2) Fake Sender's Address
3) False Sense of Urgency
4) Fake Web Links. Deceptive Web Links.
E-mail requires that you follow a link to sign up for a great deal, or to log in and verify your account status, or encourages you to view/read an attachment.
5) E-mails that appear like a Web site
6) Misspellings and Bad Grammar

Be cognizant of this threat. Before clicking on any Web link within a message or opening up an attachment, be sure the source of the e-mail is legitimate! The importance of digitally signing your messages can't be stressed enough.

Joint Integration and Interoperability of Special Operations

SPAWAR supporting the GWOT and Warfighter

By Capt. James P. Idle and Capt. Kay Hire

The Joint Integration and Interoperability of Special Operations (JIISO) was chartered to employ multiservice and other Defense Department support, personnel and equipment to investigate, evaluate and make recommendations to improve the operational effectiveness of the joint integration and interoperability of both Special Operations Forces and conventional forces.

The mission of JIISO is to increase the integration and interoperability of Special Operations and conventional forces for the joint force commander during the planning and execution of maneuver and fire support coordination during tactical operations.

The goal is to generate more timely actions and increase opportunities for the warfighter with less potential for fratricide.

The Space and Naval Warfare Systems Command (SPAWAR) escorted the JIISO Special Operations and conventional forces Mobile Training Team aboard the USS Ohio (SSGN 726). USS Ohio is the first of the new transformational capabilities submarines for the joint force warfighter in the global war on terror. It is the first of four fleet ballistic missile submarines (SSBNs) to be converted into SSGNs, or guided-missile submarines.

The Navy is engaged in the conversion of three additional SSBNs into SSGNs. One of the key capabilities that will involve SPAWAR is in the SSGN's role as the JFMCC, or Joint Force Maritime Component Commander, and in connectivity to the Global Information Grid through FORCEnet because Special Operations Forces capabilities will include joint forces as well as Navy SEALs.

The JIISO will participate in upcoming cruises on Ohio and USS Florida (SSGN 728) to test and evaluate Special Operations and conventional forces integration and interoperability in Tomahawk Land Attack Missiles deconfliction and the Naval Fires Network, to name a few.

In February 2004, the Department of Defense Joint Test and Evaluation (JT&E) Senior Advisory Council recommended that the JIISO and JT&E be chartered by the Deputy Director Air Warfare, who reports to the Director, Operational Test and Evaluation within the Office of the Secretary of Defense.

The U.S. Special Operations Command (USSOCOM), the U.S. Marine Corps and U.S. Joint Forces Command (USJFCOM) are the JT&E co-sponsors.

The JIISO JT&E focused on evaluating the military decision-making process, the Marine Corps planning process and the supporting system of systems methodology used by both Special Operations and conventional forces to synchronize combat operations.

Prior to Operation Enduring Freedom, Special Operations Forces generally operated autonomously, removed operationally, logistically and geographically from most conventional forces. As a consequence, Special Operations Forces relied largely on their own firepower. Special Operations and conventional forces were normally deconflicted through time and space separation rather than through a concerted effort to integrate operations.

The need for institutionalized integration and interoperability of Special Operations and conventional forces grew out of Operations Enduring Freedom and Iraqi Freedom. The introduction of large conventional forces into those theaters of operation, already occupied by sizable Special Operations Forces, presented new problems and, on several occasions, resulted in delayed actions and the potential for fratricide.

Without written doctrine, the degree of successful integration was attributable to the professionalism of the leadership, personal relationships developed in the battlespace and ad hoc solutions developed by the Soldiers on the ground. To become truly integrated, written codified procedures needed to be developed and incorporated into training, education and doctrine. Addressing this problem, the JIISO developed test issues for two field tests.

The test issues for field test 1 established a baseline and concentrated on the military decision-making process and the Marine Corps planning process and execution steps for both. It also established a system of systems support baseline for the integration of forces including command, control and communication systems and collaboration applications.

Field test 2 examined how recommendations for enhancements, like using checklists and a system of systems methodology, improved the integration and interoperability of conventional and Special Operations Forces. Today, revisions to joint publications are addressing these issues.

Research and testing, also revealed the system of systems supporting Special Operations and conventional forces integration and interoperability are frequently not interoperable.

The SPAWAR JIISO Mobile Training Team aboard the USS Ohio (SSGN 726), left to right: Army Master Sgt. Reuben De Leone, Army Lt. Col. Walton, Richard Bernier, Army Maj. Shannon Hume, Navy Capt. James Idle with ship's company: FTC Edward Quinlan, Lt. Jake Forett and MM2 Mike Garcia.

Nov. 9, 2006 – SPAWAR has assisted in the integration of JIISO products to global forces as seen here in Stuttgart, Germany. Capt. Kay Hire, then JIISO program manager, discusses JIISO products with Navy Cmdr. Greg Stephens, left, and Air Force Maj. Kevin Wesley, both from U.S. European Command International Interoperability, Concepts and Experimentation (ECJ9). Department of Defense photo by Air Force Tech. Sgt. Devin L. Fisher.

To address these issues, the JIISO produced an integration and interoperability handbook, a Situational Awareness Systems Guide, computer-based training applications and also developed and tested Special Operations and conventional forces integration and interoperability checklists based on analytical processes.

JIISO handbooks and systems guides contain tactics, techniques and procedures to improve the effectiveness of integrated conventional and Special Operations Forces, and streamline interoperability between U.S. combatant commands and global war on terrorism partners.

The checklists and associated handbook have been well received by units preparing for deployment and currently serving in Operation Iraqi Freedom. The Army has also adopted JIISO products for inclusion in its professional development courses.

A digital copy of the handbook has been posted on Army, Navy, Marine, Special Operations Forces and USJFCOM Web sites and is available on the SIPRNET at http://jiiso.jte.osd.smil.mil.

The success the JIISO had in reducing fratricide potential, promoting more timely actions and fewer missed opportunities for the warfighter, led to its nomination as the integration and interoperability branch within U.S. Special Operations Command. As a result, effective Dec. 1, 2006, the JIISO JT&E team was incorporated into the USSOCOM Special Operations Knowledge and Futures Directorate J7.

As the host combatant commander for the Coalition Warrior Interoperability Demonstration scheduled for June 2007, U.S. European Command will incorporate JIISO products into CWID 2007. CWID will be conducted at Kelley Barracks in Stuttgart, Germany, and at multiple sites across the United States.

The SPAWAR JIISO team will continue to provide support.

Capt. James P. Idle is the SPAWAR program manager for the JIISO team. Capt. Kay Hire is the former SPAWAR program manager for the JIISO team. CHIPS

Department of the Navy INFO Alert

Dec. 1, 2006

New DON CIO Selected to Replace Dave Wennergren

The Secretary of the Navy, Donald C. Winter, has selected Mr. Robert J. Carey to serve as the Department of the Navy Chief Information Officer (DON CIO). Mr. Carey will replace Mr. David M. Wennergren, who has taken a position as deputy assistant Secretary of Defense for information management and technology and Department of Defense deputy CIO.

Mr. Carey joined DON CIO in 2000, and in December 2002 was promoted to DON deputy CIO for policy and integration. As deputy CIO, he served as the principal adviser to the CIO and was responsible for managing and leading the DON CIO staff and developing strategies for achieving information management (IM) and information technology (IT) enterprise integration across the Department of the Navy. He has been a driving force for change, championing several successful initiatives including the creation of a single common access card for the Department of Defense. At the present time, Mr. Carey is on active duty deployed in Iraq.

Mr. Carey's appointment was based on his years of leadership and management experience throughout the DoD engineering, acquisition and IM/IT communities, coupled with his superb team building and interpersonal skills, and persistence in building strong ties among the Secretariat, the fleet and resource sponsors.

Mr. John J. Lussier, who was serving as acting DON deputy CIO in Mr. Carey's absence, will serve as acting DON CIO until Mr. Carey's return in early 2007.

Mr. Lussier was the director of operations with responsibility for all personnel, budgetary, financial and contractual management for the DON CIO. Additionally, he was dual-hatted as the telecommunications, spectrum and wireless team leader, responsible for policy formulation and strategic planning for Department-wide telecommunications, spectrum and wireless initiatives.

For more information about the work of the DON CIO, go to the DON CIO Web site at http://www.doncio.navy.mil. CHIPS

Innovation Delivered to the Warfighter by the OX

By Tom Gwiazdowski and Sandy Mieczkowski

In one arena is the warfighting community: combatant commanders, joint task forces, strike groups, squadrons, battalions and Special Forces detachments. In another — is a group of highly qualified professionals who are working on warfighting initiatives and projects for sponsors.

The Space and Naval Warfare Systems Center (SSC) Charleston Office of eXperimentation (OX) onboard Naval Amphibious Base Little Creek, Norfolk, Va., is working to bridge the gap between these two groups. Chief of Experimentation for SSC Charleston Mr. Tom Gwiazdowski and Ms. Sandy Mieczkowski comprise the workforce of the Office of eXperimentation.

The OX takes direction from SSC Charleston chief engineer Phil Charles and formally reports to the Senior Engineering Group and Science and Technology Group quarterly. The OX mission is to assist SSC Charleston in taking its newly developed technologies and engineering solutions into joint, interagency and multinational experiments for warfighter validation and feedback.

"Once we started briefing some of the key leadership in SSC Charleston, they validated that what we were proposing had significant value to both SSC Charleston and the warfighters," Gwiazdowski said.

"The whole idea is to expose what our talented engineers are working on to the warfighters to gain valuable warfighter feedback as the engineers continue to develop and refine their initiatives. The dialogue works both ways — we show the warfighters what we're working on for them — and they give us feedback to determine the true utility and how it may be improved upon."

Initial discussions were followed by conducting a Lean Six Sigma value stream mapping event with assistance from SSC Charleston Black Belt Mr. Dale Davis to identify the processes and organizations that would be involved in this undertaking.

"The Lean Six Sigma event was an important milestone in taking our thoughts and formalizing them into an effective, efficient and streamlined process. This is still a new undertaking, and we are continuously updating and adding to our process as we go along," Mieczkowski said.

Tom Gwiazdowski and Sandy Mieczkowski conducting a briefing onboard Norfolk Naval Station December 2006.

There are a number of ongoing initiatives within SSC Charleston that support a wide variety of sponsors. While these initiatives fulfill sponsor requirements, there appears to be limited opportunity for exposing these initiatives to warfighters for feedback while the initiatives are under development.

Some projects may also have a deliberately narrow focus in fulfilling sponsor requirements. A number of these projects were found to have a wider application in the larger context of joint and multinational warfighting than their sponsors originally intended or envisioned.

For example, a project designed to assist in personnel identification for ship boarding parties could have tremendous value to Special Forces detachments, infantry rifle squads or any military force that requires identification technologies in combat situations.

Gwiazdowski and Mieczkowski intend to bring initiatives like these to the greater joint and multinational warfighting communities for consideration.

Innovation and creativity are the catalysts behind the OX's approach. Research, exploration, invention and originality are values central to SSC Charleston and its engineering and business development.

New discoveries, new directions and new attitudes challenge personnel and enable SSC Charleston to grow as a business entity and world class engineering organization. Without continuous innovation, engineering and business capabilities stagnate, and the tremendous creative capital possessed by the organization can wither away.

To inspire the workforce to even greater ingenuity, SSC Charleston senior leadership established an Innovation Program in fiscal year 2006. Thirteen proposals received funding, and it is anticipated that $1–$1.5 million will be available for investment in the Innovation Program in fiscal year 2007.

Gwiazdowski and Mieczkowski intend to match the project results of the Innovation Program with existing warfighter requirements so warfighters can provide immediate feedback to the developers.

U.S. Joint Forces Command has ultimate responsibility for transformation and experimentation for the entire Defense Department and NATO, the largest and longest standing multinational alliance. Gwiazdowski and Mieczkowski plan to partner with USJFCOM to bring new capabilities to the warfighter community for assessment.

"Joint Forces Command Innovation and Experimentation Directorate (J9) continues to be a great organization to partner with on many of our efforts," Gwiazdowski said. "They are a professional, focused and dedicated group of individuals who are doing a superb job helping the warfighters.

"We recently briefed Ms. Monica Shephard from JFCOM J9 and her support was very encouraging. She provided some great advice on how to proceed. We look forward to working with them

"We will look at what high priority warfighter requirements are out there and look for matches with what SPAWAR Systems Center Charleston is working on. We've just started to scratch the surface here but already have a few quick wins."

- Tom Gwiazdowski

on as many of their experimental efforts as our initiatives can enter."

While some project managers may be reluctant to expose developing technologies to experimentation and feedback, Gwiazdowski thinks that early experimentation and warfighter valuation are essential.

"I'd rather get news in the first 12 months of my work that can help focus my efforts than in the last 12 months — or even worse — when the final capability is delivered to the warfighter."

Inserting the initiative into the proper environment at the right time is critical to the process. The OX will capitalize on the service, joint, interagency and multinational transformation and experimentation efforts in Tidewater Virginia.

The OX will perform an initial analysis and determine the experimentation venue or exercise that would provide the best focus and scenario for warfighter feedback and military utility assessment.

For example, an initiative may have greater utility in a joint and multinational environment with involvement of other U.S. government agencies as well as humanitarian and nongovernmental organizations. If so, the OX will work to have the initiative inserted into an experiment, such as the multinational experimentation series conducted by J9. If an initiative has a multinational maritime focus, the OX will find an exercise that focuses on multinational maritime warfighting.

Initiatives can also be entered into the NATO Concept Development and Experimentation program, a collaborative effort among the NATO and Partnership for Peace nations, to share information and experiment results within the alliance.

"We will look at what high priority warfighter requirements are out there and look for matches with what SPAWAR Systems Center Charleston is working on. We've just started to scratch the surface here but already have a few quick wins, Gwiazdowski said.

"We're starting to look at Advanced Concept Technology Demonstrations (ACTDs) and Joint Capability Technology Demonstrations (JCTDs), review them and determine if there are matches between those warfighter requirements and the ongoing efforts of SPAWAR Systems Center Charleston."

The OX is set to have initial operational capability in the second quarter of fiscal year 2007 with full operational capability slated for the first quarter of fiscal year 2008. But the OX has already had some successes. Gwiazdowski and Mieczkowski recently matched an SSC Charleston project with a new Joint Capability Technology Demonstration which will potentially fulfill half of the JCTD objectives much earlier in the process than originally thought possible.

They also submitted several SSC Charleston projects into USJFCOM's Multinational Experiment 5 as well as Combined Endeavor 2007, a multinational security and communications exercise sponsored by U.S. European Command and NATO. Finally, they have taken a few real gems and shown them to a couple of combatant commanders who expressed a very strong interest in them.

Linking projects directly to warfighting requirements will result in a huge payoff for the warfighter — and that is really what it's all about.

Tom Gwiazdowski is the chief of experimentation and holds the technical warrant for experimentation for SSC Charleston. He is a retired U.S. Army officer with extensive experience in operational infantry units as well as joint and multinational commands. He was one of the founding fathers of the NATO Concept Development and Experimentation program and has served as an operational manager for an ACTD.

Sandy Mieczkowski works in the Office of eXperimentation. She was previously the manager of the SSC Charleston Tidewater Node of the FORCEnet Composeable Environment (FnCE) and one of its original architects. She has supported Naval Network Warfare Command and its Sea Trial events including Trident Warrior and the Navy's participation in Joint Expeditionary Force Experiment in the FnCE Node. CHIPS

Department of the Navy Information Technology Umbrella Program Update

The Department of the Navy (DON) Information Management and Information Technology Conference is a great opportunity to meet representatives from the DON IT Umbrella Program of contracts and other acquisition professionals across the DON and Department of Defense.

The IM and IT Conference to be held January 30 through February 2 at the San Diego Convention Center, is hosted by the DON Chief Information Officer (CIO) and features knowledgeable speakers from a wide variety of topics, including commercial software acquisition and services through the DON IT Umbrella Program, DoD Enterprise Software Initiative (ESI) and SmartBUY.

Mr. Jim Clausen, from the Office of the Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer, the ESI chair; Mr. Floyd Groce, DON representative and ESI co-chair; and Mr. Tom Kireilis, from the General Services Administration, will conduct a session regarding the SmartBUY program and enterprise licensing for commercial software, Wednesday, January 31 at 11:10 a.m.

Ms. Linda Greenwade, DON IT Umbrella Program manager, will conduct a DON IT Umbrella Program update, Thursday, February 1 at 10:45 a.m.

The DON IM and IT Conference is open to all DON government, military and support contractor attendees. No conference fee will be assessed, but registration is required.

The agenda and registration are available on the DON CIO Web site at http://www.doncio.navy.mil.

For additional information call (703) 607-3435 or (703) 602-6274.

Please join us!

Interview with Joe Camacho

Joint Knowledge Development and Distribution Capability Program Manager

U.S. Joint Forces Command Joint Training Directorate and Joint Warfighting Center (J7/JWFC) lead joint warfighter capability improvement through joint training. With emphasis on the global war on terrorism and military transformation, the JWFC works to ensure America's military is the most advanced and powerful force in the world.

The JWFC commander serves as the joint force trainer to ensure the fidelity and coordination of the military's overall joint training efforts. From the JWFC facility in Suffolk, Va., the joint force trainer team and its partners revise the content and execution of training, developing advanced technologies and reshaping the overall training environment to better prepare combatant command staffs, joint task forces and the individual services (Army, Navy, Air Force, Marines and Coast Guard) to fight as a collaborative team, or a joint force. This transformation in training is a critical success factor for not only U.S. forces, but also for our multinational partners in NATO and Partnership for Peace programs.

CHIPS asked Mr. Joe Camacho, program manager for the Joint Knowledge Development and Distribution Capability to discuss how his program prepares warfighters for the many and varied missions that the U.S. military performs today. CHIPS spoke with Mr. Camacho in November 2006.

Mr. Camacho: Our training transformation program in the Department of Defense (DoD) is a new one for JFCOM, and I do appreciate you affording us the opportunity to get our message out and make other people aware of this important program.

The training transformation program has three distinct legs of the stool. Training transformation consists of a collective training piece which is called the Joint National Training Capability. That is the JNTC live, virtual and constructive technologies that afford collective training and joint training across the entire department. The director is Capt. David Frost and the program manager is Mr. Greg Knapp. It is run out of the Joint Forces Command and the Joint Warfighting Center.

The second leg of training transformation is my program, the Joint Knowledge Development and Distribution Capability, JKDDC. JKDDC is individual Web-based training. It is integrated with the Joint National Training Capability because individuals must prepare before going into a collective exercise in order to perform as a group.

The JNTC and the JKDDC are integrated, and we leverage each other's capabilities and technologies, but they are two separate programs.

The third program is the Joint Assessment and Enabling Capability (JAEC), run by the Under Secretary of Defense for Personnel and Readiness and the Joint Staff. Their job is to assess the effectiveness of the JNTC and JKDDC on the joint community.

CHIPS: How do you determine which form of training you are going to use — live, virtual or constructive?

Mr. Camacho: We determine which form of training to use for military and civilians for joint exercises. Nowadays, joint is defined as interagency, intergovernmental, multinational and, of course, across the services. There are several tools that can be used to prepare the audience to engage in the training exercise directly. Modeling and simulation, live forces and constructive simulations can be used.

The Joint National Training Capability uses a balance of those pieces to afford the best and most efficient training in the exercises that they sponsor. The new factor that we bring forward is the JKDDC factor, Web-based individual training in preparation for the exercise that also allows reachback during the exercise.

For example, if you are a participant, three months prior to the exercise, you could get on our Web site, our knowledge portal to prepare you for what your job, and roles and responsibilities will be in the exercise. You could receive training on the special skills you might need. You would have access to research, training courses and content, and chat rooms with other people that may have been in a similar exercise and have real-world experience. You could reach back into other places on the Web to properly prepare you.

Reachback is an important piece. If you can take that concept, move it forward to real-world operations, you could see where the real value is to the operator in the field during integrated operations.

Anybody from anyplace at anytime can get access to the knowledge portals which are based on the Internet — the unclassified NIPRNET and the classified SIPRNET. They can get access in real-time when they are deployed in Afghanistan or Iraq or other parts of the world. It is an important capability that we are working on.

CHIPS: Do you have to be part of a specific program or exercise to use the knowledge portal?

Mr. Camacho: If you are part of the DoD enclave, for example if you are a civilian with a CAC, Common Access Card, or if you are a military person, or anybody else that has been given special permission to enter these enclaves, it is continuously available to you 24 hours a day, seven days a week, 365 days a year.

That is what is key. It is the anytime, anywhere concept, the ability to take advantage of this joint knowledge that is available to you when you need it — not when we are ready to give it to you. That is a totally different approach, a transformational approach to providing value to the warfighter.

CHIPS: Can you provide a profile of your typical user?

Mr. Camacho: Members of a combatant commander's staff; members of a joint task force staff; individual augmentees that are being deployed around the globe; functional component staffs that the services have; joint and service school students; individual service members; interagency and intergovernmental people; multinational partners; combat support agencies; the National Guard Bureau; Reserves; industry; academia; government contractors; and anybody else inside the DoD enclave can be given access to one of our three knowledge portals to receive this training and information.

CHIPS: How many people are using the system at any one time?

Mr. Camacho: We have just inherited the program. We transitioned it from the Joint Staff over the last year, and we have just gotten our plan approved for execution in October. We have just begun to build the new system. Everything I have been talking about is part of our execution plan, approved and funded for fiscal year 2007. We are busily building the Web sites and the knowledge portals and getting the servers in place.

The program that we inherited has about 77 training courses available on the Web site, and we do not have a way to track users currently. All the things I have been talking about are in our implementation plan for execution in fiscal year 2007.

CHIPS: You specified that the portal is Web-based. Can you talk about the technology behind it?

Mr. Camacho: Initially, Web-based training courses were provided through advanced distributed learning. These courses were static where a user could read an electronic version of a book with some interaction.

Now the technology is advanced beyond that. We have interactive advanced distributed courseware that engages directly with the user. The user can ask questions. The user can stop in the middle of the course and come back the next day and pick up where he or she left off.

There are self-administered tests to determine if the user has achieved the training objectives. There is other content available in knowledge portal services. People may not want to take a training course. They may just want access to certain information or read articles. They may want to engage in a chat room, or in a Web-based or desktop video teleconference with some other subject matter experts.

All of these technologies are going to be available through the knowledge portal through the JKDDC program. It is a more sophisticated way for users to get the information they need, but to the user — it is seamless, transparent and convenient.

CHIPS: You mentioned the flexibility of the system. How quickly can you make a change if there is a new policy directive?

Mr. Camacho: Depends what the product is. For example, if you want to make a training course on a hot topic, we could generate one of those as quickly as six weeks, maybe even four, depending on the format and the subject matter expert's availability.

In the last 18 months trafficking in human beings became a secretary level interest item, and the secretary wanted everyone to receive awareness training of what was happening across the globe. Advanced distributed learning courses were developed and made available on the Web across the globe to DoD personnel in probably a two-month time period, an impressive achievement considering all the people that have been trained by that particular Web-based training module.

CHIPS: How do you work with your stakeholders — the unified commands, OSD and the other partners in your program?

Mr. Camacho: We operate the JKDDC program. JFCOM is the implementing agent for DoD. We engage in the T2 Business Model — the Training Transformation Business Model. It is a process by which we bring together all of the stakeholders, including the combatant commanders and their representatives (typically at the 06 level), the combat support agencies, the services, and other organizations that are on the perimeter.

With me as the facilitator, the stakeholders make recommendations to the T2 governance structure which includes higher-level representatives in a larger forum, the integrated process team and then to the senior advisory group at the two and three-star level and ultimately to the Executive Steering Group, which is at the four-star level. We use an open and collaborative environment in the JKDDC and JNTC, and that is why the programs have been so successful.

It is open, it is transparent, and it is accountable —meaning that we let everybody know what is going on. They are involved in the development of the overall plan which includes the budget.

If there are any changes, we call all the stakeholders back together, and we all make these changes together. It is a consensus model, not everybody gets their way, but everybody is involved in the decision-making process.

CHIPS: In reading about JFCOMS's mandate to be the joint trainer, transformational seemed to be the buzzword. How do you instill that value into your training?

Mr. Camacho: We must transform in the Department of Defense. There is no way that we can use the old mechanism of folks sitting in a classroom with an instructor. For example, if you take the typical training institutions where they train 50 to 100 students every four or five months on a certain topic, that is not nearly enough throughput to cover the Afghanistan, Iraqi and Kosovo type situations that require our military forces to be engaged in immediate, integrated operations.

The way we transform is to provide the maximum amount of appropriate training via the Web. This way you can get anywhere from 10 to 10,000 hits a day on a Web site through a knowledge portal that will provide training to folks whenever and wherever they need it — at their desk, on the job or in the field.

Forces now do not have the time to travel somewhere and sit in a classroom for six weeks. They have to be on the job because of the OPTEMPO (operations tempo) and PERSTEMPO (personnel tempo) that is required to fulfill global requirements.

Training is transformational by definition because we do not do it the old institutionalized way.

That is not to say that the venerated brick and mortar institutions have no value. There are some things that do not lend themselves to Web-based training. We call it 'blended' learning. The balance that we have between the brick and mortar institutions and the Web-based folks (such as myself) has to be determined again in this T2 Business Model where the stakeholders get together and make that determination.

CHIPS: Technology is wonderful, but sometimes you just want to talk to a human being. How easy is it for somebody using your system to talk to a subject matter expert?

Mr. Camacho: Because of the knowledge portal technology, we have a menu of various ways that the user can get information. For example, you can enter the knowledge portal and say I want a specific piece of information. The system will query you if you

Joint Force Trainer Community

USJFCOM's Joint Force Trainer community has a global responsibility for training in support of joint warfighter development. The command works with a broad range of stakeholders including:

- The Office of Secretary of Defense
- The Joint Staff
- The services and unified commands
- Interagency and multinational partners

A key to success is its continued effort to build an interdependent and collaborative atmosphere for broadening and deepening joint context and continuing to ensure joint training is the integrating environment for transformation.

Transforming Training

The Joint National Training Capability (JNTC) serves as the heart of training transformation. This enhanced training capability is one of three focal points in the Secretary of Defense's Training Transformation Plan. It covers the full spectrum of warfighter decision-making — from the strategic and operational — to tactical levels of war.

want to take a course, if you want to read articles, if you would like to see lessons learned, if you would like to see a list of subject matter experts and their contact information — when they are available, where to call or their e-mail addresses. Or a user can enter a chat room and find out who is up.

The portal offers the entire spectrum of choices because we understand that what you have said is right. For example, senior people, historically, like to talk to other senior people. A flag officer in the field that wants to talk about stability reconstruction may want to talk to his old professor at the National Defense University, or a flag officer who retired a few years ago, or a flag officer doing the same thing in another part of the world. Through our JKDDC portal, we have ways to make those connections available to the user. That is in our plan for fiscal year 2007.

We also understand that the younger generation likes to get into blogs, Web sites where everybody is talking to everybody else. This is the way they learn best. They like to play games, and we are offering games as a learning venue.

We are offering the total spectrum, the total menu of different ways that the user can get the information and the knowledge that they need to do their jobs even if it is just to talk to someone else.

CHIPS: Your portal sounds like decision-support technology.

Mr. Camacho: That is one of its key dimensions. It can be used for decision support. It can be used for performance enhancement or mentoring. It can be used for information gathering and lessons learned. It can be used for whatever the user decides he or she needs. It was designed that way.

This is an important program, not for the technology, that clearly is the enabling piece, but at the end of the day it is all about giving the warfighters what they need.

We are operators in JFCOM, and we have operationalized this concept with our plans. Hopefully, in fiscal year 2007, we will be able to deliver to the warfighter a technology-enabled system that will give them what they need to do their jobs better. That is our mission. CHIPS

USJFCOM's New Supercomputer

By Robert Pursell, USJFCOM Public Affairs

The High Performance Computing Modernization Program (HPCMP) recently assigned a supercomputer to U.S. Joint Forces Command (USJFCOM) that will enhance experimentation and training efforts in modeling and simulation.

The supercomputer is much larger and more powerful than the machines used today and will yield finer details when it comes to imaging and behavior at a faster speed.

The supercomputer will be operated mostly by the Joint Training Directorate (J7) and Joint Experimentation Directorate (J9), housed in the Joint Training and Experimentation Center and accessed through the Defense Research and Engineering Network (DREN).

The DREN is an official Department of Defense network specifically designed for computational research, engineering and testing, and is used to transfer leading network and security technologies and capabilities across the DoD and other federal agencies.

Jim Blank, USJFCOM J9 modeling and simulation division chief, explained the command's plan for using the machine.

"There's been a shift in focus, as you can imagine, from rolling deserts and plains to an urban environment," he said. "You can't model an urban environment without modeling the people. That is the most important part of the city."

Tony Cerri, J9's experimentation engineering department head, gave an example of how the supercomputer will affect a simulation of Baghdad.

"In a city like Baghdad, we can say this would be morning rush hour, all of the sudden 500,000 people get up and go to work. That's not something that we've been able to do very well," Cerri said.

Blank discussed the difference between the horsepower of a regular computer versus a supercomputer and how it impacts each individual item (called an "entity") in the simulations.

"It's fidelity versus scale. Typically, as you've increased the number of entities that you put into a simulation, your resolution of any particular entity has gone down because you just can't support a million entities at a constant level of resolution. Our entities have behaviors associated with them. Now we can maintain the full behavior characteristics of the entity as we scale out to a million," Blank said.

"In a previous life, we ran about 32,000 entities at any given time. That was probably the max that we were capable of. With supercomputers, you can run over one million entities, and we've done it," he added.

Blank said the advantage of having a supercomputer housed at USJFCOM will enhance capability and make development much easier.

USJFCOM accomplished this effort with the help of the University of Southern California Information Science Institute, which played a major part in working with the HPCMP to acquire the supercomputer. USJFCOM was negotiating for about a year before it received the final approval.

"They have significant supercomputer experience, and we worked fairly close with them because of their expertise to keep us smart, engaged and in the right direction," Blank said.

For more information, go to http://www.jfcom.mil/about/abt_j7.htm or phone USJFCOM public affairs office at (757) 836-6555. CHIPS

Developing the Information Technology Professionals of Tomorrow - Today

Wanted: Top performing Information Systems Technicians, who are seeking a challenge ...

Interested in being a part of an innovative special program that facilitates a combination of internship techniques in the achievement of engineer-level certifications and higher-level Navy Enlisted Classification codes to place the right people, with the right skills, in the right place? If so, a tour in a Navy Marine Corps Intranet Detachment may be just the assignment for you.

The NMCI is the Department of the Navy's shore enterprise network that delivers centrally managed, comprehensive, end-to-end information service through a common computing and communications environment. The NMCI Detachments were established as part of this groundbreaking initiative.

In a revolutionary approach for developing information technology core competencies, Sailors assigned to the NMCI Detachments are trained by the industry's most highly trained experts from companies such as Electronic Data Systems (EDS), Dell and Netco Government Services.

Fully integrated into the enterprise, Sailors are valued members of the NMCI team supporting a network only second in size to the Internet. Currently comprised of more than 300,000 seats, the NMCI is expected to grow to more than 360,000 seats in its final state.

Through a blended solution of instructor-led, computer-based and on-the-job training, Sailors develop the knowledge, skills and abilities to effectively operate, maintain and administer secure, reliable networks as part of the Navy's training strategy. This approach allows Sailors to return to the fleet fully capable of administering, maintaining, analyzing and securing enterprise-wide networks.

As word gets out to the fleet about the many successes of the program, commands are aggressively seeking out our Sailors for follow-on tours. The critical skills and abilities developed in the program are an immediate value to the fleet's operational readiness and are quickly gaining our Sailors recognition as some of the best qualified information technology professionals in the Navy.

As a member of the NMCI team, Sailors progress through the enterprise developing information technology core competencies through help desk, base operations and network operations job assignments. An individual development plan is devised for each Sailor based on his or her knowledge and experience to ensure optimal progression through the enterprise.

Sailors receiving valuable training. Clockwise, NMCI network monitoring administrators, IT1(SW/AW) James Ruffin, IT1(SW) Eric Young and IT2(SW) Rebecca Manns. MS Exchange administrator IT2(SW) Rondy Pringle. Windows 2000 administrators, IT1(SW/AW) Candice Rook and IT2(SW) Jason Dennis.

Along with receiving real-world information technology experience and training, the NMCI Detachments also provide Sailors with the unique opportunity of attaining industry standard certifications from leading organizations, such as the Computing Technology Industry Association (CompTIA), Microsoft and Cisco.

Created as a win-win partnership between EDS, the primary contractor, and the Navy, there are tremendous benefits for all involved. Sailors receive state-of the-art information technology training and certifications, and EDS receives knowledgeable technicians integrated into its workforce, and ultimately, the Navy returns Sailors to sea as well-trained network systems administrators fully capable of meeting fleet requirements.

The NMCI Detachments are collocated with the NMCI Network Operation Centers and help desks in Norfolk, Va., and San Diego, Calif. To qualify for assignment to this innovative program, Sailors must be motivated Information Systems Technicians who meet requirements of MILPERSMAN 1306-967, including the warfare qualification, Physical Readiness Test (PRT) standards and five years obligated service.

Go to Navy Knowledge Online: https://www.nko.navy.mil for more information, select Organization & Communities then select Organizations. The NMCI link is located under Programs or you can contact the personnel below. CHIPS

Public Affairs Officer
NMCI Detachment Norfolk, Va.
DSN (312) 646-2126 or (757) 963-1105

Senior Enlisted Leader
NMCI Detachment San Diego, Calif.
(619) 522-5564

Electromagnetic Railgun – A "Navy After Next" Game Changer

First Test of Electromagnetic Railgun Facility is a Success

By Lucia Sanchez

The next generation of naval guns was launched Oct. 2, 2006, with the successful test and stand up of an electromagnetic (EM) railgun facility at the Naval Surface Warfare Center Dahlgren Division (NSWCDD) Laboratory.

Under the auspices of the Office of Naval Research (ONR), engineers at the laboratory fired a low energy shot, the first in a series of tests required to bring the facility online.

Using a 90 mm bore launcher with a copper rail and a power plant capable of delivering 8 mega joules (MJ) of muzzle energy, a 2.4 kg projectile was fired at 830 m/s, yielding an energy of 0.8 MJ.

"We are one step closer to the future of naval weaponry with the stand up of this, the largest operational EM facility in the Navy," said ONR program manager for the electromagnetic railgun Dr. Elizabeth D'Andrea.

"The recent advances in science and technology are what has made this technology feasible, as well as the collaboration of scientists and engineers across government agencies, industry and the branches of service," D'Andrea said.

The October low-energy shot was the first in a series of tests required to bring the facility online. According to NSWC Dahlgren Electromagnetic Railgun Office program manager Charles Garnett, all systems performed well during the initial test and full capability operations are anticipated by January 2007.

"With the potential to deliver lethal, hypersonic projectiles at ranges in excess of 200 nautical miles within six minutes, a naval railgun offers a transformational solution for volume fires and time-critical strike," said Commander NSWCDD Capt. Joseph McGettigan.

"Understanding the technical dimensions of ships, ship systems and weapons, allows us to deliver innovative and affordable capability to the nation — as the standup of this facility and the work we do for ONR on this project exemplifies," McGettigan said.

As part of ONR's electromagnetic railgun program, the stored energy, launcher and terminal area will be increased in size to accommodate a 32 MJ muzzle energy gun by fiscal year 2009.

This facility provides the first steps toward the envisioned tactical Navy system of 64 MJ of muzzle energy.

How a Railgun Works

A railgun launcher consists of two parallel conductors, or "rails," bridged by an electrically conductive sliding armature. The gun is fired when a large current pulse is introduced at the end of one rail, flows down the rail, across the armature, and back up the other rail.

This current loop induces a magnetic field, which interacts with the current in the armature, to produce a force proportional to the magnitude of the current. A very large current pulse (millions of amps) will produce a force sufficient to accelerate an integrated armature-sabot-projectile launch package to hypersonic velocity.

Railguns provide a capability for sustained, offensive power projection, complementary to missiles and tactical aircraft.

Railguns may be a cost-effective solution to the Marine Corps Naval Surface Warfare Support future assault requirements for expeditionary maneuver warfare because of their unique capability to simultaneously satisfy three key warfighting objectives: (1) extremely long ranges; (2) short time-of-flight; and (3) high lethality (energy-on-target).

One important distinction between railguns and propellant-based guns is the difference in muzzle velocity. The 5-inch/54 and 5-inch/62 guns of today achieve muzzle velocities of approximately 800 m/s. In contrast, a railgun can accelerate a projectile to hypersonic velocities of 2500 m/s or Mach 7 and greater, enabling more that 200 nautical mile ranges within a six-minute time of flight.

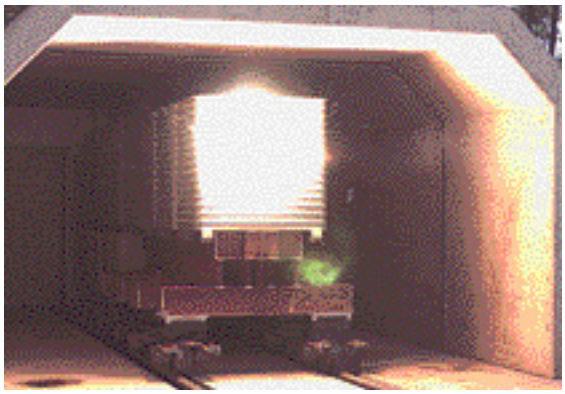
Such high muzzle velocities preclude the need for post-launch rocket-assist to achieve extended ranges. In an indirect fire mode, the projectile flight profile is predominantly exo-atmospheric, reducing the deconfliction problem and potential for Global Positioning System jamming.

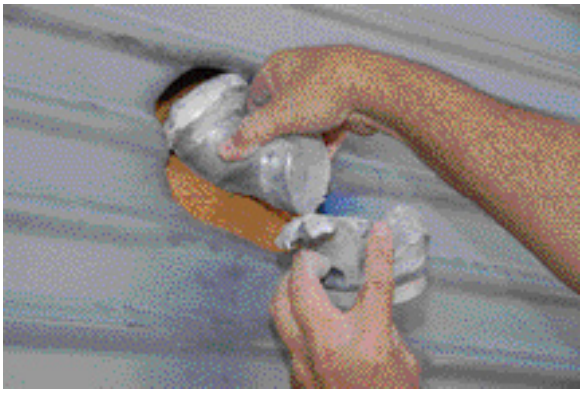
However, railguns could also be used in a direct fire mode against surface targets, with only seconds from time of launch to impact.

A notional 15 kg railgun flight body arrives on target with a 1500 m/s or Mach 5 terminal velocity, which equates to 17 MJ of available kinetic energy. This is about twice the kinetic energy available from a conventional 5-inch KE warhead from a projectile at half the weight.

Time is Right

Railguns are not a new concept. Railgun research in the United States has been ongoing for more than two decades. In the 1980s, railgun research was conducted under the Strategic Defense Initiative (SDI) in an effort to develop the space-based intercept of intercontinental ballistic missiles.





The electromagnetic rail gun, photo at right shows the strike of a projectile, which produces a flash of light. Post strike is shown at far right. Photos taken Oct. 2, 2006, at the Electromagnetic Test Facility, courtesy of the Naval Surface Warfare Center Dahlgren Division (NSWCDD) Laboratory.

EM Railgun Snapshot

- Minimizes susceptibility to GPS jamming and simplifies deconfliction
- Direct fire horizon in 6 seconds
- Hypervelocity electromagnetic launch (Mach 7.5)
- Hypervelocity impact (Mach 5) indirect fire (200+ nautical miles in 6 minutes)
- Fixed and relocatable targets at long range
- GPS guidance, navigation and control
- Ballistic trajectory; large capacity magazines; no propellants
- No explosive warheads;reduced ship vulnerability; simplified logistics
- Long-range; time-critical; persistent; all-weather (24/7)
- No unexploded ordnance issues and support for distributed operations

The Army began research in 1985 to develop a mobile, ground-based electromagnetic system capable of defeating future armored combat vehicles.

It is the refurbished SDI launcher that is currently installed at NSWC Dahlgren, while the program awaits delivery in June 2007 of a gun being built by BAE Systems. The new gun is a "laboratory" version with removable rails that weighs in at 40 tons, according to Garnett.

As Dr. D'Andrea noted, it is the combination of three technology "enablers" that sets the stage for developing a long-range naval railgun. The first stems from the Secretary of the Navy decision to make the next Navy surface combatant, DDG-1000, an Integrated Power System (IPS) ship.

This decision opened the door for a new generation of "electric" weapons, including railguns.

With proper design, the IPS can dedicate most of the power to electric propulsion motors for high-speed operations or when the tactical situation allows, the power can be shared among various electric weapons and sensors.

The amount of power required for a railgun depends on the rate of fire. With an expected 80 megawatts of installed electrical power, electric warships will have ample power to supply a railgun with the 15-30 MW necessary for sustained fires at 6-12 rounds per minute.

It's worth noting that the railgun would eliminate the need for both gun powder and explosives from the magazine. This improves ship safety and lowers logistics costs.

The second enabler is the advance in precision-guided projectile technology, evidenced by the success of programs such as Barrage, Extended Range Guided Munition (ERGM) and the Autonomous Naval Support Round (ANSR). The proliferation of Guidance, Navigation and Control (GNC) systems for Defense Department applications suggests opportunities for smaller, more robust packages at reduced cost.

These trends can only benefit the development of an affordable, hypersonic, guided projectile for railguns.

Finally, the result of Army-sponsored research at the University of Texas Institute for Advanced Technology has provided significant progress in the area of barrel life. Solutions defined at small scale in the university environment will be tested at large scale at the Dahlgren Electromagnetic Launch Facility.

Future Plans

For the ONR-sponsored program at NSWC Dahlgren, the build to a fully operational facility will be conducted in steps. The low-energy initial shot will lead to gradual increases in energy and speed that will lay the groundwork for the engineering team with data, analysis and hands-on experience in preparation for the delivery of the 32 MJ gun expected in summer 2007.

In parallel, the program will be increasing its pulse power capabilities to power the higher energy launcher.

The envisioned tactical Navy system of 64 MJ of muzzle energy is one step closer to fruition with the stand up of the Navy's largest operational EM facility. The engineers at Dahlgren, under the sponsorship of the ONR Electromagnetic Railgun Program will continue to exploit the recent advances in science and technology that made this technology feasible.

Lucia Sanchez is with the NSWCDD corporate communications office.

CHIPS

– Fact Sheet from Program Executive Office, Ships

DD(X) 1000

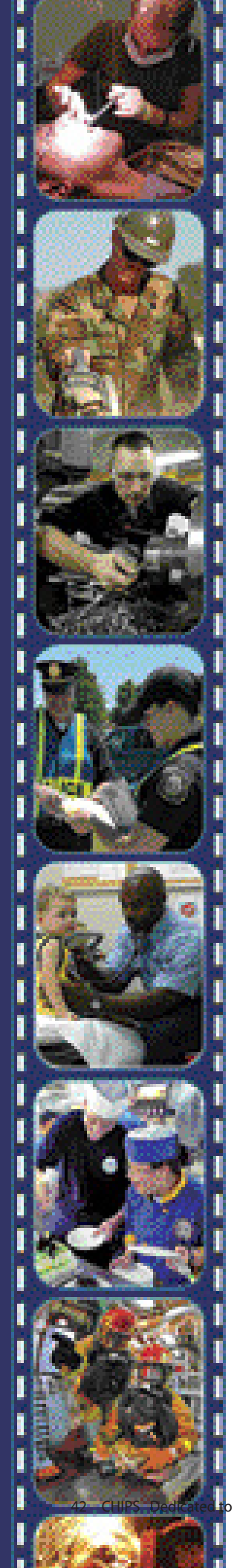
The Navy's first DD(X) destroyer featuring an Integrated Power System (IPS) will be designated DDG 1000. As the lead ship in the class, it will be named in honor of former Chief of Naval Operations Adm. Elmo R. "Bud" Zumwalt Jr.

Zumwalt is the lead ship in a class of next-generation, multimission surface combatants tailored for land attack and littoral dominance, with capabilities designed to defeat current and projected threats as well as improve battle force defense.

Compared to current U.S. Navy destroyers, the Zumwalt-class destroyer will triple both current naval surface fire coverage, as well as capability against anti-ship cruise missiles. It has a 50-fold radar cross section reduction compared to current destroyers, improves strike group defense 10-fold and has 10 times the operating area in shallow water regions against mines. The Zumwalt class fills an immediate and critical naval warfare gap, meeting validated Marine Corps fire support requirements.

The IPS technology includes an advanced gun system, an advanced peripheral vertical launch system, integrated undersea warfare automation for mine avoidance, dual-band radar, at-sea weapons effect and an autonomic fire suppression system and the Total Ship Computing Environment.

Under the Navy's dual lead ship acquisition strategy proposed in the President's budget for fiscal year 2007, Northrop Grumman Ship Systems and General Dynamics Bath Iron Works will concurrently build the dual lead ships. Zumwalt will be delivered in 2012.



Navy "COOL" Web site provides credentialing information for Navy workforce

By Darlene Goodwin

The Navy Credentialing Opportunities On-Line Navy "COOL" Web site provides comprehensive information on occupational credentials related to Navy work experience and training.

Capt. Kevin R. Hooley, commanding officer for the Center for Information Dominance (CID) Corry Station and Navy COOL project leader, said the site is another innovative Navy blended training solution. "Navy COOL is all about personal and professional development and readiness," he said. "It harnesses a vast amount of information and Web links on one site and provides a road map for earning certifications, licenses and apprenticeships."

A portable copy of Navy COOL, "COOL to Go," has been developed for those with limited Internet connectivity. COOL to Go is downloadable to a hard drive, compact disc or thumb drive. It is identical to Navy COOL, minus connectivity to external sites if used offline. COOL to Go compact discs are planned for distribution with the December 2006 edition of All Hands magazine.

Interest in Navy COOL is high, with more than 6 million hits and 136,000 visits since its June 2006 launch. Even more impressive is that most users spend an average of 11 minutes on the site.

"In the information age, an 11-minute visit in the cyber medium is a long time," Hooley said. "Web visitors are generally looking for quick information and moving on to the next thing, so the fact that Navy COOL visitors are spending longer amounts of time on the site tells me they are finding plenty of helpful information — the information they need. We're also receiving overwhelmingly positive feedback from users."

Rear Adm. Dave Gove, commander, Navy Personnel Command and Deputy Chief of Naval Personnel, encourages all Sailors to visit Navy COOL.

"We believe that Sailors who are provided the opportunity to enhance their professional development are not only better performers on the job, but these top performers are more likely to choose to continue their service in the Navy," said Gove.

"We are striving to create and retain the most highly skilled workforce possible, and this key investment in the professional development of our workforce is a win-win for the Navy and the nation."

Visit Navy COOL at https://www.cool.navy.mil.

For more information, contact the Navy Credentials Program Office via e-mail at crry_cqcredentials@navy.mil.

Darlene Goodwin is the public affairs officer for the Center for Information Dominance Corry Station. She can be reached at crry_pao@navy.mil or (850) 452.6672.

CHIPS

Credentialing the DON IA/CND Workforce

The Navy COOL Web site is just one of the new professional development tools supporting commercial credentialing

In the Federal Information Security Management Act, the Department of Defense directed military services to commercially certify Information Assurance (IA) and Computer Network Defense (CND) professionals. In compliance with the directive, the Department of the Navy's credentialing program is well underway toward bolstering military, civilian and contractor capability in a highly trained joint IA workforce. (The Department of Defense "IA Workforce Improvement Program" Manual (DoD 8570.01-M) is located at http://www.dtic.mil/whs/directives/corres/html/857001m.htm.)

Today Navy IA and CND professionals are preparing for commercial certification tests — transforming IA training from traditional venues to a blended solution of e-learning and commercial and military classrooms, in a continuum of life-long learning.

The Navy Credentialing Opportunities On-Line (COOL) Web site is just one of the new professional development tools supporting commercial credentialing. Navy and Marine Corps IA Training Management Systems, as well as an electronic paperless test voucher system, are also being piloted.

All Defense Department IA/CND personnel with privileged access or who perform IA management tasks are required to obtain either an IA or both IA and operating system commercial certification, depending on the competencies required of their job.

Enterprise-funded test vouchers are available through the Navy Credentials Program Office at no cost. To obtain a free test voucher, Navy and Marine Corps IA professionals must take a pretest to determine if there are learning gaps that need to be mitigated prior to taking the commercial certification test. See the Navy COOL Web site for details at https://www.cool.navy.mil.

For more information about credentialing the DON IA Workforce, please phone (703) 413-7013.

CHIPS

Enabling Warfighter Mission Assurance Through Effective Vulnerability Remediation

By Steve Muck

A component of the DON Critical Infrastructure Protection (CIP) Program is remediation of vulnerabilities identified by either an outside assessment team or as the result of a self-assessment conducted by the command. This is an integral part of Secretary of the Navy CIP Instruction 3501.1A and supports the Department of Defense Directive 3020.40, Defense Critical Infrastructure Program (DCIP). The following article describes a new DON CIP initiative in the area of remediation.

Providing vulnerability remediation training has been a goal of the Department of the Navy Critical Infrastructure Protection (DON CIP) Program for some time, a goal whose urgency has grown as the issues facing installation commanders have become more complex.

Funding, personnel, materiel, time — in some cases all of these — have made the decision of what and how to remediate difficult at best. In response, the DON CIP team has developed a Command Remediation Visit initiative that assists installation commanders in this area by providing on-site risk management based training and analytical guidance.

A major component of the Command Remediation Visit is the **"Remediation: Analysis, Strategy and Action Plan (ASAP)"** course, a training program developed specifically for DON regional and installation representatives.

Remediation training can occur at any time, but it is most effective when it occurs shortly after the completion of a vulnerability assessment. The first implementation of the CIP remediation initiative (at Naval Air Station Whidbey Island Wash., in September 2006) followed this preferred protocol by occurring shortly after a Chief of Naval Operations Integrated Vulnerability Assessment (CNO IVA), which was completed in August.

The DON CIP team presented the ***Remediation: ASAP*** training course to 12 senior Navy and civilian staff representatives from NAS Whidbey Island and various tenant commands. The class focused on training the installation staff to utilize the course's disciplined remediation analysis processes (see Figure 1), which were applied to a sample of the vulnerabilities identified during the August CNO IVA.

This instruction enabled the staff to evaluate and prioritize assessment findings and the remediation options available for each vulnerability identified. A product of the training was a set of proposed courses of actions created by class participants for remediating the assessment's more significant vulnerabilities.

Figure 1. Training focused on a disciplined approach.

This set of actions was briefed by the NAS Whidbey Island Executive Officer, Cmdr. Dan Brown, to the Commanding Officer, Capt. Syd Abernethy.

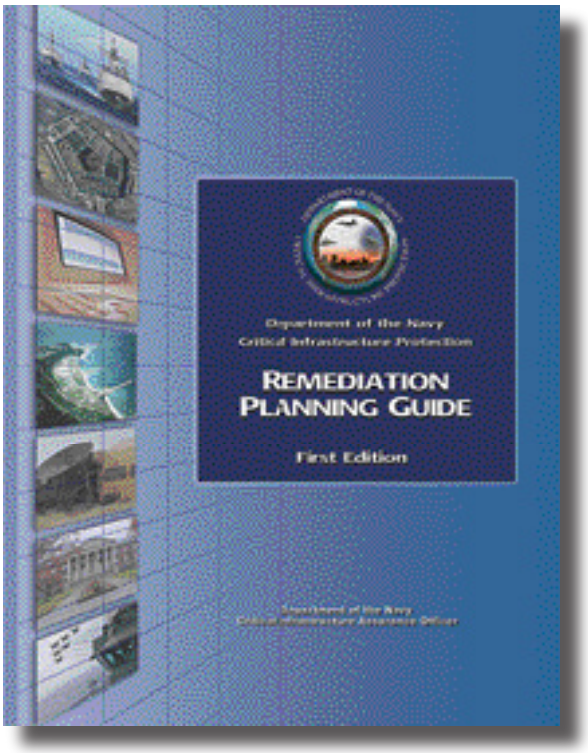


Figure 2. DON Remediation Planning Guide.

An ongoing benefit is that with the understanding gained over two days of intense classroom training, the installation and tenant command staffs can now apply the ***Remediation: ASAP*** processes to the remaining assessment findings in order to develop a comprehensive remediation action plan.

Feedback from course participants was overwhelmingly positive, with most stating that their training experience produced a plan that was both viable and valuable. The structured methodology to work through vulnerabilities set the stage for implementation and gave users a tangible plan of action.

Reactions included comments such as: "The session encouraged out-of-the-box thinking that resulted in imaginative solutions ..."

"Using a cross-functional approach with non-subject matter experts having equal opportunity for input really helped us work toward smarter decisions …"

Capt. Abernethy said, "For us, it was a positive experience we would recommend to other installations."

Training Foundation and Key Tool: The Remediation Planning Guide

The CIP team developed the training from the concepts discussed in the DON Remediation Planning Guide, published in 2004 by the DON Chief Information Officer (CIO), as the DON Critical Infrastructure Assurance Officer (see Figure 2).

This planning document provides a methodology and plan of action that assists DON entities in developing vulnerability remediation strategies that balance resources and risk.

For example, the guide defines four factors critical

Figure 3 illustrates the four factors that are critical to successful remediation within a disciplined approach.

to successful remediation, as shown in Figure 3: (1) procedures/policy; (2) an informed chain of command; (3) key personnel; and (4) a disciplined approach. The first three factors are controlled by the command.

The ***Remediation: ASAP*** training course provides the disciplined approach necessary to develop and implement a successful remediation plan.

The effectiveness of the approach taught within the course depends on the involvement of key installation and tenant command personnel, the support of an informed chain of command and a thorough understanding of the particular policies and procedures applicable to the installation.

The goal of successful remediation is to reduce vulnerabilities while achieving maximum return on investment and focusing limited resources on the most essential assets.

Remediation can provide proactive protection against criminal and natural acts that threaten to disrupt mission accomplishment. Because proper remediation may actually thwart or minimize the chances of a terrorist attack, it makes sense to "harden" those assets believed critical to the warfighter's mission through remediation actions.

The DON CIP Program's Command Remediation Visit initiative is a valuable tool that supports mission assurance by promoting effective remediation strategies and plans.

To access CIP policy and guidance, go to the DON CIO Web site at http://www.doncio.navy.mil, click on the Project Teams tab, then click on Critical Infrastructure Protection.

CHIPS

Coalition Interoperability Reaches New Heights in RIMPAC 2006

Forty ships, six submarines, 160 aircraft and more than 19,000 personnel from Australia, Canada, Chile, Japan, Peru, South Korea, the United Kingdom and the United States engaged in seamless communications during RIMPAC 2006 …

By Lt. Cmdr. Vince Augelli, Lt. Cmdr. Dave Samara and Lt. Cmdr. George Haw

Commander, U.S. Third Fleet achieved unprecedented coalition interoperability during the latest Rim of the Pacific (RIMPAC) exercise. Scheduled by the Commander, U.S. Pacific Fleet, RIMPAC is a biannual multinational exercise conducted in the Hawaiian operating area. The exercise, conducted from June 26 through July 28, featured 40 ships, 6 submarines, 160 aircraft and more than 19,000 personnel from Australia, Canada, Chile, Japan, Peru, South Korea, the United Kingdom and the United States.

Cooperative Maritime Forces Pacific

The major advance in RIMPAC '06 was the introduction of the Combined Enterprise Regional Information Exchange System (CENTRIXS) community of interest called the Cooperative Maritime Forces Pacific (CMFP).

CMFP offered Web-browsing, e-mail, chat and the common operational picture over a secure network. While different security enclaves within CENTRIXS have been used in previous RIMPAC exercises, this was the first time that all participants had access to a common network.

A comparison between RIMPAC '04 and RIMPAC '06 will better illustrate this. The January-March 2005 edition of CHIPS featured an article *(available at http://www.chips.navy.mil/archives/05_Jan/web_pages/RIMPAC.htm)* describing the C4I architecture for RIMPAC 04. It included four different security enclaves for coalition releasability: CENTRIXS FOUR EYES – used by U.S., U.K., Canadian and Australian forces; CENTRIXS-J – used by U.S. and Japanese forces; CENTRIXS-R – used by U.S., South Korean and Chilean forces; and SIPRNET – used by U.S. forces.

For these four different security enclaves partial interoperability was achieved through the use of air-gapping, replication and a high assurance mail guard.

Of note, only the exercise's Task Force Commander/Combined Forces Maritime Component Commander (CFMCC) ashore in Pearl Harbor enjoyed access to all four enclaves. All other participants were dependent on the redistribution of information from this central node. While cleverly done, time delays were unavoidable.

In contrast, CENTRIXS Cooperative Maritime Forces Pacific was accessible to CFMCC headquarters, the outlying shore sites including all component commanders and commanders of maritime task forces, and every U.S. and coalition ship in the entire exercise. Information that was seen at Pearl Harbor was available afloat at the same time. This led to an unprecedented level of operational execution and planning.

CMFP Provides Unprecedented Interoperability

CMFP is a new community of interest in the existing CENTRIXS Global Counterterrorism Task Force (GCTF) security enclave. It was developed by Mr. Bob Stephenson, chief technology officer for command, control, communications, computers and intelligence operations at the Space and Naval Warfare Systems Command, and Mr. Tim Gannon, a division head from the Naval Network Warfare Command. The CMFP was used on a large scale for the first time during RIMPAC '06.

"We were a victim of our own success. Everyone wanted more CMFP."

– admiral participating in RIMPAC 2006

Based at the Pacific Regional Network Operations Center at Wahiawa, Hawaii, CMFP was the core of the integrated planning and execution in RIMPAC '06. Servers were also located at Esquimalt, British Columbia, and the Australian NOC at Canberra, as shown in Figure 1.

Ships connected to CMFP through satellite connection. U.S. ships had Internet Protocol connectivity through the Defense Satellite Communications System super high frequency X-band termination or dedicated International Maritime Satellite Bravo (Inmarsat-B) lease.

Coalition ships used dedicated Inmarsat-B leases with the exception of HMAS Manoora, which used a commercial Ka-band termination to Australia. Notably, this was the first RIMPAC in which each ship had continuous round-the-clock CENTRIXS connectivity versus intermittent dial-up connection.

The RIMPAC Combined Air Operations Center was established for the first time at Kenney Headquarters at Hickam Air Force Base. The RIMPAC Combined Forces Air Component Commander was able to leverage Kenney's tremendous capabilities and infrastructure while enjoying the same CMFP connectivity with coalition forces.

The core of the Combined Forces Air Component Commander's planning was conducted on a special version of the Theater Battle Management and Core System that was created for coalition use.

The result was a reliable, secure network which succeeded in attracting an unprecedented number of collaborators.

Whereas CENTRIXS access in previous exercises had been largely limited to watchstations, CMFP attracted hands-on attention from numerous participants throughout the chain of command up to flag level.

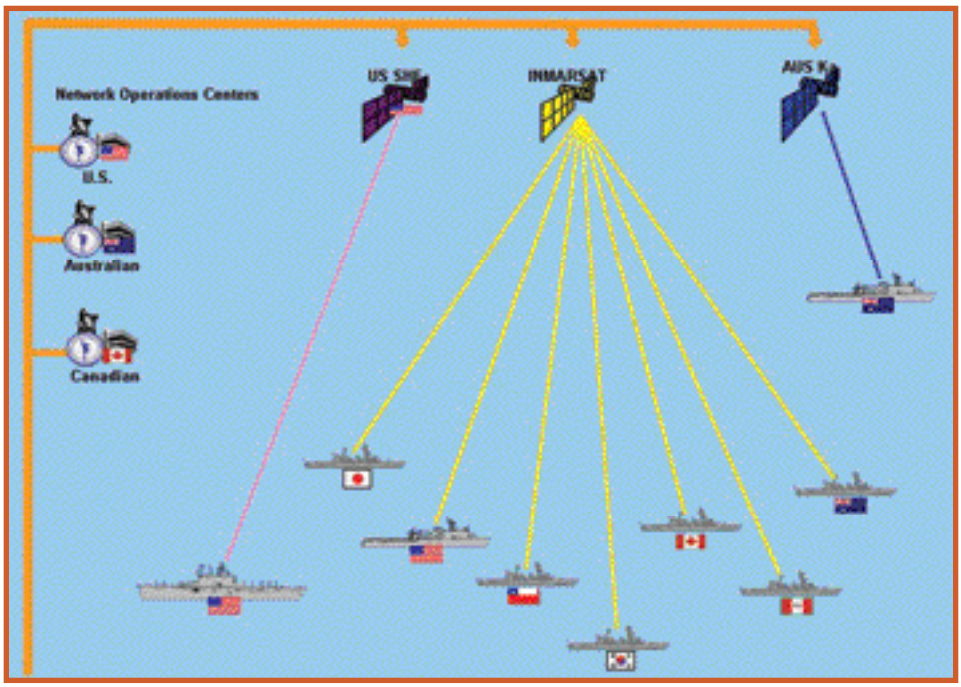
One admiral aptly summed up the phenomenon by noting that, "We were a victim of our own success. Everyone wanted more CMFP."

Hopefully, that will indeed be the case in RIMPAC 2008.

The authors were members of the Third Fleet staff for RIMPAC '06. Lt. Cmdr. Augelli is the fleet communications officer, Lt. Cmdr. Samara is the knowledge manager and Lt. Cmdr. Haw is the fleet information systems officer.

CHIPS

Figure 1. RIMPAC 2006 CENTRIXS CMFP Architecture.



CHIPS 25th Anniversary

CHIPS celebrates 25 years in publication in 2007 as the Department of the Navy Information Technology Magazine.

Our founding motto — Dedicated to Sharing Information, Technology and Experience, aligns with our goal — to deliver knowledge superiority to the warfighter.

CHIPS is sponsored by the DON IT Umbrella Program of contracts and the Department of the Navy Chief Information Officer (DON CIO). Each issue contains a message from the DON CIO and articles highlighting the latest IT policies and initiatives in the DON and Department of Defense.

The Umbrella Program team assembles the latest information regarding the Umbrella Program contracts and Blanket Purchase Agreements (BPAs). Each issue contains an easy to use shopping guide — Under the Contract — spotlighting better than GSA pricing for all your technology needs.

Every issue is packed with cutting-edge technology topics, such as FORCEnet; knowledge dominance; C4ISR and network-centric warfare programs; e-business; e-learning; professional development — and interviews with top leadership from the DON and DoD.

We welcome articles from our readers! Please help us celebrate by submitting your articles and ideas to the CHIPS editors at chips@navy.mil.

CHIPS is published quarterly. Articles must be approved by your public affairs office and your chain of command prior to submitting your article to CHIPS.

CHIPS writing guidelines are available on our Web site at http://www.chips.navy.mil/chipsguidelines.html. For assistance, and to request a subscription or extra copies of CHIPS, contact a CHIPS editor at (757) 444-8704 or DSN 564.

Thank you for your support! It has been a pleasure for us to serve you, and we look forward to serving you for another 25 years!

CHIPS

You are invited to the
DON IM and IT Conference

Department of the Navy Information Management and Information Technology

Hosted by the Department of the Navy Chief Information Officer (DON CIO)

The DON IM and IT Conference provides a venue to share information about the latest DON IM and IT initiatives, policy, and guidance. Conference topics include:

- Certification & Accreditation
- Critical Infrastructure Protection
- Data Management
- DON IM/IT Civilian Workforce
- DON IT Umbrella Program
- Enterprise Architecture
- Enterprise Software/IT Asset Management
- FISMA
- Information Assurance
- IT Performance Measurement
- Knowledge Management in Support of the Warfighter
- Privacy
- Public Key Infrastructure
- Service Oriented Architecture
- Strategic Management of the Electromagnetic Spectrum
- Telecommunications
- USMC Civilian ITM Community of Interest
- WiMAX
- Wireless
- World Radio Conference 2007

The DON IM and IT Conference will be open to all DON, government, military and support contractor attendees. No conference fee will be assessed, but registration is required.

The agenda and registration are available on the DON CIO web site at http://www.doncio.navy.mil. For additional information call (703) 602-6274 or (703) 607-5650.

QuABO

An Interview with Cmdr. John Ingersoll

Cmdr. Ingersoll is a Reservist who has supported the Space and Naval Warfare Systems Center (SSC) Charleston in a number of capacities for the last five years. As a physicist specializing in quantum physics, he has developed a concept of knowledge discovery based on quantum physics principles, which he theorizes can assist, among other Defense Department and Department of the Navy developing approaches, in thwarting a terrorist threat before it occurs.

His concept, called Quantum Affects-Based Operations (QuABO), can provide new insight and novel problem-solving approaches to the war on terror. Using the tenets of quantum physics at the macroscopic level and potentially relying on meta-systems theories, medical research and other scientific discoveries, QuABO, at the core of the Knowledge Discovery Program (KDP), can lead to adaptive results aimed at dealing effectively with asymmetrical warfare.

CHIPS asked Cmdr. Ingersoll to discuss the QuABO concept in August 2006.

CHIPS: What gave you the idea for the Knowledge Discovery Project and using quantum physics in the development of the QuABO?

Cmdr. Ingersoll: During my Reserve duty about four years ago, I was in a discussion about traditional command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) activities with some SSC Charleston personnel. The discussions centered on ideas as to what could be done to counter the enemy's asymmetric advantage.

In this situation, our adversaries employ strategies and tactics outside the bounds of conventional warfare in an attempt to level the huge disparity due to our military and technological superiority.

In response, we developed a concept called Quantum Affects-Based Operations. The idea is to use the tenets of quantum physics to a process that can be applied to the war against terror.

CHIPS: I've read about the exploration of innovative alternative approaches to solving this problem.

Cmdr. Ingersoll: In the last several years, the DoD realized that traditional warfare is not as effective in dealing with asymmetrical warfare, such as the war on terror. U.S. military forces have implemented other techniques in addition to traditional warfare as an approach to this problem.

This approach is essentially a realization of the effects-based operations (EBO) concept. The EBO idea has its origins in the Vietnam War era, when we realized that military actions alone were not sufficient to win the war. You can win battles militarily and still end up losing the war. That evolution of EBO attempts to augment military operations with a much broader scope of elements well beyond the traditional sense of attrition or warfare.

These elements may include a combination of diplomatic, information, military and economic (DIME) instruments or actions. By uniting all of these other elements, you could win ultimately. However, EBO type approaches can be best applied to determine the outcome of 'what if scenarios' to impart valuable knowledge to analysts about possible outcomes as well as the likelihood of unintended consequences of specific actions.

We are offering the QuABO model as an alternative approach based on the concepts of quantum physics applied to the macroscopic world. We are using the concepts of interconnectedness, uncertainty or indeterminacy and coherence to develop a new approach to dealing with the enemy.

CHIPS: How is the QuABO different than the effects-based model in addressing this problem?

Cmdr. Ingersoll: The solution perceived in recent years is to analyze a lot of data with the hope that one can extract something meaningful. But there is too much information, and you are essentially drowning in it. Computational power is not sufficient to deal with the situation and even the best artificial intelligence we have cannot deal with the problem.

Some data can be irrelevant. The enemy may be deliberately sending us information that is useless in the hope that we will spend a lot of time trying to figure out something out of nothing.

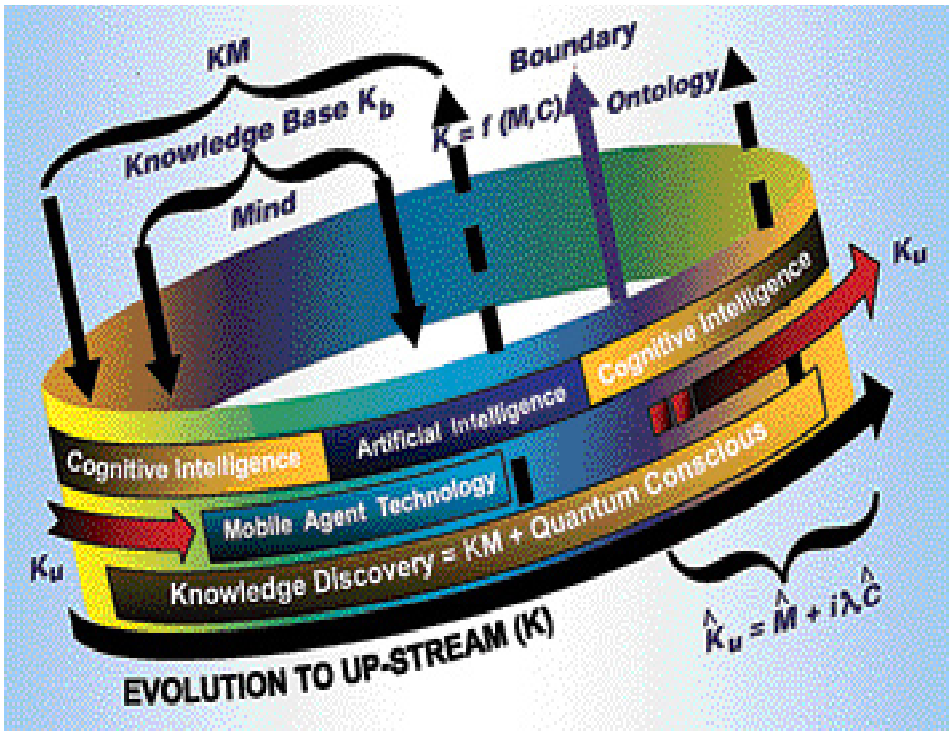


Figure 1. The Knowledge Discovery Continuum.

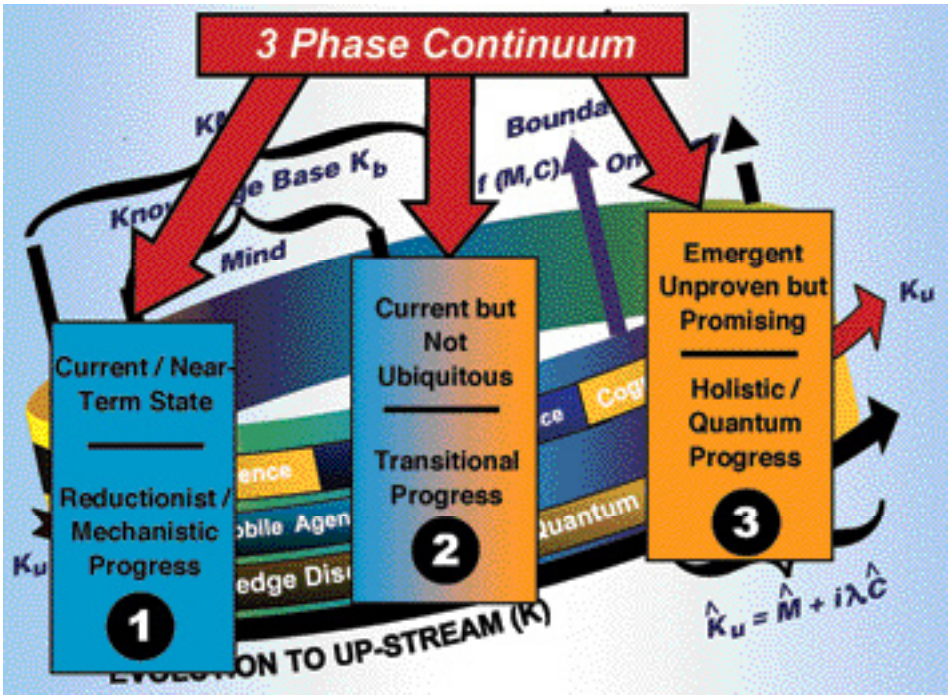


Figure 2 shows the evolution of Knowledge Discovery. No. 1 is where we are right now — the state of knowledge management or knowledge discovery as it is today. No. 2 shows the opportunities that we currently have but are not using. Semantic Web technology is an example of that. No. 3 shows the emergent QuABO concept of using new methods for creating knowledge that have not been used in the past.

We have tried to rely on machinery too much for direction. Human beings are the fundamental component of making intelligent decisions. Consequently, QuABO attempts to rectify this imbalance by refocusing human intelligence and knowledge discovery principles.

The tenets of knowledge discovery can be summarized in four bullets shown here:

- How to make use of the abundance of information available to the maximum advantage of the warfighter;
- How to discover the 'unknown unknown';
- How to remove information "overload" as a problem;
- How to reach ground truth on any given issue.

For DoD, enabling the warfighter is the ultimate objective. The 'ground truth' is ultimately our goal. Ground truth is not preordained; it is based on our constitution as sentient beings within the moral compass of our consciousness.

The reality is created as we move forward. All the elements of bias must be stripped to figure out what is there.

The schematic, Figure 1, is an evolving continuum. First of all, you have to distinguish between information and knowledge. Information means all kinds of data. Knowledge discovery means something that has an intelligent or utilitarian aspect to it. It is usually actionable. Figure 2 shows the progression of the knowledge discovery evolution.

Knowledge discovery is much more profound than information. Knowledge discovery can be created only with human interaction; it cannot be created by machines. That is an important distinction.

Knowledge discovery is continuously augmented or discovered, like a spiral where you keep adding value, and moving to higher and higher levels. Figure 3 illustrates this concept in how knowledge will find users in the future.

CHIPS: How does quantum physics play a part in this process?

Cmdr. Ingersoll: One of our claims, based in quantum physics, is that the human intelligence/interaction is not constrained within our physical bodies.

Knowledge discovery in our model consists of two independent entities: One is matter and/or energy. The second is consciousness, which is not directly measurable or quantifiable by physical means, but it can be inferred indirectly.

Knowledge discovery is the outcome of the interaction of these two independent entities among intelligent beings and their environment.

The world is becoming more and more intertwined. It represents now a much bigger entity. The increasing complexity of this entity makes it very difficult to figure out how to continue improving our productivity and our standard of living, for example.

You may note that I have used the word entity rather than system in order to differentiate between the quantum and classical concepts, respectively.

The current approach to dealing with complex systems has worked very well for the last 300 years, but in the last 40 years that model has started failing.

The view of the world as an assembly of vastly independent entities is no longer a valid approach. You have to work in a holistic way where everything is considered in its totality.

We cannot use a mechanistic view to do that. We have to enable a totally different approach. The quantum process is what we think could provide a solution to the present situation.

Our approach is to give the individuals at the bottom the ability to function, interact and make decisions. Instead of the current top-down method of command and control, we can create a bottom-up approach that engages everybody who cares to participate over a period of time determined by the participants.

Our adversaries in the war on terror lack our sophisticated organization and structure. There is no single authority; no single individual on the ground who makes decisions for all. Hence, they appear to be decentralized, informal and highly adaptive. The conflict then becomes asymmetric.

Knowledge discovery realized through QuABO becomes, in our opinion, the key element in combating asymmetric warfare effectively.

CHIPS: In this holistic approach, who would be contributing to knowledge discovery?

Cmdr. Ingersoll: A large number of voluntarily participating individuals from diverse backgrounds and multiple disciplines, for example, warfighters, civilians

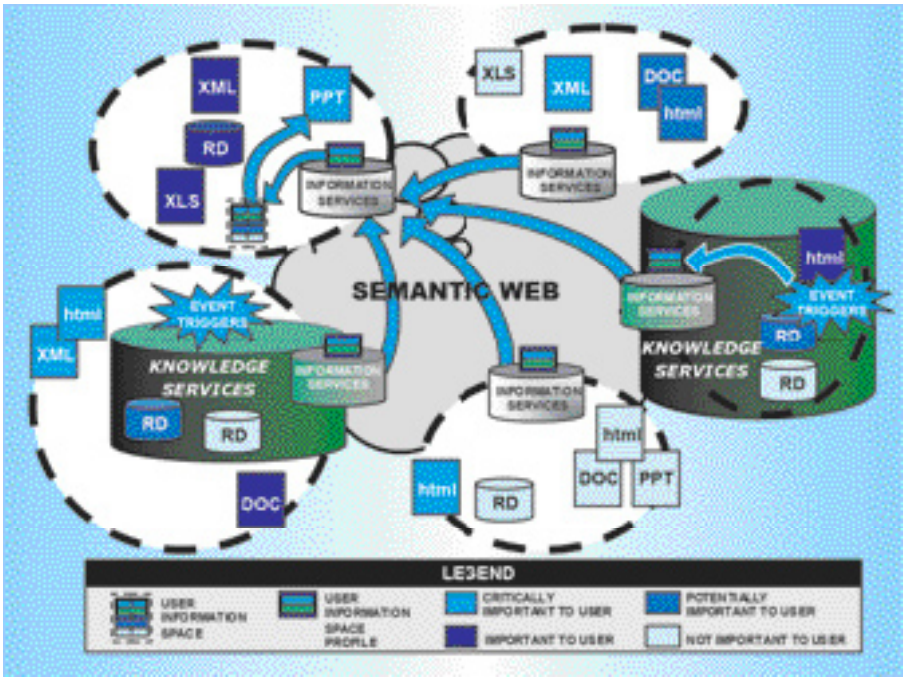


Figure 3 illustrates the concept of how knowledge will find users in the knowledge continuum.

"Knowledge discovery is much more profound than information. Knowledge discovery can be created only with human interaction; it cannot be created by machines. That is an important distinction. Knowledge discovery is continuously augmented or discovered, like a spiral where you keep adding value, and moving to higher and higher levels."

– Cmdr. John Ingersoll

and others associated with a particular situation or event. These participants would adhere to a prescribed interaction process instead of attempting to produce a preconceived outcome.

This interaction would take place at a 'present' time, which is expanded to fit the needs of the situation at hand. Communication among these participants will be in real time, in person or over large distances facilitated with the aid of modern technology.

CHIPS: How is QuABO and, by extension, knowledge discovery different?

Cmdr. Ingersoll: In classical mechanics I can watch everything around me and separate myself from the rest of the universe as an 'objective' observer.

In quantum physics that is impossible: objective is supplanted by subjective. I am part of the equation, and every time I chose to interact with my environment, I change it, while it changes me. Hence, the origin of 'affect' versus 'effect.'

The key part is that I cannot be an observer without affecting the entity I am interacting with. Knowledge discovery is not my contribution, your contribution or another person's contribution. It becomes a combined outcome of the interaction of all participants.

The underlying process is akin to 'the invisible hand' that Adam Smith used to describe the actions of the large number of actors in a free market economy. The appropriate interaction of a large number of human actors augmented by technology would realize QuABO in any particular situation.

There are a lot of mysteries about how sensors work in the body. If we can figure out how they work, we can potentially apply it to the real world and use that to enhance physical communications. There is a lot of intuitive processing that happens within the body.

CHIPS: So you will be looking beyond visible and audio communications?

Cmdr. Ingersoll: Yes. For example, the total of your communication with people that you know well — parents, significant other, children — cannot be entirely described by physical means or biology, physics or chemistry alone. There is another level of interaction that creates this communication, which we call consciousness.

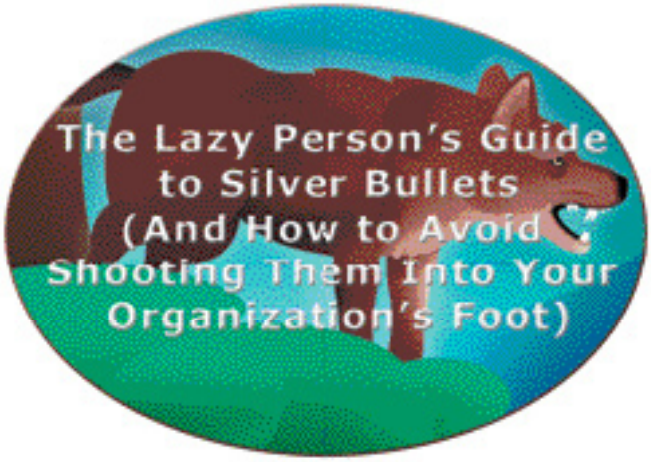
There are still many unknowns about the human body and human interaction. Our concept needs to be developed further. We have established a team of eight made up of people from multiple disciplines. On our team now we have, for example, a theology major who understands cultural differences. The team has a dynamic of both educational and cultural diversities.

It is important for the team to get along and to share and create something that is bigger than what each team member could produce on his or her own.

We need a three-year period for additional research to understand how to derive benefits for the warfighter from the QuABO model by developing the proper analytical and other simulation tools of the process in order to be able to design and carry out suitable interactions pertaining to actual situations.

We want to deliver as much as we can to the warfighter — as soon as we can. CHIPS

Cmdr. John Ingersoll is a Reservist and part of SPAWAR Reserve Unit 506 stationed in Norfolk, Va. SPAWAR Reservists possess unique, highly technical skill sets. SPAWAR Reserve Unit 506 has employed Ingersoll's unique physics and engineering duty officer abilities to solve tough fleet issues for several years.



By Retired Air Force Major Dale J. Long

"Of all the monsters that fill the nightmares of our folklore, none terrify more than werewolves, because they transform unexpectedly from the familiar into horrors. For these, one seeks bullets of silver that can magically lay them to rest."

– Frederick P. Brooks Jr.

No Silver Bullet – essence and accidents of software engineering

In the beginning, it all sounded so simple, use Total Quality Management (TQM) techniques to improve organizational effectiveness. But is it that simple? Try mixing and matching the silver bullets below with the desired outcomes and see if any of the resulting phrases sound familiar:

Total Quality Management	Reduce our costs.
Strategic Planning	Improve our products.
Management by Objectives (MBO)	Increase our productivity.
Object-Oriented Programming (OOP)	Make us a better organization.
Business Process Reengineering (BPR)	Make our customers happy.
Extensible Markup Language (XML)	Make our employees happy.
Mint Condition Beanie Babies	Fund my child's college education.

The quote from Fred Brooks is from his classic essay on the myth of a free lunch and magical solution or silver bullet for software development problems. However, I believe his insight applies to any magical solution to whatever ails an organization.

Before we go into details I would like to state that, with the exception of investing in Beanie Babies, all the techniques listed above have shown some durable value over time. However, each has also had its reputation tarnished by high profile failures, usually by organizations that implemented them in name only without adhering to their core principles.

At some point government agencies and some notable industries have tried or are engaging in initiatives that will result in high performance. On the short list of the management initiatives currently in vogue are Lean Six Sigma, Capability Maturity Models, the Balanced Scorecard and the Malcolm Baldrige National Quality Program, among others. While the attempts at process improvement are laudable, and, in some cases, mandated, organizations can encounter pitfalls along the way.

In the interest of protecting current and future investments in process improvement, let's look at some lessons learned from programs of 10 to 20 years ago to see how a potentially good silver bullet can misfire.

The Appearance of Quality

TQM was originally developed in Japan during the 1950s and later become well-known in the United States in the 1980s. TQM focuses on an organization's culture, attitude and structure to provide customers with products and services that satisfy their needs. TQM stresses quality in all aspects of the company's operations, for example, do things right the first time while eliminating operational waste and defects.

After some successes by early adopters, many public and private organizations implemented TQM principles as a cure to various organizational ailments with varying results.

The key concepts of TQM are:

Customer-driven quality. Under this concept, an organization will only be successful if its customers are satisfied. Being sensitive to customer requirements goes beyond merely meeting requirements or resolving complaints. Each organizational component also operates within the organization as a customer to some functions and as a supplier to others. Each component must treat its internal customers with the same sensitivity and responsiveness as it does for external customers.

Leadership and commitment from top management. For TQM to succeed, top management must articulate clear goals for the organization and create and deploy well-defined systems, methods and performance measures for achieving those goals.

Continuous improvement. This is the heart of TQM. A high performing organization understands that customer satisfaction is obtained by providing a high-quality product while also continuously improving the product.

TQM also recognizes that product quality is the result of process quality, so there is a focus on continuous improvement of the organization's processes, which includes a strong emphasis on preventing problems before they occur.

Rapid response. This one is pretty straightforward. The faster you can respond effectively, the happier your internal and external customers will be.

Fact-based actions. TQM focuses on using objective data, statistical analysis and performance tracking. While these are common elements of most management systems, a unique aspect of TQM is that it recognizes that most problems are system-related, rather than caused by individual employees.

In practice, data are collected and put in the hands of the people who are in the best position to analyze results, not managers, but the workers in the midst of the process.

Employee empowerment. TQM requires a committed, well-trained workforce that participates fully in quality improvement activities. The organization gives employees key process data and encourages them to take more responsibility, communicate more effectively, act creatively and innovate continuously. Any employee can stop a process if he or she finds defects.

TQM sounds marvelous, much like apple pie, motherhood and democracy. However, like democracy, TQM is a participatory culture. Thin, superficial applications simply won't provide any lasting value. Studies of TQM implementations over the last 20 years indicate that attempts to integrate TQM into both public and corporate organizations failed at a rate of 64 to 77 percent. TQM generally fails when:

- Internal processes become more important than serving customers, either internal or external.

•Top management delegates responsibility for TQM to lower levels and then moves on to the next initiative.

•Products are considered "good enough" and when processes, "ain't broke, don't fix 'em."

•Employees are rewarded for following internal rules instead of being responsive.

•Management hides bad data to avoid embarrassment.

•Employees are either not given responsibility or not trained to accept it.

However, even when you try to implement something like TQM correctly, it still might not take hold. One of the headquarters organizations that I worked under while on active duty committed to TQM. A flag officer personally led the first day of training for all employees and all 1,500 employees received at least 40 hours of TQM training. We went by the book in implementing the program.

Two years later, the only consistent sign of TQM that remained were some people who insisted on using meeting agenda forms, though participants in many meetings didn't stick to them. Some pockets of quality remained, but given the normal churn rate of people into and out of any military organization, trained employees were regularly replaced by people with a different outlook. Departing employees left for other assignments with a different quality emphasis.

Yes, there was probably a positive effect overall on the organization due to everyone being exposed to TQM, but it did not result in a sweeping transformation of organizational culture. Once the push for TQM relaxed, entropy developed, and we returned to pretty much where we were before.

There are two other topics I would like to discuss in relation to silver bullets: change and the sunk cost fallacy.

Change Requires Force

Newton's First Law of Motion states that unless acted upon by an external force, a body at rest will remain at rest and a body in motion will remain in motion.

Taken at face value, the first part of the statement agrees with what we see every day. Leave a book on a table and that book will stay there, unless an external force moves it. Please bear in mind, however, that "rest" does not mean an absence of force. In the case of the book, gravity (another of Newton's favorites) pulls it down and the table holds it up. Rest, in the case of motion, essentially means zero net force — not just an absence of force.

The second part of the law states that a body in motion will keep moving unless acted upon by an external force. This part is not generally supported by what we perceive in the physical world. If we set an automobile in motion and then apply no further force it will eventually come to rest through a combination of gravity and friction, external forces that act on it to deplete the force moving it.

To keep the car in motion, we need to provide external force sufficient to counter the forces acting against the motion to achieve zero net force. The car will stay in motion as long as we maintain this balance.

There is one other principle of this law that we should consider before relating it to organizational change: Uniform linear motion is the natural state of motion. To use a more familiar phrase: Motion takes the path of least resistance, which is usually a straight line. Keeping the car in motion and changing the direction and speed of the car take more force than simply keeping it rolling in a straight line.

The term we normally use to represent Newton's First Law of Motion is "inertia," which relates to an object's amount of resistance to change in velocity. In this context, organizations generally remain both "in motion," at least internally, due to their constant activity and "at rest" due to a zero net force balance of forces in how they operate.

In other words, we chug along at a relatively constant speed and direction unless some force acts upon us to change things.

Introducing TQM (or Lean Six Sigma) into an organization is an attempt to change velocity, either internally, externally, or both. Overcoming organizational inertia usually requires sustained effort over time. Depending on the amount of resistance, the amount of force required is at least inversely proportionate to the length of time in which you try to make the change. In essence, it takes at least 10 times the force to make a change in one year than it does to make the same change over 10 years.

One of the reasons silver bullets get their name is that people who employ them expect instant results, not gradual change over time. They are an attempt at, as the name suggests, a violent solution to what ails us. Applied with this intent, however, all they are likely to do is put a hole in your foot.

Sink Faster

There is one other element that contributes to the organizational pain of self-inflicted silver bullet wounds: the sunk cost fallacy (SCF). This delusion takes the form of thinking that just because we've spent a lot of money on something, giving up on it would "waste" the money already spent.

Devotees of the SCF believe that all they need to do to fix things is to spend even more money to get things back on track. Unfortunately, spending more money is like loading extra gold bullion onto a ship that's already holed below the waterline.

It's mainly a matter of pride. No one really wants to admit that a beloved brainchild has gone awry. Like a gambler on a losing streak, all but the most realistic of us will keep playing in the hopes of getting even.

The sunk cost fallacy is the reason why some organizations push new changes long after it becomes apparent that they will not make any substantive difference. SCF is why professional sports teams sometimes keep playing marginally performing stars with huge contracts instead of replacing them with potentially better, but lower paid players.

The sunk cost fallacy is how, for example, you can start with a $8.3 billion plan to build a space station and, after you've spent $100 billion, it's still not finished and probably won't work as originally envisioned when it is.

The kings of the SCF were WorldCom and Enron. Both companies were, for a while, at the top of their markets. However, as we found out later, they propped up their financial operations with schemes that might best be described as the corporate version of an M.C. Escher sketch where people climb endlessly up stairs in a circle. It makes for interesting art, but you cannot sustain the illusion in the real world.

And yet, even when it was apparent that things were going badly, WorldCom's chief executive officer, Bernard Ebbers, still managed to convince the WorldCom board of directors to lend

him $400 million to try and get things back on track.

The best ways to prevent sunk costs are to establish concrete, measurable benchmarks for any change. If you do not meet these benchmarks, do not spend any more money until you reassess what you are really trying to achieve and where your plans went awry. There has to be a benefit to going forward other than not wanting to admit failure or waste money already spent. We must be prepared to cut our losses if we can't meet our targets.

One good example of this was a government project to build an immense underground 54-mile ring particle accelerator under Waxahachie, Texas. After 14 miles of tunnels had been dug, Congress canceled the Superconducting Super Collider in 1993 due to cost estimates rising well beyond initial estimates. We may have spent $2 billion for a 14-mile hole in the ground, but at least we didn't spend $20 billion for a bigger one.

Closing Thoughts

In summary, here are my thoughts on firing silver bullets:

- Choose your ammunition carefully. Do not attempt to kill mosquitoes with a howitzer or elephants with a BB gun.
- Choose your target carefully. Some things that look enticing may prove to be bulletproof no matter how well you implement.
- Match your expectations of how long the change will take to the size of the change. If you intend to transform your entire organization, you should allow one year for every level in the organization between the person in charge and the lowest level employee.

A good example of this was the Defense Department's transformation to a joint environment. Congress passed the Goldwater-Nichols Act in 1986, and DoD completed most of the transformation 10 years later.

- Be ruthless. If an initiative is not meeting targets, either revise your expectations or kill the project.
- Do not turn people into targets for change. They tend to resent it and resist. Instead, give them weapons and turn them into shooters. The more people you have on your side firing in the same direction, the more likely it will be that your silver bullets will find their mark.

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.

CHIPS

"Big T" Hosts PEO EIS Working Group

By Mass Communications Specialist (SW/AW) Kelly Morgan

Supporting the Naval warfighter, the amphibious assault ship, USS Tarawa (LHA 1), hosted a working group conference Dec. 12, 2006, chaired by Rear Adm. Timothy Flynn, Program Executive Officer for Enterprise Information Systems (PEO-EIS).

Chief Petty Officer Nelson Mozzini, foreground, attached to Commander Amphibious Squadron One, explains the integration process between the Joint Operations Center and Combat Information Center to Rear Adm. Timothy Flynn, Program Executive Officer Enterprise Information Systems, right, background, and his team, aboard the amphibious assault ship USS Tarawa (LHA 1) in San Diego. U.S. Navy photo by Mass Communications Specialist Third Class (SW/AW) Kelly Morgan.

The PEO EIS team came aboard Tarawa to interact with the Naval warfighter and get honest feedback and suggestions from fleet Sailors on the PEO EIS product line. The team was very interested in seeing how their products that are currently deployed are put into play aboard a large deck "amphib."

Flynn currently oversees a portfolio of large-scale information technology projects and programs designed to enable common business processes and provide standard information technology capabilities to the Department of Navy. They include the Navy Marine Corps Intranet (NMCI), Navy Enterprise Resource Planning (ERP), Global Combat Support System-Marine Corps (GCSS-MC), Sea Warrior, Navy Standard Integrated Personnel System (NSIPS) and the Navy Manpower, Personnel, Training and Education (MPT&E) portfolio.

The admiral was accompanied by two Senior Executive Service personnel, engineering and acquisition staff and various program managers. Together, they toured the big deck "gator" lending their experience and support to Sailors and Marines along the way. In doing so, they engaged with the Office of the Chief of Naval Operations on the Next Generation Enterprise Network, the NMCI, in both CONUS and OCONUS implementations, pierside services and more.

"This visit provided a tremendous opportunity to meet an outstanding crew," Flynn said, in response to the ship's capabilities and manpower.

In reference to combat systems and combat readiness, the admiral asked about the services and systems the Space and Naval Warfare Systems Command (SPAWAR) currently provides to the fleet in comparison with the now outdated IT-21 program.

The admiral was very impressed with the knowledge of Tarawa's Sailors and the informative briefs that he received during his visit.

Prior to departing the Big T, Flynn expressed his appreciation to Tarawa's crew for their feedback during the team's visit.

For more information about the PEO EIS, go to the SPAWAR Web site at http://www.spawar.navy.mil and click on the PEO EIS seal. For more information about Tarawa, contact PAO@Tarawa.navy.mil.

CHIPS

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.

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.esi.mil/.

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.*** (W91QUZ-04-A-0002)
Ordering Expires: Upon depletion of Army Small Computer Program (ASCP) inventory
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Business Intelligence

Business Objects

Business Objects - Provides software licenses and support for Business Objects, Crystal Reports, Crystal Enterprise and training and professional services. Volume discounts range from 5 to 20 percent for purchases of software licenses under a single delivery order.
Contractor: ***EC America, Inc.*** (SP4700-05-A-0003)
Ordering Expires: 04 May 10
Web Link: http://www.gsaweblink.com/esi-dod/boa/

Mercury

Mercury Software - Provides software licenses, training, technical support and maintenance for Mercury Performance Center, Mercury Quality Center, Mercury IT Governance Center and Mercury Availability Center.

Contractor: ***Spectrum Systems, Inc.*** (SP4700-05-A-0002)
Ordering Expires: 21 Feb 09
Web Link: http://www.spectrum-systems.com/contracts-ESI.htm

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: 17 Dec 11
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Database Management Tools

Microsoft Products

Microsoft Database Products - See information under Office Systems on page 57.

Oracle (DEAL-O)

Oracle Products - Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers. Contact Navy project managers on the next page for further details.
Contractors:
DLT Solutions (W91QUZ-06-A-0002)
Mythics, Inc. (W91QUZ-06-A-0003)
Ordering Expires:
DLT: 31 Mar 07 (Call for extension information)
Mythics: 18 Mar 07 (Call for extension information)
Authorized Users: This has been designated as a DoD ESI and GSA SmartBUY contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Special Note to Navy Users: On Oct. 1, 2004, and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Sept. 30, 2013. The enterprise license provides Navy shore-based and afloat users to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations. Navy users in joint commands or supporting joint functions should contact the NAVICP Mechanicsburg contracting officer at (717) 605-3210 for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) San Diego DON Information Technology (IT) Umbrella Program Office.

The Navy Oracle Database Enterprise License provides significant benefits including substantial cost avoidance for the Department. It facilitates the goal of net-centric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

Programs and activities covered by this license agreement shall not enter into separate Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software and software maintenance that is acquired:

a. as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
b. under a service contract;
c. under a contract or agreement administered by another agency, such as an inter-agency agreement;
d. under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
e. by a contractor that is authorized to order from a Government supply source pursuant to FAR 51.101.

This policy has been coordinated with the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), Office of Budget.

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

IBM Software Products

IBM Software Products - Provides IBM product licenses and maintenance with discounts from 1 to 19 percent off GSA. On June 28, 2006, the IBM Rational Blanket Purchase Agreement (BPA) with immixTechnology was modified to include licenses and Passport Advantage maintenance for IBM products including IBM Rational, IBM Database 2 (DB2), IBM Informix, IBM Trivoli, IBM Websphere and Lotus software products.

Contractor: ***immixTechnology, Inc.*** (DABL01-03-A-1006); Small Business; (800) 433-5444
Ordering Expires: 26 Mar 09
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Management

CA Enterprise Management Software (C-EMS2)

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.*** (W91QUZ-04-A-0002); (800) 645-3042
Ordering Expires: Effective for term of the GSA FSS Schedule
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Citrix

Citrix - Provides a full range of Metaframe products including Secure Access Manager, Conferencing Manager, Password Manager, Access Suite & XP Presentation Server. Discounts range from 2 to 5 percent off GSA Schedule pricing plus spot discounts for volume purchases.

Contractor: ***Citrix Systems, Inc.*** (W91QUZ-04-A-0001); (772) 221-8606
Ordering Expires: 23 Feb 08
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

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); (980) 776-8283
Ordering Expires: 30 Jun 07
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

NetIQ

NetIQ - Provides Net IQ systems management security management and Web analytics solutions. Products include: AppManager; AppAnalyzer; Mail Marshal; Web Marshal; Vivinet voice and video products; and Vigilant Security and Management products. Discounts are 10 to 8 percent off GSA Schedule pricing for products and 5 percent off GSA Schedule pricing for maintenance.

Contractors:
NetIQ Corp. (W91QUZ-04-A-0003)
Northrop Grumman - authorized reseller
Federal Technology Solutions, Inc. - authorized reseller
Ordering Expires: 5 May 09
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

ProSight

ProSight - Provides software licenses, maintenance, training and installation services for enterprise portfolio management software. The software product provides the enterprise with a suite of solution specific applications for Capital Planning and Investment Control (CPIC) Budgeting (OMB 300/53); CPIC Process (Select/Control/Evaluate); IT Governance; FISMA (Federal Information Security Management Act) and Privacy Compliance; Project Portfolio Management; Application Rationalization; Research and Development (R&D) and Product Development; Asset Management; Grants Management; Vendor and Service Level Agreement Management; and Regulatory Compliance. ProSight products have been designated as a DoD ESI and GSA SmartBUY. The BPA award has been determined to be the best value to the government and; therefore, competition is not required for software purchases. Discount range for software is from 8 to 39 percent off GSA pricing, which is inclusive of software accumulation discounts. For maintenance, training and installation services, discount range is 3 to 10 percent off GSA pricing. Credit card orders are accepted.

Contractor: ***ProSight, Inc.*** (W91QUZ-05-A-0014); (503) 889-4813
Ordering Expires: 31 Dec 07 (Call for extension information. Currently in review for extension.)
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Quest Products

Quest Products - Provides Quest software licenses, maintenance, services and training for Active Directory Products, enterprise management, ERP planning support and application and database support. Quest software products have been designated as a DoD ESI and GSA SmartBUY. Active Directory Products only have been determined to be the best value to the government and; therefore, competition is not required for Active Directory software purchases. Discount range for software is from 3 to 48 percent off GSA pricing. For maintenance, services and training, discount range is 3 to 8 percent off GSA pricing.

Contractors:
Quest Software, Inc. (W91QUZ-05-A-0023); (301) 820-4800
DLT Solutions (W91QUZ-06-A-0004); (703) 709-7172
Ordering Expires:
Quest: 14 Aug 10
DLT: 31 Mar 07
Web Link:
Quest
https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-05-A-0023
DLT
https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-06-A-0004

Telelogic Products

Telelogic Products - Offers development tools and solutions which assist the user in automation in the development life cycle. The major products include DOORS, SYNERGY and TAU Generation. Licenses, maintenance, training and services are available.

Contractors:
Bay State Computers, Inc. (N00104-04-A-ZF13); Small Business Disadvantaged; (301) 352-7878, ext. 116
Spectrum Systems, Inc. (N00104-06-A-ZF31); Small Business ; (703) 591-7400
Ordering Expires: 29 Jun 07
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/telelogic/telelogic.shtml

Enterprise Resource Planning

Digital Systems Group

Digital Systems Group - Provides Integrated Financial Management Information System (IFMIS) software that was designed specifically as federal financial management system software for government agencies and activities. The BPA also provides installation, maintenance, training and professional services.

Contractor: ***Digital Systems Group, Inc.*** (N00104-04-A-ZF19); (215) 443-5178
Ordering Expires: 23 Aug 07
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/dsg/dsg.shtml

Oracle

Oracle - *See information provided under Database Management Tools on page 53.*

RWD Technologies

RWD Technologies - Provides a broad range of integrated software products designed to improve the productivity and effectiveness of end users in complex operating environments. RWD's Info Pak products allow you to easily create, distribute and maintain professional training documents and online help for any computer application. RWD Info Pak products include Publisher, Administrator, Simulator and OmniHelp. Training and other services are also available.

Contractor: ***RWD Technologies*** (N00104-06-A-ZF37); (410) 869-1085
Ordering Expires: Effective for term of the GSA FSS Schedule
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/rwd/rwd.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) 312-3905
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

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 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) 947-2059
BearingPoint (N00104-04-A-ZF15); (703) 747-5442
Computer Sciences Corp. (N00104-04-A-ZF16); (856) 252-5583
Deloitte Consulting LLP (N00104-04-A-ZF17); (703) 885-6428
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.esi.mil
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/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Securify

Securify - Provides policy-driven appliances for network security that are designed to validate and enforce intended use of networks and applications; protects against all risks and saves costs on network and security operations. Securify integrates application layer seven traffic analysis with signatures and vulnerability scanning in order to discover network behavior. It provides highly accurate, real-time threat mitigation for both known and unknown threats and offers true compliance tracking.

Contractor: ***Patriot Technologies, Inc.***
Ordering Expires: 4 Jan 11 (if extended by option exercise)
Web Link: http://www.esi.mil

Symantec

Symantec - Provides the full line of Symantec Corp. products and services consisting of over 6,000 line items including Ghost and Brightmail. Symantec products can be divided into eight main categories that fall under the broad definition of Information Assurance. These categories are: virus protection; anti-spam; content filtering; anti-spyware solutions; intrusion protection; firewalls/VPN; integrated security; security management; vulnerability management; and policy compliance. ***Notice to DoD customers regarding Symantec Antivirus Products:*** *A DoD Enterprise License exists for select Antivirus products through DISA contract DCA100-02-C-4049 found below.*
Contractor: ***immixTechnology, Inc.***
Ordering Expires: 12 Sep 10
Web Link: http://www.immixtechnology.com/esi/Symantec/ or http://www.esi.mil

Symantec Antivirus

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.esi.mil
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/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.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; and Gold Premium support contract/year (PSP), which includes six POCs.

Contractor: ***Government Technology Solutions*** (DCA100-03-C-4011)
Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.
Web Link: http://www.esi.mil
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/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Xacta

Xacta - Provides Web Certification and Accreditation (C&A) software products, consulting support and enterprise messaging management solutions through its Automated Message Handling System (AMHS) product. 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. Xacta's AMHS provides automated, Web-based distribution and management of messaging across your enterprise.

Contractor: ***Telos Corp.*** (F01620-03-A-8003); (703) 724-4555
Ordering Expires: 31 Jul 08
Web Link: http://esi.telos.com/contract/overview/

Office Systems

Adobe

Adobe Products - Provides software licenses (new and upgrade) and upgrade plans (formerly known as maintenance) for numerous Adobe and formerly branded Macromedia products, including Acrobat (Standard and Professional); Photoshop; Encore; After Effects; Frame Maker; Creative Suites; Illustrator; Flash Professional; Dreamweaver; Cold Fusion and other Adobe products.

Contractors:
ASAP (N00104-06-A-ZF33); Small Business; (800) 248-2727, ext. 5303
CDW-G (N00104-06-A-ZF34); (703) 621-8211
Softchoice (N00104-06-A-ZF35); Small Business; (703) 480-1957
Softmart (N00104-06-A-ZF36); Small Business; (610) 518-4192
Ordering Expires: 31 May 08
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/adobe-esa/index.shtml

Four Blanket Purchase Agreements (BPAs) provide both new and upgrade software licenses for Adobe products. These agreements also provide Adobe software upgrade plans, formerly known as maintenance agreements. The BPAs include software licenses formerly known under the Macromedia product brand. Products include: Acrobat (Standard and Professional); Photoshop; Encore; After Effects; Frame Maker; Creative Suites; Illustrator; Flash Professional; Dreamweaver; Cold Fusion; and other Adobe products.

iGrafx Business Process Analysis Tools - NEW!

iGrafx - Provides software licenses, maintenance and media for iGrafx Process 2005 and 2006 for Six Sigma and iGrafx Flowcharter 2005 and 2006.

Contractors:
Softchoice (N00104-06-A-ZF40); (703) 480-1972
Softmart (N00104-06-A-ZF39); (610) 518-4192
Software House International (N00104-06-A-ZF38); (304) 725-6110
Authorized Users: Open for ordering by all Department of Defense (DoD) Components, U. S. Coast Guard, NATO, Intelligence Community and authorized DoD contractors.
Ordering Expires: 16 Jul 08
Web Links:
Softchoice
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softchoice/index.shtml
Softmart
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softmart/index.shtml
Software House International
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/shi/index.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
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) 463-5325
Hewlett-Packard (N00104-02-A-ZE80); (800) 535-2563 pin 6246
Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638 or (312) 655-9167
Softmart (N00104-02-A-ZE84); (610) 518-4000, ext. 6492 or (800) 628-9091 ext. 6928
Software House International (N00104-02-A-ZE86); (732) 868-5926
Software Spectrum, Inc. (N00104-02-A-ZE82); (800) 862-8758 or (509) 742-2208
Ordering Expires: 30 Mar 07
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.shtml

Red Hat

Red Hat *(Netscape software formerly owned by AOL, not Linux)* - In December 2004, America Online (AOL) sold Netscape Security Solutions Software to Red Hat. This sale included the three major software products previously provided by DISA (Defense Information Systems Agency) to the DoD and Intelligence Communities through AOL. *Note: The Netscape trademark is still owned by AOL, as are versions of Netscape Communicator above version 7.2. Netscape Communicator version 8.0 is not part of this contract.*

August Schell Enterprises is providing ongoing support and maintenance for the Red Hat Security Solutions (products formerly known as Netscape Security Solutions) which are at the core of the DoD's Public Key Infrastructure (PKI). This contract provides products and services in support of the ongoing DoD-wide enterprise site license for Red Hat products. This encompasses all components of the U.S. Department of Defense and supported organizations that use the Joint Worldwide Intelligence Communications System (JWICS), including contractors.
Licensed software products available from DISA are the commercial versions of the software, not the segmented versions that are compliant with Global Information Grid (GIG) standards. The segmented versions of the software are required for development and operation of applications associated with the GIG, 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 GIG, GCCS or GCSS, you must contact one of the Web sites listed below to obtain the GIG 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.

GIG or GCCS users: Common Operating Environment Home Page
https://coe.mont.disa.mil
GCSS users: Global Combat Support System
http://www.disa.mil/main/prodsol/gcss.html

Contractor: ***August Schell Enterprises***
Ordering Expires: 06 Mar 07
Download provided at no cost.
Web Link: http://iase.disa.mil/netlic.html

Red Hat Linux

Red Hat Linux - Provides operating system software license subscriptions and services to include installation and consulting support, client-directed engineering and software customization. Red Hat Enterprise Linux is the premier operating system for open source computing. It is sold by annual subscription, runs on seven system architectures and is certified by top enterprise software and hardware vendors.

Contractor: ***DLT Solutions, Inc.*** (HC1013-04-A-5000)
Ordering Expires: 30 Apr 09
Web Link: http://www.dlt.com/contracts-Redhat-BPA.asp

WinZip

WinZip - This is an IDIQ contract with Eyak Technology, LLC, an "8(a)" Small Disadvantaged Business (SDB)/Alaska Native Corp. for the purchase of WinZip 9.0, a compression utility for Windows. Minimum quantity order via delivery order and via Government Purchase Card to Eyak Technology, LLC is 1,250 WinZip licenses. All customers are entitled to free upgrades and maintenance for a period of two years from original purchase. Discount is 98.4 percent off retail. Price per license is 45 cents.

Contractor: ***Eyak Technology, LLC*** (W91QUZ-04-D-0010)
Authorized Users: This has been designated as a DoD ESI and GSA SmartBUY Contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.
Ordering Expires: 27 Sep 09
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

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

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. BPA listed below.

Gartner Group (N00104-07-A-ZF30); (703) 378-5697; Awarded 01 Dec 2006
Ordering Expires: 30 March 08
Authorized Users: All DoD components. For the purpose of this agreement, DoD components include: the Office of the Secretary of Defense; U.S. Military Departments; the Chairman of the Joint Chiefs of Staff; Combatant Commands; the Department of Defense Office of Inspector General; Defense Agencies; DoD Field Activities; the U.S. Coast Guard; NATO; the Intelligence Community and Foreign Military Sales with a letter of authorization. This BPA is also open to DoD contractors authorized in accordance with the FAR Part 51.
Web Link: http://www.it-umbrella.navy.mil/contract/r&a/gartner/gartner.shtml

Records Management

TOWER Software

TOWER Software - Provides TRIM Context software products, maintenance, training and services. TRIM Context is an integrated electronic document and records management platform for Enterprise Content Management that securely manages business information in a single repository through its complete life cycle. The TOWER TRIM solution provides: document management; records management; workflow management; Web-based records management; document content indexing; e-mail management; and imaging. The DoD Enterprise Software Initiative (ESI) Enterprise Software Agreement (ESA) provides discounts of 10 to 40 percent off GSA for TRIM Context software licenses and maintenance and 5 percent off GSA for training and services.

Contractor: ***TOWER Software Corporation*** (FA8771-06-A-0302)
Ordering Expires: 17 Feb 08 (5 Dec 10 if extended by option exercise)
Web link: http://www.esi.mil

Section 508 Tools

HiSoftware 508 Tools

HiSoftware Section 508 Web Developer Correction Tools - Includes AccRepair (StandAlone Edition), AccRepair for Microsoft FrontPage, AccVerifyfor 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: 15 Aug 07
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 Expires:
Contract ordering for all new equipment purchases has expired. All Labor CLINS, Support Services and Spare Parts can still be ordered through 28 Jul 07.
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
Direct Ordering to Contractor
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:

Dell (N68939-97-A-0011); (800) 727-1100, ext. 7233795
GTSI (N68939-96-A-0006); (800) 999-4874, ext. 2104
Hewlett-Packard (N68939-96-A-0005); (800) 727-5472, ext. 15614
Ordering Expires:
Dell: 31 Mar 07 (Call for extension information)
GTSI: 31 Mar 07 (Call for extension information)
Hewlett-Packard: 07 May 07 (Call for extension information)
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:
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
http://www.it-umbrella.navy.mil/contract/tac-solutions/HP/HP.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) 225-2600; Awarded 7 May 97

Ordering Expires: 31 Mar 07 (Call for extension information)

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:

Centurum Information Technology, Inc. (Small Business) (N00039-98-A-3008); (619) 224-1100; Awarded 15 Jul 98

Lockheed Martin (N68939-97-A-0017); (703) 367-3407; Awarded 1 Jul 97

Northrop Grumman Information Technology (N68939-97-A-0018); (703) 413-1084; Awarded 1 Jul 97

SAIC (N68939-97-A-0020); (703) 599-0140; Awarded 1 Jul 97

Ordering Expires:
Centurum: 14 Jul 07 (Call for extension information)
Lockheed Martin: 30 Jun 07 (Call for extension information)
Northrop Grumman IT: 11 Feb 07 (Call for extension information)
SAIC: 30 Jun 07 (Call for extension information)

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

Web Links:
Centurum
http://www.it-umbrella.navy.mil/contract/itss/centurum/itss-centurum.shtml
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

New Enterprise Software Agreement!

Enterprise Application Integration

BEA - NEW!

BEA Products - Supplies integration and service-oriented architecture (SOA) software including: BEA WebLogic Server; BEA WebLogic Portal; BEA WebLogic Integration; BEA WebLogic Workshop; BEA JRockit; BEA AquaLogic; BEA Tuxedo and other BEA products.

Contractors:
CompSec (Computer Security Solutions, Inc.) (N00104-07-A-ZF43); Small Business; (703) 917-0382
immixTechnology, Inc. (N00104-07-A-ZF41); Small Business; (703) 752-0659
Merlin International (N00104-07-A-ZF42); Small Business; (703) 752-8369

Ordering Expires: 19 Dec 09

Web Links:
CompSec
http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/CompSec/index.shtml
immixTechnology
http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/immix/index.shtml
Merlin International
http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/Merlin/index.shtml

The DON IT Umbrella Program Team offers great customer service!

Visit us on the Web

DON IT Umbrella site: www.it-umbrella.navy.mil

ITEC Direct e-Commerce site: www.itec-direct.navy.mil

DoD Enterprise Software Initiative site: www.esi.mil

DON IT
umbrella program

You are invited to the
DON IM and IT Conference

Department of the Navy Information Management and Information Technology

Hosted by the Department of the Navy Chief Information Officer (DON CIO)

18-20 June 2007

Virginia Beach Convention Center, Virginia Beach, VA

The DON IM and IT Conference provides a venue to share information about the latest DON IM and IT initiatives, policy and guidance. Conference topics include:

- Certification & Accreditation
- Critical Infrastructure Protection
- Data Management
- DON IM/IT Civilian Workforce
- DON IT Umbrella Program
- Enterprise Architecture
- Enterprise Software/IT Asset Management
- FISMA
- Information Assurance
- IT Performance Measurement
- Knowledge Management in Support of the Warfighter
- Privacy
- Public Key Infrastructure
- Service Oriented Architecture
- Strategic Management of the Electromagnetic Spectrum
- Telecommunications
- USMC Civilian ITM Community of Interest
- WiMAX
- Wireless
- World Radio Conference 2007

The DON IM and IT Conference will be open to all DON, government, military and support contractor attendees. No conference fee will be assessed, but registration is required.

The agenda and registration are available on the DON CIO Web site at http://www.doncio.navy.mil. For additional information call (703) 602-6274 or (703) 607-5650.

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

PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND ADDITIONAL
MAILING OFFICE
SSC CHARLESTON
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988