

Sharing Information - Technology - Experience

CHIPS



JULY - SEPTEMBER

M a g a z i n e

2 0 0 8

Testing - Training - Modeling - Simulations - Experimentation - Exercises -
Peacekeeping - Deterrence - Maritime Security Operations



CHIPS July – September 2008

Volume XXVI Issue III

Department of the Navy Chief Information Officer
Mr. Robert J. Carey

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

Space & Naval Warfare Systems Center Charleston
Commanding Officer Captain Bruce Urbon



Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Layout and Design
Sharon Anderson

Web support: Deborah Midyette
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: 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.

Features



Commander, Air Force Cyberspace Command (Provisional) Maj. Gen. William T. Lord talks about the AFCYBER mission and operations, the importance of dominance in cyberspace and progress to date in phase one of AFCYBER's stand up slated for Oct. 1, 2008.

Deputy Director U.S. Second Fleet Combined Joint Operations from the Sea Center of Excellence Royal Navy Commodore R.J. Mansergh discusses the CJOS COE's mission to help NATO transform into a more agile and responsive alliance, capable of supporting the full range of operations, which may be required to counter the new security threats and challenges of the 21st century.



Commander Nassau Expeditionary Strike Group Capt. Robert G. Lineberry talks about the power of international partnerships, training with coalition forces and the strike group's participation in coalition exercises in support of maritime security operations for 5th and 6th Fleet commanders.

The military men and women of NSWC Dam Neck, Va. As one of the Naval Sea Systems Command's warfare centers, NSWC Dam



Neck engineers C5I systems for a net-centric force and builds relationships with key partners to deliver capabilities to the fleet.

Navigation Guide

- 4 Editor's Notebook
- 5 From the DON CIO Robert J. Carey
- 6 Interview with Air Force Maj. Gen. William T. Lord
AFCYBER (Provisional) Commander
- 10 Q&A with Royal Navy Commodore R. J. Mansergh
Deputy Director, U.S. Second Fleet Combined Joint Operations from the
Sea Center of Excellence
- 12 Collaboration and Connectivity for the Warfighter – JEFX 08-3
Navy leverages Air Force experiment to focus on command and control
- 14 Phoenix Express 2008 – U.S. and coalition partners demonstrate a
multinational commitment to maritime security in the Mediterranean
- 17 Focus on Nassau Expeditionary Strike Group
*Coalition Forces Complete Goalkeeper III Exercise
Coalition comes together to complete disaster relief training*
- 18 U.S., Pakistan Forces Complete Inspired Union 2008
- 20 NSWC Dam Neck — Face to the Fleet
Engineering C5I capabilities for a net-centric force
- 22 FROST– Future Readiness and Optimized Scheduling Tool
- 23 Navy Reestablishes U.S. 4th Fleet
- 24 Strike Force Interoperability – Navy officers and government engineers
ensure combat systems are strike group ready and surge capable
- 25 ASDS – Advanced Sensor Distribution System
A digital, real-time, efficient and cost-effective sensor distribution method
- 26 NSWC Dam Neck Awarded Wireless Grants
Improving battlefield command and control communications
- 28 Remote Monitoring – SWE improves equipment operating condition
feedback to support fleet readiness
- 29 CWID Answers the Call for Future Capabilities
- 30 A Trident Warrior 08 Journal – A SITREP by the deputy director of TW08
- 34 The Maturation of Cyber Crime: It's a Job – Cyber crime is fast-growing and
lucrative ... and increasingly easier using sophisticated automated tools
- 37 DICE – DoD's Interoperability Communications Exercise – *If you aren't
prepared — you're rolling the dice*
- 40 Navy ERP Achieves Initial Operational Capability
- 41 Department of the Navy Architecture Federation Pilot
- 43 Navy transitions to Wideband Global System
- 44 Key tactical data link systems clear operational testing and prepare for
introduction to the fleet
- 45 Records Management Tool Aids Disposition Decisions
LIFELines
- 46 Solar flares and their effect on DoD equipment
- 48 Benefits gained from Combined Endeavor 2008 as varied as the nations
involved
- 50 Work continues on multinational common operating picture at CE 08
- 51 Military Coalition Frequency Management
- 52 C4I Project Management in U.S. Forces Korea
- 54 The Army's Central Technical Support Facility – *Ensuring system integration
and interoperability to meet warfighter needs*
- 56 Commander Second Fleet Implements ITIL – *Customer focus and continuous
process improvement lead to effective management of Navy networks*
- 57 Create a Digital Dashboard to Share Management Information
- 58 NAVYForMoms.com
- 59 SPAWAR Employees 2008 Winners of the Dr. Delores M. Etter Top Scientists
and Engineers Award
SSC Charleston's 2008 Top Navy Engineer
- 60 SSC San Diego's 2008 Top Scientists, Engineers and "Emerging Innovators"
- 63 Fleet Readiness Center Southwest Lauded for Energy Saving Programs
- 64 Hold Your Breaches! – *Case stories of real privacy breaches in the Navy*
- 65 CNO Visits MRAP Facility at SSC Charleston
- 66 The Lazy Person's Guide to Botnets
- 69 Under the Contract

Cover - MEDITERRANEAN SEA (April 17, 2008) Members of the visit, board, search and seizure (VBSS) team from the guided-missile frigate USS John L. Hall (FFG 32) approach landing craft utility (LCU 1661) in a rigid hull inflatable boat during a Phoenix Express (PE 08) training exercise. PE 08 is the third annual exercise in a long-term effort to improve regional cooperation and maritime security to increase interoperability by developing individual and collective maritime proficiencies of participating nations, as well as promoting friendship, mutual understanding and cooperation. U.S. Navy photo by Mass Communication Specialist 2nd Class Amanda Clayton.

Editor's Notebook

Can you guess what the focus is for this issue by looking at the interlocking circles on the cover? Capt. Jon Greene, commanding officer of NSWC Dam Neck gave me the idea. He said that relationship building and working cohesively with partners is one of his most important objectives, and for many effective leaders, this is true. He also credited CHIPS with being a useful channel to connect Navy and Defense Department users and leaders for that relationship building that is so important for any project to succeed.

It's a great compliment and one that illuminates how the Navy and joint force work every day partnering and building relationships with each other, as well as with other government agencies, nongovernment agencies and coalition friends, in experiments, exercises and training events.

"Think of the potential when we start saying, I am working on this and you are working on something very similar, what's the best of breed? Where can we do better for the warfighter and the taxpayer?" Greene said.

To that end, we explore the power of partnerships with a look at NSWC Dam Neck; Phoenix Express; DoD's Interoperability Communications Exercise (DICE); Joint Expeditionary Force Experiment 2008-3 (JEFX 08-3); Trident Warrior 2008; Coalition Warrior Interoperability Demonstration (CWID); and Combined Endeavor. You will see how building relationships and working together through training, exercises and experiments are essential to mission preparation and execution.

In June, the CHIPS staff participated in the DON CIO's exhibit at the Joint Warfighting Conference which was held at the same time and location as the DON IM/IT Conference in Virginia Beach, Va. If you didn't attend, you missed a marvelous opportunity to connect with technology and acquisition professionals and leaders across government, academia and industry.

DON IM/IT Conference sessions, led by subject matter experts, were informative and provided a forum for serious discussion on the Department's IT programs and policies.

The next DON IM/IT Conference will be held in San Diego, Calif., Feb. 9-12, 2009. Go to the DON CIO Web site for more information at www.doncio.navy.mil.

Welcome new subscribers!

Sharon Anderson



Personnel Specialist 2nd Class Jeffrey Brawler, Lt. David McKenney and Yeoman 1st Class Vivian Favors from the Expeditionary Combat Readiness Center exhibit assistance tools for Sailors serving as individual augmentees (IA) at the Joint Warfighting Conference. IAs are administratively assigned to ECRC during their expeditionary tour. ECRC has access to a diverse network of resources and programs that were set in place to assist IA Sailors and their families. For more information, go to the ECRC Web site at www.ecrc.navy.mil.



Panelists from the Joint Warfighting Conference discussion on *How Can We Fix the Defense Acquisition Process? Using IT as a Case Study*: the Honorable Jacques S. Gansler, former Under Secretary of Defense for Acquisition, Technology and Logistics; Mr. Robert J. Carey, Department of the Navy Chief Information Officer; Lt. Gen. Jeffrey A. Sorenson, Army CIO/G-6; and Mr. James P. Craft, deputy director C4 and deputy CIO for the Marine Corps. The Joint Warfighting Conference is co-sponsored by AFCEA International and the U.S. Naval Institute. The DON IM/IT Conference, sponsored by the DON CIO, was held at the same time and location as the Joint Warfighting Conference in June in Virginia Beach, Va.

Correction: The name of Capt. Mark Kohlheim, commanding officer of Space and Naval Warfare Systems Center San Diego, was misspelled in a picture caption in the Editor's Notebook column in the last issue of CHIPS. Our apologies to Capt. Kohlheim.



D O N C I O

Putting information to work for our people

My office hosts the Department of the Navy (DON) Information Management/Information Technology (IM/IT) Conferences to coincide with the co-sponsored AFCEA International and U.S. Naval Institute conferences in San Diego and the Norfolk area. The West Coast conference held in February was a tremendous success as was the most recent East Coast event in June 2008. I spoke at the IT workforce town hall meeting at the DON IM/IT Conference and participated in a panel discussion at the AFCEA/USNI Joint Warfighting Conference, both held at the same time and location in Virginia Beach.

The DON IM/IT Conferences provide a venue where the entire Department, including military, civilians and support contractors, can hear the latest information on key IM and IT initiatives. We conducted more than 30 sessions on topics that ranged from "Electromagnetic Spectrum: Why Should I Care?" to "Identity Theft and How to Protect Your Privacy Information." Our sessions are geared toward anyone in the DON who uses IT, so that would include virtually everyone in the Department. The sessions draw an audience of committed people from throughout the DON who are interested in learning what they need to know to better perform their jobs and ultimately, better support the warfighter.

At the town hall, questions were raised about the future of the IT workforce as well as skills needed to remain competitive and current within our ever-changing world of IT. Specific to the questions was the recurring theme of Web 2.0. These technologies can be important tools, enabling sharing and collaboration to deliver secure, actionable information supporting agile decisions. Just as our naval workforce is already exploring the impact of new technologies on accomplishing our mission in exercises such as Trident Warrior, the Department must harness the potential of Web 2.0. Today's joint decision making will require our use of collaboration to be successful.

My staff worked really hard to present topics they thought would be of most value to the Department at large. Based on the number and engagement of attendees, I think they did a good job of determining those hot topic areas. Realizing that subject matter expertise in many areas resides outside the DON CIO, we invited SMEs from various Navy and Marine Corps commands and the Defense Department to participate as speakers and share their experience and knowledge.

The synergy created by holding the DON IM/IT conferences at the same time and location as the AFCEA/USNI conferences is remarkable. While our sessions are focused on IT issues and initiatives that are relevant to the DON, the AFCEA/USNI sessions, which are also open to DON attendees, focus on the bigger joint picture. The speakers include leaders from all the services, representing their services and joint commands.

Our DON IM/IT Conference attendees were welcome to browse the Joint Warfighting exhibit hall and see technology presented by hundreds of industry, Navy, Marine Corps and DoD exhibitors. I had a chance to visit some of these exhibits and while I enjoyed my discussions with industry partners, I was most impressed by two young winners of the 2008 AFCEA National High School Science Fair Award. They represent the innovative minds of this great nation and were motivated solely by the ability to solve a problem and make a difference. It is this type of drive that we also see in our Navy and Marine Corps team which makes them the finest in the world.

This CHIPS issue encompasses the importance of training with new technologies, experimentation and mission preparation. The June conference was an example of all of these areas in action. New technologies and experimentation were discussed during the sessions and on display in the exhibit hall, with the overarching goal of mission preparedness and working jointly with the other services, government agencies, non-government agencies and with coalition partners.

The importance of being prepared for the variety of missions that the Navy is called on to do cannot be overstated. Daily, the Navy and Marine Corps perform humanitarian assistance, maritime security operations, homeland security and defense, and peace-keeping — globally and at home — working with many organizations and nations. Information technology provides the basis to enable mission success. Training and experimentation in support of these missions are fundamental to our national security and economic prosperity.

Continuously learning and keeping up with technology will benefit the DON as we move forward in this 21st century warfighting environment. CHIPS magazine and our DON IM/IT Conferences will continue to provide a venue to share information, technology and experience.

Robert J. Carey



DEPARTMENT OF THE NAVY - CHIEF INFORMATION OFFICER

W W W . D O N C I O . N A V Y . M I L

Interview with Air Force Maj. Gen. William T. Lord

AFCYBER (Provisional) Commander

Maj. Gen. William T. Lord is commander, Air Force Cyberspace Command (Provisional). He is responsible for establishing cyberspace as a domain in and through which the Air Force flies and fights, to deliver sovereign options for defense of the United States. AFCYBER signals the beginning of equipping and organizing a new breed of warrior, that being Air Force cyber warriors, to dominate the cyber domain. One of the key enablers to fully standing up AFCYBER will be the staff's ability to leverage and enhance the existing command and control concepts of operations and capabilities of other Air Force major commands and Defense Department services and agencies. The planned date for phase one of the AFCYBER stand up is Oct. 1, 2008.



Maj. Gen. William T. Lord

AFCYBER (Provisional) was activated Sept. 17, 2007, at Barksdale Air Force Base, La. The need is urgent, so in 2003, the White House issued "The National Strategy to Secure Cyberspace," part of an overall effort to protect the nation against cyber threats. The strategy presents cyberspace security as a subset of homeland security and defines a wide range of initiatives to "protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States."

One of those initiatives calls for the government to "improve coordination for responding to cyber attacks within the U.S. national security community." According to "The National Strategy to Secure Cyberspace," "a spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security."

In this regard, AFCYBER will act as both a deterrent and a combatant to safeguard the nation's cyber structure.

Gen. Lord and his staff are working many of the items needed for initial operations capability including: establishing a budget, articulating details of organizational realignments, developing and assigning manpower requirements, and establishing policies and procedures for daily operations. Many of these details are either still being defined or are under review.

CHIPS spoke with Maj. Gen. Lord May 5, 2008.

CHIPS: When the Secretary of the Air Force announced the stand up of the Cyberspace Command in 2005; many saw it as a bold move into new ground. Do you think that AFCYBER will serve as a blue print to other defense and federal organizations in regard to offensive, tactical use of the cyber domain?

Maj. Gen. Lord: I hope we can be a blueprint for other defense and federal organizations as a virtual organization. We can show other elements of government how we can operate from about a dozen different locations — a major air command headquarters and a couple hundred people with four wings assigned to us all over the United States — and not have laid one brick for any brick and mortar construction.

I think that could be a great example. We have talked to Naval Network Warfare Command and the Army's NETCOM because they have been established longer than we have.

CHIPS: Will you be working with the Army and Navy?

Maj. Gen. Lord: At the operational level, there is not a huge overlap, but we all provide forces for U.S. Strategic Command. Our work with other services has been more administrative than operational, to date.

CHIPS: I read that AFCYBER is going to be more of a tactical command, taking on the offensive approach to network operations.

Maj. Gen. Lord: The work of an AF MAJCOM is the organizing, training and equipping of forces ... not tactical operations. As

the operator of the AF portion of the network, I believe the majority of that work is in the defensive business. One of the reasons that the Air Force decided to stand up this capability is because of the Air Force's dependence on technology in command and control of our own forces.

If you are flying a Predator from Las Vegas over Afghanistan, that is a thin command and control link. We want to make sure that we are not just assuming that it will always be there but have the ability to defend it.

Offensive capabilities, that is force employment, belongs to combatant commanders. We, as the Air Force, don't do that; we give forces to U.S. Strategic Command for employment. Principally, we're an 'organize, train and equip' command. We will be educating those young people to be able to do both (offensive and defensive), but in the employment mode, they don't belong to us.

CHIPS: There is speculation in the trade press that the Air Force stood up AFCYBER to prepare for cyber conflicts with China, given that many attacks against U.S. government networks come from the Chinese mainland.

Maj. Gen. Lord: I have read the same stories, but I don't believe that they are completely correct. It is really about the Air Force's dependence on cyber and our ability to defend our own command and control, so that we can continue to operate in the joint fight as the COCOM wishes.

Clearly, there are nation-states that are developing this capability, but a 12-year-old kid in the Philippines wrote malicious

software code that froze the world's economy for a day and a half. It's cyber criminals, cyber terrorists, and potentially nation-states, but this AF initiative isn't because of one nation-state.

CHIPS: AFCYBER will apply the Laws of Armed Conflict, which include rules of engagement, delivering proportional responses to attacks and observing distinctions between combatants and civilians. This can be a gray area when attacks may come from civilians acting under state sponsorship. Have the Laws of Armed Conflict been clearly defined to allow you to operate tactically as well as defensively?

Maj. Gen. Lord: I think they are, however, when that begins to go over into commercial systems, the Internet, for example, now we are not so sure. As we apply the rules of engagement to kinetic weapons, we must do so with the same due diligence with non-kinetic weapons — same rules — and they already exist.

CHIPS: You've been quoted as saying that future conflicts will be fought in the electromagnetic spectrum and in non-kinetic ways. Do you think the U.S. may be lagging behind in what rogue nations and non-state players are already doing in cyberspace?

Maj. Gen. Lord: I don't think we are lagging; the trouble is the price of admission into this kind of conflict is low. When it's the price of a computer and a network connection, our adversaries don't have to have a large offensive army, navy, marine corps or air force. Whether a nation-state or a bunch of criminals, they can attack asymmetrically. We need to have the same capability, and we need to have the ability to counter those kinds of things. You have to stay nimble.

CHIPS: Many have said that we are already engaged in cyber warfare and claim that it is the Cold War of the 21st century.

Maj. Gen. Lord: We are attacked all the time, whether it is a malicious attack or a device coming up on the network that we haven't ever seen before, and we have to figure that out and identify it. We have no way of knowing if it's a new device on the network that is attempting to ping other devices or if it's somebody attempting to penetrate a network.

You have to respond to all those very quickly and in a manner such that you don't assume that it's always just another device trying to come up in the network when maybe it's not.

Is that warfare? No, but if you are on the inside watching somebody trying to ping your network, you consider it warfare until you figure it out.

CHIPS: Is AFCYBER's role duplicative in terms of what the National Security Agency and Department of Homeland Security do to protect the homeland's information infrastructure?

Maj. Gen. Lord: The Air Force Cyberspace Command role is principally aimed at the Air Force. NSA, DHS, the Department of Justice and the Department of Defense all operate under different titles of U.S. Code: Title 50, Title 10, Title 18, and potentially Title 32, and many different activities, and we have great relationships between us, but what we need are the processes that allow us to exchange information more quickly.



Maj. Gen. William T. Lord, AFCYBER (P) commander, meets with communications troops who helped to install the Air Force's newest Area Processing Center at Andrews Air Force Base, Md. The APC consolidates e-mail, file sharing and many other data and information services for more than 160,000 Air Force workers. The general greets SSgt. Christopher Newbill, Senior Airman Sean Manning, Airmen 1st Class Taji Eggleston and Brenden Maloy. Photo by Senior Airman Steven Doty, 316th Wing public affairs.

CHIPS: Does AFCYBER have a permanent location yet? I've read that states from Louisiana to Maine are vigorously lobbying to have AFCYBER located within their borders.

Maj. Gen. Lord: No. We haven't completed the analysis on that and don't expect to announce a location until late 2009. When we stand up in October, it will be in the provisional location in Louisiana. As a virtual organization, we will be at about 12 operating locations throughout the United States. We exist where the expertise exists today.

CHIPS: Have you had a typical day at AFCYBER yet?

Maj. Gen. Lord: No, I don't think there is one yet. In the development of a new organization we have a lot of questions to answer such as what units will be assigned, how to develop the manpower, what are the skills we need to teach to cyber warriors of the future, and what courses do we need for the 'old warriors' that need to be re-crafted.

Some things we do are changing our culture, while some of it is just the mechanics of how you build a budget, for example. Every day is a new adventure.

There are those who think it will be a great capability ... while some are still hesitant.

CHIPS: Why is that?

Maj. Gen. Lord: It is mostly about change. Change is hard, and that's why it's so important that we have such great standard-bearers in the Chief of Staff of the Air Force and in the Secretary of the Air Force, who are pushing the institution to create this capability.

It's not as if we are new in the cyber business; we have been doing it awhile. The reason to stand up the command is to focus



Electronic warfare officers, Lt. Col. Tim Sands, 53rd Electronic Warfare Group AF-CYBER Transition Team Chief, Capt. Jon Smith, 36th Electronic Warfare Squadron Suppression of Enemy Air Defenses test director and Lt. Col. John Arnold, 36th Electronic Warfare Squadron commander in the Central Control Facility at Eglin Air Force Base April 16. Photo by Capt. Carrie Kessler 53rd Wing public affairs.

mass and energy at the resource problem. We have been doing this in pockets all over the Air Force for a long time; it really is to get it all organized under one command.

CHIPS: What progress have you made thus far in making AFCYBER fully operational?

Maj. Gen. Lord: We now have a strategic vision published, manpower documents built, and we have Air Force doctrine in cyber that's going through the coordination stage. We have ensured that there are cyber activities happening in every one of our major exercises throughout the Air Force.

We are building the budget and collecting it from already existing Air Force programs, which amount to between \$5 billion and \$6 billion. We have had a lot of positive movement in a short time to do the organizing, training and equipping so that our Air Force command and control systems are protected. We have trained forces to give to combatant commanders to execute whatever it is they need to execute during their operations.

CHIPS: Do you have staffing levels set yet?

Maj. Gen. Lord: For the headquarters itself, it is about 400 to 500 people spread between 12 locations. When you add the wings, some of which already exist today, it brings the total to a little over 8,000 people.

CHIPS: Can you envision what a typical day at AFCYBER will be like once you are fully operational?

Maj. Gen. Lord: From the standpoint of an AF MAJCOM, it's mostly finding the resources to make sure there's enough manpower, money and training to do what we need to do because MAJCOMs don't fight battles — other than budget battles.

We will be fighting for the resources to make sure that operational wings can perform their combat missions. The operational wings will be doing electronic warfare, network attack, network defense and exploitation, and watching directed-energy weapon development and information operations.

At the major command level, it involves mostly resources policy to support those operational units. That's no different than what the other 10 Air Force major commands do.

CHIPS: Will warfighters on the ground be able to call on AFCYBER for air cover or electronic warfare assets?

Maj. Gen. Lord: Yes, and they do that through a combatant commander, who is either a theater combatant commander, like U.S. Central Command, or global commanders that provide regional flex, like U.S. Strategic Command.

In the case of jamming, it could be airborne jammers, it could be space-borne jammers, or it can be jamming provided by a cyber effect. The integration of all the air, space and cyber capabilities is to create an effect to destroy the enemy's capability or render it unusable.

At the operational unit, Airmen — men and women — would be tasked to do that. Those taskings come through the combatant commanders, not through me as a resource provider.

CHIPS: Can you talk about the skill sets of your staff?

Maj. Gen. Lord: It's everything from the men and women who establish this domain, the communications, the radar, or the tactical airborne data link folks that establish the domain or use the domain, to the folks who pay attention to router switches and hubs.

It can be our network attackers, our network defenders or our electronic warfare officers. It also includes influence operations, such as behavioral scientists, cultural linguists, psychologists and psychiatrists, for example.

There are many different skills, not just computer skills or electrical engineering skills. If we are changing the nature of warfare — and it is about changing the behavior of an enemy — we don't have to do that with a 2,000-pound bomb. Perhaps we can do that with a message.

CHIPS: Will AFCYBER be issuing policy and monitoring networks, combat systems and the command and control structure?

Maj. Gen. Lord: Yes, there is a direct correlation to what NETWARCOM does and what we will do for the Air Force. Terrestrial networks and airborne networks will be our responsibility.

CHIPS: Will this include the Air Force's shore infrastructure?

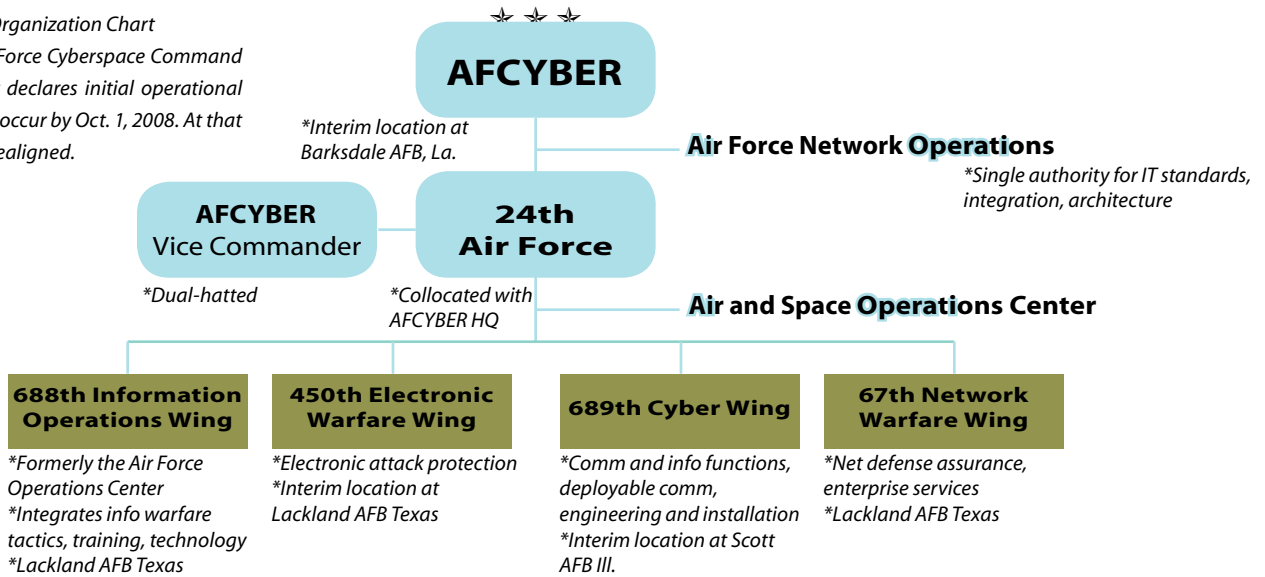
Maj. Gen. Lord: Yes, I think the Navy does that under the contract with Navy Marine Corps Intranet, and that is done differently in the Air Force. We have a common configuration for desktops. There are use licenses that we buy from Microsoft. We do asset visibility and push out patches to maintain both the network fixes and the vulnerabilities. Most places do that routinely every day. We will monitor that activity from AFCYBER for the entire Air Force.

Units currently receive policy doctrine direction from the Commander of Air Force Network Operations, which resides under 8th Air Force. Their policies cross all commands. That will change Oct. 1, and AFNETOPS will be in Air Force Cyberspace Command.

CHIPS: AFCYBER is a great recruiting tool for young adults. It's a domain they grew up in. Next to the thrill of being an Air Force pilot, being a cyber warrior sounds like an amazing adventure.

Proposed Organization Chart

**This is what the Air Force Cyberspace Command will look like when it declares initial operational capability, which will occur by Oct. 1, 2008. At that time all units will be realigned.*



Maj. Gen. Lord: Many of them bring high-tech skills, and we want to bring them to a high-tech organization. The matching of those skills is important, and we are getting a lot of response.

There is a cyber awareness ad that the Air Force has been airing on television since 'March Madness.' The Air Force also aired ones about intelligence, surveillance and reconnaissance, and space-related specialties as well.

We have developed a career field roadmap that will map today's specialties into tomorrow's cyber specialties. Young men and women, enlisted and officers, will have cyber careers.

CHIPS: The Navy consolidated ratings to develop the information systems technician rating and created information professional officers to meet the challenges of changing technology. Has the Air Force looked at its personnel structure in this regard?

Maj. Gen. Lord: We are driving that consolidation, and recently the Secretary of the Air Force signed a roadmap that gives us a 10-year plan for how we will develop our forces. Our officers assigned in this 'domain' will be cyberspace operations officers.

CHIPS: Will they do the same things that IPs do in the Navy?

Maj. Gen. Lord: It will be bigger than just IT because it involves electronic warfare and directed energy. It also consists of work not normally included in the communications and information career fields, which is what I would have called it in the old days in the Air Force.

The enlisted personnel get mapped into cyber operations, cyber maintenance and some of those are the more traditional skills, like ETs, electronics technicians in the Navy. In this business there will also be enlisted offensive operators which will be unusual for the Air Force.

CHIPS: How is it unusual?

Maj. Gen. Lord: In the Air Force, most of our people who are providing kinetic options, that drop the bombs, are officers flying aircraft. In the network attack business, it can be officers and enlisted personnel.



- AFCYBER proposes to be the lead command for:
- network defense;
 - warfare support and exploitation;
 - computer security issues (information assurance);
 - network attack;
 - electronic warfare and directed energy;
 - Information Operations;
 - overall network operations;
 - global command and control integration;
 - expeditionary (deployable) communications networks such as satellite communications (not to include satellite control or missile warning networks);
 - data links;
 - electromagnetic spectrum operations;
 - data integration, common communication and information functions;
 - engineering and installation of communications support; and
 - electronic maintenance and evaluations such as satellite communications, weather radar, cryptological, air traffic control and landing systems and network infrastructure.

– www.afcyber.af.mil

For more information about Air Force Cyberspace Command, go to www.afcyber.mil.

*Q&A with Royal Navy Commodore R. J. Mansergh
Deputy Director, U.S. Second Fleet
Combined Joint Operations from the Sea Center of Excellence*

Commodore Bob Mansergh is the deputy director of 2nd Fleet's Combined Joint Operations from the Sea Center of Excellence (COE). In his varied and distinguished naval career, he has commanded two nuclear attack submarines, HMS Trafalgar and HMS Tireless, as well as taking on the role of teaching future submarine commanding officers as the prospective CO instructor — known in the Royal Navy as "Teacher."

No stranger to the USA, Commodore Mansergh deployed to U.S. Central Command in late 2002, as the deputy director of a newly-formed Operation Enduring Freedom coalition planning and assessment team, tasked to provide advice to U.S. commanders on long-term strategy in Afghanistan and East Africa.

As leader of the team responsible for strategic planning in East Africa, the commodore was honored to represent the United States at the G-8 Africa Experts' meeting in Washington D.C., in October 2004. He has taken a keen interest in all aspects of military strategy development since.

Commodore Mansergh took over his current role as the deputy director of the Combined Joint Operations from the Sea Center of Excellence (CJOS COE) in August 2007. The CJOS COE is one of 19 Centers of Excellence established to help NATO transform into a more agile and responsive alliance, capable of supporting the full range of operations which may be required to counter the new threats and security challenges of the 21st century.

To optimize transformation, member nations agreed to take advantage of national and multinational COEs that provide opportunities to enhance education and training; improve interoperability and capabilities; assist in doctrine development and/or test and validate concepts through experimentation.

In a visit to observe 2nd Fleet's simulation of portions of a Maritime Headquarters with Maritime Operations Center (MHQ with MOC), during its participation in the Air Force's Joint Expeditionary Force Experiment 2008-3 (JEFX 08-3) in April, the CHIPS staff met briefly with the commodore.

Commodore Mansergh: Joint Expeditionary Force Experiment 08-3 has been a great opportunity for Second Fleet elements to work with the U.S. Air Force, in particular, experimenting on various Maritime Headquarters with Maritime Operations Center procedures, which need to be 'teased' through before the center becomes operational later this year.

It has also given the U.S. Navy, through the Second Fleet headquarters, a good chance to look at the interfaces at the operational level with the other services and at the needs of coalition partners, in this case, the United Kingdom, Australia and Canada. All three have been represented at the Combined Air and Space Operations Center at Langley [Air Force Base, Va.].

The experiment has tested a range of capabilities, not only technical systems solutions (and there has been a lot of that, and I have experienced some of that personally, and it is certainly a step way ahead of what most countries already have in place), but also the procedural aspects and the information sharing aspects which are particularly important for the United States in developing the 'Global Maritime Partnership' which is underpinning the latest U.S. Navy, U.S. Marine Corps, U.S. Coast Guard Strategy for 21st Century Seapower. ["A Cooperative Strategy for 21st Century Seapower"]

The scenario for the experiment has been a fictitious island divided into three countries and represents what I think is quite a good view of the future challenges we face with global resource shortages. The cause of the conflict on which the experi-



Commodore Bob Mansergh

ment focuses has primarily been disagreements between the nations over the rights to mineral resources in a mineral field which spans the border of two different countries.

Some of the aspects of the scenario have been optimized heavily towards the air battle, which is not surprising because 10 of the 13 individual experiments in JEFX 08-3 have been Air Force experiments, a lot of them to do with targeting and the procedures to manage multiple different sources of target information.

From a maritime perspective, it has been great for me, personally, to get back into thinking about the practical problems at the waterfront, as opposed to the hypothetical problems up in the 'ether' [heavens] (which is where I tend to spend most of my time at the moment in this job) and think about the positioning of ships, submarines and aircraft to dominate the maritime battlespace.

From a coalition perspective, the experiment is important because not only do we learn a lot about what is intended for the Maritime Headquarters with Maritime Operations Center construct for the future, but also we may have a little to offer in terms of our own experiences in the past.

The U.K. has split the responsibilities for administering the fleet and running operations between two physically separated headquarters for some time. I was directed, back in 2000, to review the Fleet Headquarters structure, which at that time was focused on type commanders and a tribal budgetary system.

We looked at reorganizing the Fleet HQ to be more focused on fleet outputs, as opposed to type commander outputs, giving the fleet commander himself greater control over his own budget. This resulted in a geographical separation of the administrative functions of the Fleet Headquarters, which is now in the U.K. based in Portsmouth, England, from the operational part of the Fleet Headquarters, which remained in Northwood.

We have learned quite a bit through that process: in particular, having our Maritime Operations Center collocated with the joint force commander's headquarters staff gives us great advantage. The officers executing the operations control functions in the fleet routinely also execute functions in a joint context on behalf of the joint force commander.

Because we work on a smaller scale than you do in the United States, we have been able to optimize our linkages to NATO and the equivalent Maritime Component Command Headquarters, which is collocated in Northwood alongside our national Fleet Headquarters. Our Commander-in-Chief Fleet executes a NATO role as a dual-hatted commander.

In terms of the detail of how business is conducted inside those Maritime Operations Centers, there is still a lot to rinse through for the United States. The thrust of our strategic development in both areas, both in the U.K. and the U.S. at the moment, very much looks at addressing problems with a 'Whole of Government' approach.

Therefore, [we are] looking at how to bring the interagency elements together more effectively. The Department of State, in the U.S. case, and the intelligence agencies outside the military and other government departments all have a critical role to play. We are looking at how to bring these authorities into the equation at a much earlier stage, so that the planning takes into account what their requirements are, rather than having to amend military contingency plans at the last minute to accommodate non-military inputs.

In the U.K., I don't think we are any further ahead with that. We are just setting up a National Security Council in the U.K. for the first time. It is a reflection of the need to bring together the other government departments at an earlier stage in the planning process and have a view, what you would call in the United States an interagency perspective, from the start.

There are structural elements of difficulty in the United States in terms of the way the government is structured, which make that more difficult for the U.S. than it is for the U.K.

In terms of the ways I am evolving my role here in the Combined Joint Operations from the Sea Center of Excellence ... The first two years of CJOS's existence under my predecessor were very much trying to set the organization up alongside Second Fleet and working out how we would work to leverage best practices both from the U.S. Navy and also from the other NATO sponsoring members of CJOS COE.

I think that has gone well. We have created a mission for ourselves, since I arrived, which focuses slightly more on what we are trying to deliver. The original mission was based on delivering transformational products to NATO, which is absolutely right, but it is difficult to define what a transformational product is.

We are now focused more clearly on what we are actually trying to do, which is improving allied ability to conduct combined joint operations from the sea. We have also created a vision for ourselves over the next five years, which aims toward a

higher profile organization here, clearly recognized as a useful, leading-edge thinking organization, using the latest ideas and best practice available to help improve multinational maritime operations.

CHIPS: How would you define your role?

Commodore Mansergh: The CJOS COE works primarily for its 13 sponsoring nations, and it is very clear that we are not inside the NATO command structure. Theoretically, NATO should not task us. We can be asked or requested to do things, but the first source of formal tasking should always be from the 13 sponsoring nations.

The principle we follow is that, where we can see good ideas or best practices from any of those 13 individual nations, we will pull them through into NATO, by doing any development or coordination work outside and then submitting our products to NATO for consideration and agreement by the 26 members.

That may be a quicker way of getting good practice moved through to NATO, rather than having to get the whole thing worked through the 26 individual nations in the consensus process (from the start), which is what NATO currently has to go through.

The other Center of Excellence, which is certainly larger and perhaps more mature, and, so far, has been more prominent than our own, is the Joint Air Power Competence Center (JAPCC) of Excellence in Germany, which has nearly 100 people, as opposed to the 26 in the CJOS COE here.

That one [JAPCC] has been remarkably successful, producing a number of joint air power products for NATO, most of which have been accepted straight into doctrine.

We are going to do a similar thing. The niche areas, which the Joint Air Power Competence Center identified early, when it was setting up its own working program, are not so easy to find for the maritime side, because NATO operations at sea have always been strong, and information sharing and cooperation have always been good.

Without wishing to denigrate the maritime contribution in the Northern Arabian Gulf in any way, it is clearly less prominent than the air and land contributions. As a result, NATO has tended recently to focus on land and to a degree, air operations, at the expense of the maritime. Therefore, the Joint Air Power Competence Center has a better chance of its products being directly relevant to the day-to-day operations than perhaps we do.

The challenge for the U.S., in delivering the Global Maritime Partnership, will be in finding sufficient common ground and understanding with those nations which it wants to work with, to build a durable partnership, based on trust and mutual respect.

The CJOS COE potentially has a key role to play in helping in this regard, as it can act as an extremely effective sounding board for emerging U.S. thinking and in facilitating improved relations with the key nations around the world, which will have an important role to play in the partnership.

For more information, go to the 2nd Fleet Web site at www.secondfleet.navy.mil or contact 2nd Fleet public affairs at C2FPAO@SECONDFLEET.NAVY.MIL.

CHIPS

Collaboration and Connectivity for the Warfighter – JEFX 08-3

Navy leverages Air Force experiment to focus on command and control operations

By Sharon Anderson

The pace was brisk; adrenaline was pumping at 2nd Fleet's Maritime Headquarters with Maritime Operations Center (MHQ with MOC) located in Norfolk, Va., April 23, as about 70 battle watch officers, as well as more than 100 other Army, Navy and Air Force officers at various locations across the country, manned stations that linked simulated portions of the MOC with Navy Warfare Development Command's Modeling and Simulation Lab in Newport, R.I., and the Air Force Air Operations Centers (AOC) across the country to participate in the Air Force's Joint Expeditionary Force Experiment 2008-3.

JEFX 08-3, held from April 14 – 25, is part of the JEFX 08 series of related Air Force-sponsored experiments focusing on network command and control operations. It also emphasized integration, distributed operations, and data links to enhance joint and coalition warfighting environments.

The Navy's participation in JEFX 08-3 is aimed to develop and refine the MHQ w/MOC processes in relation to other tactical C2 centers. JEFX provided an environment for the Navy to experiment with techniques, tactics and procedures for communicating with other MOCs and carrier and expeditionary strike groups, as well as with collaboration through machine-to-machine communications rather than by telephones and radios.

A MOC consists of organizational elements that share information and knowledge in support of the planning, execution and assessment stages of operations as required by the MHQ commander. The experiment explored the different ways that MOCs can globally link with each other and with Air Force AOCs.

"This is one of the only events that we can leverage off an Air Operations Center. The Air Force has a distributed [Combined] CAOC in this experiment. They have been very cooperative with our needs, and it's a venue that is unique in working with an AOC," said Capt. Steven Swittel, director of the Maritime Battle Center for Sea Trial experimentation at NWDC. Swittel worked with 2nd Fleet for two years in designing and developing the experiment structure for the Navy.

"We are stressing the processes between the MOC and the AOC and looking at joint maritime fires, and we are looking at the processes and tools. We are doing some 'live fly' and we have aircraft on the range that we control from here and send missions to them. They can take pictures, send pictures here, we can evaluate — and if we want to hit that target — we can send a strike order back to the same aircraft and they can do it. They can take a re-picture of it and send the battle hit assessment back to the MOC.

"The main thing is the operational level and how the MOC and AOC tie together. We have Air Force guys here during the debrief to make sure that we get the best out of the data we are collecting," Swittel said.

Second Fleet's participation in the experiment primarily focused on its MOC's ability to interact with other operation centers around the world — to globally network, emphasized Capt. Steve Snyder, deputy director of the MHQ w/MOC at 2nd Fleet. The experiment allows an opportunity to build in more

commonality, consistency and compatibility between the numbered fleet MOCs and the Naval Network Warfare Command's tailored MOC, Snyder said.

"In JEFX, as we work with our partners, the other sister services and other nations, if the Air Force has to work with Fifth Fleet and Second Fleet, it benefits both if Fifth Fleet and Second Fleet's operations centers are similar. It will also add value to our tactical forces.

"If we take a carrier strike group and an expeditionary strike group through all their training on the West Coast or East Coast, many of them will go through three or four AORs (areas of responsibility) under command of a different maritime operations center. They start here at Second Fleet, go through Sixth Fleet and could end up in Fifth Fleet's AOR. The same is true of our West Coast forces starting with Third Fleet, going to Seventh Fleet and perhaps Fifth Fleet again.

"For that strike group, it is important that as they get different bosses, that the way that they interact with those bosses has a common flavor," Snyder said.

Navy MOCs have been evolving for about four years. Adm.



Capt. Steve Snyder, deputy director of the MHQ with MOC at Second Fleet; Mr. Tom Forbes, Second Fleet's science adviser; and Capt. Steven Swittel, director of the Maritime Battle Center for Sea Trial experimentation at Navy Warfare Development Command.

Mike Mullen, when he was Chief of Naval Operations, drove the idea for a MOC, standard, globally networked capabilities needed at the operational level where commanders can go for expertise for any number of capabilities. The Navy calls this reachback, and it is critical to operational success, according to Snyder.

"Reachback has a couple of different flavors. One is unique skills, information operations is a good example, where for NETWARCOM and their federated IO structure that is a capability that all the MOCs ought to be able to tap into.

"Whether I am at Second Fleet, Fifth Fleet or Seventh Fleet, I ought to be able to reach back. There is always going to be distributed capability, but in terms of the scalability, I can reach back to Norfolk and NETWARCOM.

"There is also reachback in terms of load level. If something goes hot on one of our fleet AORs that drives a manpower requirement above their existing staffing level, and we don't have the time to flow operational level command and control people there, maybe they can reach back to another fleet staff and get some planners because their demand signal just went way up," Snyder said.

The MHQ with MOC is intended to streamline processes and communications at the operational level between fleet and naval component commands. Through MHQ with MOC, the Navy is creating a global network of maritime headquarters that will be in constant communication with each other and able to consistently and quickly transition from peacetime operations to combat, humanitarian relief, or other operations as needed.

JEFX is a "forcing function" for integration of new or emerging technologies and assessment of interoperability with existing C2 systems and subsystems.

"We want to force collaboration," said Tom Forbes, 2nd Fleet's science adviser. "We don't want people to collaborate face-to-face because we need to wring out the networks and the applications and see how they perform and how they support collaboration.

"We put the CSG and the ESG people in physically separate locations from where the maritime component commander is located so they can't talk to one another face-to-face just as if they were aboard their ships out at sea. We created the conditions such that they had to rely on the tools in order to do their jobs," Forbes said.

The experiment combines live, virtual and constructive air, space, naval and ground force simulations and technology insertion into a near-seamless joint warfighting environment.

Navy Warfare Development Command provided the simulation through its JSAF, Joint Semi-Automated Forces, a maritime-specific simulation, fed from Newport to Hurlburt Field, Fla., for the overall simulation environment for the exercise. But not just any scenario will do, said Snyder.

"Scenarios are not easy. There is a lot of work that goes in to make sure that the scenario stresses the things you are trying to test. Every time you get a group together, you want it to be more than just do the electrons flow?

"Every time you have people in a room working through a process, they are learning. If you have a type commander or a captain playing in this environment for the first time, they need to learn something that they might use in the fleet when they are doing this for real," Snyder said.

While providing a fine-tuning process for the joint warfighter, the experiment also helped establish groundbreaking command and control technology.

"ISPAN, Integrated Strategic Planning and Analysis Network, is a tool developed by U.S. Strategic Command. It is user-friendly and extremely useful in the first phase of this experiment so we brought it back for a closer, broader look in this event. It continues to serve us well, and that is a big win for us," Forbes said.

"We have already incorporated that in the 2010 baseline. It is a Web service, and it supports the military style of planning, it is universally applicable across the land, sea and air domains."

Some of the other applications and systems tested were the TBMCs, Theater Battle Management Core Systems and JADOCs, Joint Automated Deep Operations Coordination System.

"JADOCs has served us well as a battle management tool that allows us to coordinate actions across the number of warfare commanders in our doctrine as well as coordinating with the other services so that we bring the right effects onto the target at the right time.

"TPG, Target Package Generator, allows us to send imagery via Link 16 from this building to an FA-18 in the air in Nevada over an IP network.

"We assembled a team of folks that had never worked together before, and they had no experience on any of the tools that we gave them. We trained them for three days and on the fourth day, we had ROC (rehearsal of concept) drills, then we went right into the scenario ops. It has been a dynamic experience, and they have done tremendously well," Forbes said.

Lessons learned are documented in STIMS, the Sea Trial Information Management System, a database maintained by NWDC.

"We have learned a lot about how the MOC and the tailored MOC, the federated IO, needs to work together to support one another. The information operations domain is federated and works through the tailored MOC at NETWARCOM through five FIOCs, Fleet Information Operations Centers.

"They are networked together via IP networks, and they provide the non-kinetic effects, the information operations, the influence shaping, computer network operations, and all sorts of computer network defense — an intangible force that we need to be able to operate with efficiently," Forbes said.

For the electronic warfare element of JEFX, the Navy provided the airborne electronic attack aircraft EA-18G Growler at Nellis Air Force Base, Nev.

Some of the experimentation is only applicable at the numbered fleet commander level, the tailored MOC at NETWARCOM or for the theater maritime commander, according to Forbes.

"But it is also applicable down to the strike group commander and staff level and even down to individual ships in some cases. We have some representatives from a carrier strike group and an expeditionary strike group in the experiment audience," Forbes said.

Technologies will be deployed in spirals for the 2010 baseline.

"We have defined what we think we will need in FY10 and what we are planning to invest in ought to be the C4I, command, control, communications, computers and intelligence, profile for maritime operations," Snyder said.

Ultimately, the importance of the experiment is not really about technology, according to Snyder.

"We want to make sure there is seamlessness across the boundaries. Those boundaries are horizontal, AOC to MOC, and vertical as in MOC to the strike groups to the tactical forces.

"For example, what good is one cell phone? You need to make sure that there is something on the other end, whether that is horizontally or vertically," Snyder continued.

"The applications and the technology we are using need to enhance our ability to fight and operate at the operational level, but we also need to make sure they are connecting across all of our different boundaries."

For more information about JFEX-08, go to www.gcic.af.mil/News/JEFX.asp.
For more information about 2nd Fleet, go to www.secondfleet.navy.mil/. **CHIPS**

Phoenix Express 2008

By Sharon Anderson

Bringing the National Maritime Strategy to life is just one facet of Phoenix Express 2008, the Navy's third annual two-week exercise that demonstrated a multinational commitment to regional stability and maritime security in the Mediterranean.

Participants from 11 nations came together, April 8-22, to improve their ability to perform maritime interdiction operations (MIO) individually and in a combined effort. Countries that participated in the MIO events, included: Algeria, Greece, Malta, Morocco, Portugal, Spain, Tunisia, Turkey and the United States. France and Italy also participated in PE 08.

PE 08 included two phases of training: in port and at sea. In addition to MIO, participants conducted search and rescue operations, small boat handling, division tactics, medical training and ashore maritime coordination.

In the U.S. Navy, maritime interdiction operations are handled by what is called each ship's visit, board, search and seizure teams. VBSS teams help to ensure mission readiness while focusing on the importance of maritime security operations. Maritime interdiction operations set the conditions for security and stability and complement the counterterrorism and security efforts on the high seas and in nations' littoral waters.

PE 08's combined maritime forces conducted workshops in helicopter operations and safety, damage control and firefighting, navigation and deck seamanship. There was also an enlisted leadership round table and a welcome reception with 200 guests aboard the amphibious assault ship USS Nassau (LHA 4) on the exercise's opening day.

Underway events focused on maritime domain awareness and the shipboard Automatic Identification System that included interaction between forces afloat and a maritime operations center ashore.

While in port in Souda Bay, Crete, teams worked together in the newly established NATO Maritime Interdiction Operational Training Center (NMIOTC), which provided a realistic environment with multiple threat scenarios for training in small arms, fast rope insertion and tactical sweeps.

Two ships from the Nassau Expeditionary Strike Group, Nassau and the amphibious transport dock ship USS Nashville (LPD 13), along with the frigate USS John L. Hall (FFG 32) and the fleet replenishment oiler USNS Patuxent (T-AO 201), represented the U.S.

Eight other ships also participated in the exercise, including the Algerian training ship La Soummam (937); the French salvage ship FS Acheron (A 613); the Greek auxiliary ship Evros (A 415); the Greek frigate HS Spetsai (F 453); the Moroccan frigate Mohammed V (611); the Portuguese frigate NRP Corte Real (F 332); the Spanish corvette SPS Infanta Elena (P 76); and the Turkish frigate TCG Gelibolu (F 493).

Aboard Nassau April 24, Capt. Bob Lineberry, officer in charge of PE 08 and Nassau ESG commander, talked about some of the highlights of the exercise.

"NATO stood up the training center [NMIOTC], and it was accredited and certified on April 2. We were their first customer. There were 116 personnel on 10 teams, and over a four-day peri-

od, they went through their training regimen to allow the teams to come together to train and go out and practice that training at sea.

"We started with in-port training, which was the basis of getting the teams together and forming a good understanding of what the 6th Fleet wanted us to do as far as training objectives.

"We took the plan, finalized it, matured it, and knew that we were going to be able to meet those objectives. Everyone understood what the plan was. For the first five or six days in Souda Bay, we briefed the plan to make sure that everyone understood it, that we could execute it, and then we all got underway," Lineberry said.

The training agenda provided maritime forces with numerous opportunities to operate together and develop productive relationships through diverse and challenging operational scenarios, according to Lineberry.

"This year — this is new for Phoenix Express 2008 — it was a scenario-driven exercise. In the past, they have not had so much scripted out. There were intelligence injects from the exercise control group that drove some of the decision-making on how, when and where we were going to be making the boardings.

"We had four target ships in the operating area and our surface action group commanders had to decide, based upon intelligence, which teams they were going to send to which ships. It made for a much better, more realistic exercise. Phoenix Express continues to grow in size as well as complexity," Lineberry said.

Phoenix Express helps create an environment that promotes safety, interoperability, and by demonstrating the capabilities of a multinational maritime force, it serves as a warning to maritime criminals, extremists and terrorists.

Because training and working together are so vital to the success of the exercise to prepare for real-world operations, careful attention is paid to each participant's needs in planning the exercise events, Lineberry said.

SOUДА BAY, Crete (April 11, 2008) Service members from Algeria participate in Phoenix Express 2008, a training exercise aboard a mock ship at the NATO Maritime Interdiction Operational Training Center (NMIOTC). U.S. Navy photo by Mass Communication Specialist 3rd Class David R. Quillen.





SOUDA BAY, Crete (April 9, 2008) Capt. Robert Lineberry, commander of the Nassau Expeditionary Strike Group, speaks with commanding officers from several international naval vessels aboard the amphibious assault ship USS Nassau (LHA 4) during Phoenix Express 2008. U.S. Navy photo by Mass Communication Specialist 3rd Class Coleman Thompson.

“During the exercise development process and the various planning conferences, every country sends representatives. There are four times we get together prior to an exercise. During each one of those planning sessions, we will lay out everyone’s training objectives. We will match up those countries’ training objectives to the sponsoring commander’s overall training objectives — Sixth Fleet sponsored the exercise this time.

“Everyone can see what the training will be, and we get more than just maritime interdiction operations, sometimes called maritime intercept operations. We get low slow flyer exercises and we get fast-boat attack exercises,” Lineberry said.

The simulated target vessels were often Nashville and Patuxent. Landing craft utilities from Nassau were also used as target craft in several scenarios. Nassau as the central hub for the exercise, hosted many liaison naval officers from the other participating countries.

Two helicopters from Helicopter Sea Combat Squadron (HSC) 28 provided transportation from Nassau’s flight deck to the target vessels, often taking foreign teams who had never flown in an American helicopter.

“We all share the maritime environment and to communicate and have a better understanding and to be able to build that friendship and that relationship while we are at sea will add to the security and the stability of the region.

“We achieved that but the focus of most of the training was primarily the MIO boardings, but the much greater purpose was being able to build the energy, build the excitement and get the leadership involved with going out and operating among 11 nations with 12 ships and numerous boarding teams.

“We did it successfully and we did it safely to achieve the [6th Fleet] commander’s objectives. That’s what it was all about and we had a blast. It was a lot of fun,” Lineberry said.

All the nations participating are committed to enhancing maritime capabilities that will help future joint peacekeeping efforts, humanitarian operations and to stop destabilizing elements and maritime criminals in the Mediterranean Sea. Although, acts of piracy off the coast of Somalia and the Horn of

Africa make headlines almost daily, the Mediterranean is a security concern as well.

“There are a lot of illegal activities in the Med. That is a concern for the Sixth Fleet commander as well as the other countries. That would be a purpose for MIO boardings.

“[Personnel conducting] MIO boardings could be looking for terrorists or terrorist-type equipment or activities. They could also be looking for illegal activities such as smuggling, drugs, weapons or human trafficking. Those are the issues they deal with in the Mediterranean.

“[The purpose of] Phoenix Express is to help countries keep the security in the region, keep the stability in the region, and be able to share information. Each country brings its own capabilities — many countries come to learn — but many also come to teach.

“Every country had some sort of training evolution whether it was on the beach or flight deck safety. When we went to sea, we had some countries lead the low slow flyer exercise. Some countries led a tow exercise where one ship tows another ship,” Lineberry said.

The new National Maritime Strategy has at its foundation cooperation with friends and allies to promote global peace and prosperity. PE 08 achieved its training objectives but also promoted friendship, mutual understanding and cooperation.

Lineberry said that the nations and crews not only learned from the experience but also enjoyed the port visits and camaraderie with multinational forces.

“When we all got together the first week, at the NMOTC and on the ships, we came together as participants, and we left as friends,” Lineberry said.

In PE 08, more than 3,100 multinational maritime forces came together to build regional stability and maritime security in the Mediterranean. When not performing boarding exercises, the multinational teams also found other ways to improve their collective skills, including friendly competitions and small arms firing.

“We were excited to have the opportunity to work with sailors and marines from Morocco or Algeria or Spain or Portugal — or many of the other countries that participated. Our young kids got a kick out of the opportunity to share stories. They have a lot of great memories, and they made a lot of great friends.

“We have an exchange program. Several Sailors and Marines went from one ship and spent time on another country’s ship. Here on the Nassau, we had all of our liaison officers onboard to help us execute the plan and communicate the plan to the various countries. This has become the hub, the international hub, for the exercise,” Lineberry said.

Participants used Battle Force Email, which was set up on each ship to provide communications supporting the execution of events around the clock, from air operations exercises to refueling-at-sea evolutions.

“It is not new technology. It is something we have used in the past. We need to find one that is more user-friendly. One of our challenges with the Battle Force Email was having the system be user-friendly to people who are not familiar with the system and having the system be reliable to the various users.

“One of our lessons learned is that we need a system that is more flexible with a higher rate of information exchange to make it more reliable,” Lineberry said.



MEDITERRANEAN SEA (April 17, 2008) Visit, board, search and seizure team members from the guided-missile frigate USS John L. Hall (FFG 32) return to their rigid hull inflatable boat after conducting a boarding on Landing Craft Utility (LCU 1661) during Phoenix Express 2008. U.S. Navy photo by Mass Communication Specialist 2nd Class Amanda Clayton.

“Every ship, every country, every team, brings its own unique capability, and it varies from country to country. We had to find the best way to communicate for each country, and that was the primary method we used to communicate the plan and to execute the maritime interdiction boardings,” Lineberry said.

The at-sea phase of PE 08 came to a close April 19 in Augusta Bay, Sicily, where the participating countries met to discuss the outcome of the exercise. Data from the exercise will be analyzed and used to plan future exercises.

“The day before yesterday, we brought in six flag officers from the other countries to participate in the After Action Review. That was a lessons learned session.

“The Sixth Fleet commander will take those lessons learned, and the planners will send those out to the different countries. They are sending out invitations already for Phoenix Express 2009. Those lessons learned and those commander’s issues will get turned back into making Phoenix Express 2009 a better exercise and to meet the needs of our multinational partners,” Lineberry explained.

The job still isn’t done for the Nassau ESG, according to Lineberry.

“We are going to catch up with the rest of our [strike group] ships, and we are heading over to the Arabian Gulf, to the Fifth Fleet. We are going to spend a couple of months working for the Fifth Fleet commander and the CENTCOM (U.S. Central Command) commander carrying out maritime security operations and a variety of missions ...”

CHIPS

Nassau Strike Group

To the Beach, and Beyond!

The Nassau Expeditionary Strike Group (NASSG), with its more than 2,800 Sailors and Marines, deployed Feb. 19-20 for a regularly scheduled deployment to the Navy’s 5th and 6th Fleet areas of operation in support of maritime security operations.

Commanded by Capt. Robert G. Lineberry, the NASSG is made up of the amphibious assault ship USS Nassau (LHA 4); the amphibious transport dock ship USS Nashville (LPD 13); the amphibious dock landing ship USS Ashland (LSD 48); the guided-missile destroyers USS Ross (DDG 71) and USS Bulkeley (DDG 84); the attack submarine USS Albany (SSN 753); all homeported at Norfolk; and the guided-missile cruiser USS Philippine Sea (CG 58), homeported at Mayport, Fla.

Philippine Sea departed from Mayport Feb. 19, with Ashland deploying from Naval Amphibious Base Little Creek, Va., on the same day. The remaining ships departed Naval Station Norfolk Feb. 20.

The strike group, with 2,800 Sailors, returned to Norfolk, Va., July 11, 2008.

The mission of the NASSG consists of five primary components:

- **Expeditionary Power Projection**

- **Maritime Security Operations**

- Anti-Air Warfare
- Anti-Submarine Warfare
- Anti-Surface Warfare
- Mine Warfare

- **Amphibious Operations**

- **Crisis Response**

- **Humanitarian Assistance**

- Disaster Relief
- Non-Combatant Evacuations Operations
- Enabling Operations

NASSG Unit Composition:

Commander, Amphibious Squadron Six (CPR-6)

USS Nassau (LHA 4) – Flagship

USS Nashville (LPD 13)

USS Philippine Sea (CG 58)

USS Ashland (LSD 48)

USS Bulkeley (DDG 84)

USS Ross (DDG 71)

USS Albany (SSN 753)

Marine Expeditionary Unit 24 (24 MEU)

- Ground Combat Element

- Air Combat Element

Helicopter Anti-Submarine Squadron Light 46 (HSL-46)

Helicopter Sea Combat Squadron 28 (HSC-28)

Tactical Air Squadron 21 (TACRON 21)

Fleet Surgical Team Two (FST-2)

Naval Beach Group Two (NBG 2) Det. C

- Assault Craft Unit 4 (ACU 4) (LCAC)

- Assault Craft Unit (ACU 2) (LCU)

- Beach Master Unit (BMU 2) (LMU)

Navy Information Operations Command (NIOC) Det.

Strike Group Oceanography Team (SGOT)



– Nassau Expeditionary Strike Group Public Affairs

Focus on Nassau Expeditionary Strike Group

NASSG participates in coalition maritime security operations exercises designed to strengthen regional partnerships and promote global prosperity

Coalition Forces Complete Goalkeeper III Exercise

*By U.S. Naval Forces Central Command/
5th Fleet Public Affairs*

Coalition forces, led by Royal Bahrain Navy Brig. Gen. Abdulla Saeed Al Mansoori, commander, Task Force (CTF) 152, conducted Exercise Goalkeeper III (GKIII) in the Arabian Gulf, May 12-14.

The three-day exercise focused on maritime security operations (MSO) and provided coalition forces an opportunity to work together and exercise their ability to locate and track various contacts, conduct visit, board, search and seizure (VBSS) operations as well as command and control functions. GKIII included partners from Bahrain, New Zealand, the U.K., the U.S. and other regional countries.

Al Mansoori said GKIII gave coalition navies an opportunity to improve interoperability and training proficiency.

"We are working together, continuing operations that counter illicit activities in the maritime arena to create a lawful maritime order," explained Al Mansoori, who oversees all maritime operations in the central and southern Arabian Gulf region.

"Coalition maritime forces conduct maritime security operations under international maritime conventions to build security, which promotes stability and global prosperity in the maritime environment and complements the counterterrorism and security efforts of regional nations," he continued.

Units participating in GKIII included Bahraini Navy frigate RBNS Al Manama (FPBGH 50), Royal New Zealand Navy frigate HMNZS Te Mana (F 111), amphibious assault ship USS Nassau (LHA 4), guided missile cruiser USS Philippine Sea (CG 58), fleet ocean tug USNS Catawba (T-ATF 168), members of Commander, Destroyer Squadron 9 and various U.S. maritime patrol aircraft.

According to Capt. Jim Loeblein, commander of Task Group 152.0 and Destroyer Squadron 9, the exercise's key event was coalition team members handling

command and control of a specific vessel of interest that could pose a threat to one of the coalition nations in the Gulf region.

The exercise allowed coalition boarding teams to board the vessel of interest, locate and take control of a person of interest and practice the procedures for turning him over to Coast Guard ships.

Loeblein said that building security is not the only advantage of these exercises.

"While helping to build regional security, exercises like GKIII also allow us to maintain our open sea lanes. This is a very important area of the world for merchant traffic and regional Navy traffic, and exercises like this allow us [to] build confidence in our regional partners and provide a combined opportunity to provide security."

Loeblein said the exercise was a tremendous success noting GKIII was the most complicated exercise CTF 152 has conducted to date.

"I'd like to see more coalition member states participating. I think the more you get involved with bilateral and multinational exercises, the more it improves the

ability of the coalition and regional partners to work together towards a common security objective," Loeblein said.

Al Mansoori assumed command of CTF 152 March 4, marking the first time coalition forces have been commanded by a Gulf nation. He said coalition initiatives like this have added to improved cooperation efforts within the region.

"I believe Bahrain's leadership of CTF 152 has been very successful and has improved cooperation in maritime security within the region," Al Mansoori said. "The 20-plus members of the coalition all work together seamlessly. We are proud of the work we have accomplished while leading CTF 152."

Editor's Note: British Royal Navy Commodore Peter Hudson became the new CTF 152 commander June 5.

CHIPS

Coalition comes together to complete disaster relief training

*By Mass Communication Specialist 3rd Class
Coleman Thompson*

Combined Task Force 59 (CTF 59) recently completed a humanitarian assistance training exercise in the Arabian Gulf. The exercise was designed to improve the task force's collective response capabilities in the event of a natural disaster.

MEDITERRANEAN SEA (April 16, 2008) The amphibious assault ship USS Nassau (LHA 4), the amphibious transport dock ship USS Nashville (LPD 13) and the Military Sealift Command fleet replenishment oiler USNS Patuxent (T-AO 201) and international naval vessels transit the Mediterranean Sea. The Nassau Expeditionary Strike Group has participated in a number of maritime security training exercises since its deployment in February. U.S. Navy photo by Mass Communication Specialist 1st Class James C. Davis.



The "In Lieu Of" exercise tested the joint task force's abilities to set up a command and control center to facilitate relief efforts without, or in lieu of, the support of a Marine expeditionary unit.

Likewise, the exercise, part of expeditionary strike group (ESG) training, provided an excellent opportunity for the United States to show its willingness to support regional nations in times of crisis.

"The purpose of the exercise is to deepen our capability in humanitarian assistance, disaster recovery," said Rear Adm. Kendall L. Card, commander, ESG 3.

"We're trying to broaden our capabilities, and by doing so, we reduce the response time, and we reduce deaths and mitigate human suffering," Card said.

The units that participated in the exercise were ESG 3, CTF 59, the amphibious assault ship USS Nassau (LHA 4), U.S. Army Central, U.S. Air Force Central, U.S. Marine Corps Central Command, U.S. Naval Forces Central Command (NAVCENT), CTF 56, CTF 55 and CTF 53.

CTF 59, NAVCENT's crisis response task force, is responsible for planning and executing contingency operations in the region including disaster relief, humanitarian assistance, oil spill response, non-combatant evacuation and foreign consequence management.

"We rely on all the services' capabilities to provide the best response to these crises.

"Each of the services has unique capabilities and by putting them all together under one commander we provide the very best the United States has to offer in terms of resources," Card said.

The exercise took place from May 18-25 both at sea on Nassau and on shore in a camp built by Naval Mobile Construction Battalion (NMCB) 74, a NAVCENT detachment in Bahrain. The exercise involved the movement of personnel and equip-

ment from ship-to-shore and establishing a command and control environment both on land and afloat.

"Exercises like this are important because it tests our ability to stand up a joint task force and to conduct crisis response operations, which is something that we're responsible for as CTF 59," said Lt. Cmdr. Joseph Pezzato, contingency planner for ESG 3 and CTF 59.

In the event of an actual crisis in the U.S. Central Command area of operations, CTF 59 is the command and control task force currently assigned to immediately respond if the host nation requests aid.

Said Pezzato, "As NAVCENT's agent for crisis response, it's something that we don't always get to practice because it involves members of all different services coming together to form a joint task force."

Aside from testing and improving the abilities of the task force, the exercise also helps to strengthen regional relationships and demonstrates the U.S. commitment to the security and welfare of the region.

"This provides an opportunity for us to deepen our relationship with the friendly countries out here," said Vice Adm. Kevin J. Cosgriff, then commander of U.S. 5th Fleet, commander, Combined Maritime Forces, and NAVCENT commander.

"We have to make sure that other countries see us as reliable and that we want to contribute to the well-being of the citizens," Cosgriff said.

"Exercises like this improve our relationship with the host nation because even though we're not actually provid-

ing assistance to any one nation, it shows them that it is one of our missions to help out in the event of a crisis.

"It demonstrates our commitment to the region and shows that we're not just here for warfighting, we're also here to maintain a presence of the United States in helpful situations," Pezzato said.

CTF 59 is made up of personnel from ESG 3, which is based in San Diego. The ESG 3 command element is currently deployed to Naval Station Activity Bahrain.

Editor's Note: Vice Adm. William Gortney assumed command of NAVCENT/5th Fleet/Combined Maritime Forces July 5. For more information, please contact U.S. Naval Forces Central Command public affairs office at 011-973-1785-4027 or navcentpao@me.navy.mil. CHIPS

U.S., Pakistan Forces Complete Inspired Union 2008

By Nassau Strike Group Public Affairs

Pakistan and U.S. naval forces completed Exercise Inspired Union 2008 in the North Arabian Sea May 21, which focused on air, surface and anti-submarine training, as part of regional maritime security operations (MSO).

Pakistani forces, including PNS Badr (D 184), PNS Shahjahan (D 186), PNS Nasr (A-47) and Pakistan Air Force Explosive Ordnance Disposal, participated in the bilateral exercise along with Sailors from USS Curtts (FFG 38) and USS Ross (DDG 71). Other U.S. forces participating included

PERSIAN GULF (May 14, 2008) The amphibious assault ship USS Nassau (LHA 4) leads a formation of coalition ships including the guided missile cruiser USS Philippine Sea (CG 58), the Bahraini Navy frigate RBNS Al Manama (FPBGH 50), the Royal New Zealand Navy frigate HMNZS Te Mana (F 111) and the United Arab Emirates Navy missile boat UAENS Mubarraz (P4401) during Exercise Goalkeeper III in the Persian Gulf. The multilateral Goalkeeper III exercise includes participation from Bahrain, New Zealand, United Arab Emirates, Qatar, Great Britain and the U.S.



“Visits by U.S. Navy ships symbolize the continued friendship and partnerships between countries and military services — it allows us to increase our cooperative engagement and exemplifies our commitment to building trust and confidence among friends worldwide.”

– Commanding Officer USS Curts (FFG 38) Cmdr. Yvette Davids

Destroyer Squadron 50 and Combined Task Forces (CTF) 54, 55 and 57.

“This exercise allowed the U.S. and the Pakistani Navy to demonstrate and improve our interoperability in a variety of warfare areas,” explained Capt. Paul Severs, commander, Destroyer Squadron 50. “Inspired Union focused on surface warfare, air defense, visit, board, search and seizure (VBSS) operations and ended with a final event using all warfare areas.”

Pakistan is an integral member of the coalition and has commanded Combined Task Force 150 twice, most recently from November 2007 through February 2008.

Coalition Maritime Forces regularly operate throughout international waters in the North Arabian Sea to conduct MSO. Coalition ships assigned to CTF 150 operate throughout the Arabian Sea, Gulf of Oman, Gulf of Aden and the Red Sea.

“It was a very successful exercise,” Severs said. “From the planning conferences to the pre-sail seminars and the at-sea events, the exercise was well-coordinated. Inspired Union also allowed sailors from both navies to participate in professional exchanges to understand how different coalition ships operate at sea.”

Severs noted that the bilateral cooperation was key to the exercise’s success.

The exercise also provided an opportunity for Curts to visit Karachi during a

three-day port visit. The visit offered the crew an opportunity to plan for Inspired Union, conduct cultural exchanges and engage in sporting events with their Pakistani Navy counterparts.

“This is the first visit by a U.S. ship to Karachi since September 2006, and we are grateful for the opportunity to visit Pakistan,” said Cmdr. Yvette Davids, Curts’ commanding officer.

“Visits by U.S. Navy ships symbolize the continued friendship and partnerships between countries and military services — it allows us to increase our cooperative engagement and exemplifies our commitment to building trust and confidence among friends worldwide,” Davids said.

Curts, homeported in San Diego, Calif., is part of the USS Abraham Lincoln Carrier Strike Group. USS Ross, homeported in Norfolk, Va., is part of the USS Nassau Expeditionary Strike Group. CHIPS

Top, right: MEDITERRANEAN SEA (April 16, 2008) Servicemen from the Tunisian Navy stage an assault from an SH-60 Seahawk onto the Military Sealift Command fleet replenishment oiler USNS Patuxent (T-AO 201) during a training exercise designed to simulate a visit, board, search, and seizure operation utilizing skills and techniques developed during the two-week Phoenix Express 2008 exercise. US Navy photo by Mass Communication Specialist 3rd Class David R. Quillen.



MEDITERRANEAN SEA (April 16, 2008) A group of U.S. Marines stand on the mess decks of landing transport dock ship USS Nashville (LPD 13) after completing maritime interdiction operations training as part of Phoenix Express 2008. U.S. Navy photo by Mass Communication Specialist 1st Class Charles L. Ludwig.



PERSIAN GULF (May 9, 2008) Members of the helicopter visit, board, search and seizure (VBSS) team of the aircraft carrier USS Abraham Lincoln (CVN 72) perform a helicopter rope suspension maneuver out of an MH-60 Seahawk helicopter over the flight deck of the amphibious assault ship USS Nassau (LHA 4) during a training exercise. Both Nassau and Lincoln are deployed supporting maritime security operations in the U.S. 5th Fleet area of responsibility. U.S. Navy photo by Mass Communication Specialist 3rd Class Coleman Thompson.

NSWC Dam Neck – Face to the Fleet

Bridging gaps, building relationships and engineering C5I systems for a net-centric force with an experienced, dedicated staff

By Sharon Anderson

The crown jewels of the Navy science and technology domain are the Naval Sea Systems Command's warfare centers. They have the fleet perspective, a unique perspective that doesn't exist in industry or even the universities that partner with the Navy in developing technologies.

There are 11 warfare centers, two undersea and nine surface, including NSWC Dam Neck on the Virginia coast. There are also another dozen subordinate sites. These commands employ nearly 18,000 people, most of which are scientists and engineers.

Closely aligned with warfighter needs and an eye toward inserting technological advances into combat systems, NSWC Dam Neck is a leader in engineering solutions that are affordable and agile.

On a sunny, crisp day in April, the CHIPS staff toured several NSWC Dam Neck labs beginning with a call on NSWC Dam Neck Commanding Officer Capt. Jon A. Greene and NSWC Dam Neck's Technical Operations Manager Mark J. Lucas.

"We are relatively small and we are organized into small teams working on projects with limited budgets, but they are having a big impact across the spectrum of command and control," Greene said.

Program Executive Office Integrated Warfare Systems (PEO IWS) is NSWC Dam Neck's largest customer, followed by NAVSEA, U.S. Joint Forces Command and 2nd Fleet, according to Greene.

NSWC Dam Neck's location for fleet support is ideal: it is within 30 minutes of 50 percent of the Navy's largest fleet concentration area, JFCOM headquarters and three of four JFCOM component commands, as well as the only NATO command on U.S. soil.

"We have 11 commands within NAVSEA's naval surface warfare centers and naval undersea warfare centers and only one of them is in a fleet concentration area — and that's us. Oddly, we are the smallest of the sites but that gives us number one, a unique opportunity to engage with the fleet, and number two, a unique responsibility to take that oppor-

tunity and to provide that fleet feedback to the other warfare centers. We are working hard to try to do that," Greene said.

In addition to working with the other warfare centers, Greene said that Dam Neck is eager to bridge the gap from NAVSEA to the FORCENet enterprise to help add the fifth "C" in C5I (for combat systems) by working with the Space and Naval Warfare Systems Command, who has traditionally been the C4I (command, control, communications, computers and intelligence) engineer.

"We have the traditional combat system focus that is consistent with what has been done with NAVSEA and PEO IWS, real-time, fire control-type focus. On the other hand, SPAWAR is focused on the C4I world; we want to work with them to bridge that gap," he said.

NSWC Dam Neck is also aggressively pursuing the linkage from NAVSEA to the joint force. While Greene acknowledged building relationships takes time he is committed to the task and he credits CHIPS for being a reliable communications forum for project leaders and commands.

"The biggest challenge, and CHIPS does a tremendous service, is that there are a lot of people working very hard on their individual projects, and there is inadequate collaboration and communica-

NSWC Dam Neck Commanding Officer Capt. Jon A. Greene and NSWC Dam Neck's Technical Operations Manager Mark J. Lucas on the steps of Hopper Hall, home to the NSWC Dam Neck workforce. NSWC Dam Neck personnel engineer C5I system capabilities across the life cycle. NSWC Dam Neck's mission is to arm warfighters with innovative capabilities by delivering force-level integrated and interoperable engineering solutions, mission critical control systems, and associated testing and training technologies which meet the requirements of the maritime, joint, special warfare and information operations domains. The CHIPS staff toured NSWC Dam Neck's labs April 16.

tion across families, across organizations, across warfighting enterprises. If we can break down those stovepipes, the potential for what we can do is incredible," Greene said.

Capt. Greene attributes much of the success in partnership building to Mark Lucas.

"My hat is off to Mark, he has worked very hard in the last year to develop relationships. Port Hueneme Det. Virginia Beach is down the street, and we have developed a close relationship with them. We are working with Carderock [Division] Combatant Craft Department, and we are working with the SPAWAR Systems Center Charleston group in Norfolk on a number of issues.

"Think of the potential when we start saying, 'I am working on this and you are working on something very similar, what's the best of breed? Where can we do better for the warfighter and the taxpayer?' We are starting to make inroads there," Greene said.

Historically, NSWC Dam has delivered combat direction systems life cycle support and software support activities to the fleet, but Lucas said the center is undergoing a transformation that integrates its product line across a network for a net-centric force. An important part of the transformation is a capable workforce.

"You have to think about what skills you need in your workforce in advance of those requirements. That is probably one of our biggest challenges, but it is one of the things that I am fiercely proud of: we have a fleet-minded organization that is driven to support the needs of the war-



fighter above and beyond just the day-to-day.

"We have a diverse mix despite our size. We are about a 350-person organization, from a government standpoint, about 10 percent military and the rest civilian. That itself is an anomaly. If you look at an acquisition warfare center activity, it is rare to see 10 percent of the workforce be military because a lot of the emphasis is on the up-front research and development. It's critical to us to be able to align our investments to the needs of the fleet," Lucas said.

While NSWC Dam Neck employs scientists and engineers, it also has technicians that understand how the systems will be used in their intended environment and who are able to provide the feedback through the requirements process, Lucas said.

Greene agreed, but said the fleet operators, the operations specialists, bring recent fleet experience and create a synergistic alliance with Dam Neck's scientists, engineers and technicians.

"They are the folks with recent 'wounds' from the fleet, but you also have the added benefit when those folks roll back to sea. Those folks have a better understanding of the technology and they have a ready 'Rolodex' of folks that are working on these problems, and they continue that dialogue when they return to the fleet," Greene said.

Next to the NSWC Dam Neck workforce, Greene and Lucas are most proud of the products they produce.

"Things we are proud of ... It's going to be a long list. I'll start with the Integrated Tactical Mobility System. The ITMS was designed for the Naval Special Warfare Development Group for one of their platforms that operates in a very harsh environment," Greene said.

"It was originally built by a contractor and Dam Neck was asked to do the IV&V (Independent Verification and Validation), and it did not go well. The folks asked if our team of engineers could help them get it operational. In a period of about six months, Dam Neck took the initial design and got it so it would operate in the environment that we're talking about," Greene added.

ITMS is a small craft situational awareness system that provides both tactical and navigational capability. It is Microsoft Windows-based and incorporates both

commercial off-the-shelf (COTS) and government off-the shelf (GOTS) software.

"Today, they are on their third generation of equipment and a number of other platforms. They have developed some superb components and a superb integrated system that provides situational awareness for these folks.

"They developed, a 2.2 gig Pentium with a 200-megabyte hard drive, dual core. It's about the size of a cigar box, weighs less than 3 pounds, requires no external cooling, goes from minus 40 to plus 135 degrees Fahrenheit, and will take a 30 G-shock. You can submerge it under a meter of water for up to an hour, it will keep running, and it costs about \$5,000," Greene said.

The system design is so compact, durable and robust that Greene said it could serve a variety of uses.

"When you start thinking about space and weight considerations that we are dealing with on all platforms, including surface ships, aircraft, and things like that, this starts to make a lot of sense. The question that I ask everybody is why don't all tactical computers look like this? I think they should [this capability] in the not too distant future," Greene said.

Another system developed by Dam Neck engineers, in a collaborative effort with NSWC Panama City and SPAWAR Systems Center San Diego, is the Multi-Vehicle Control System (MVCS) designed for the Littoral Combat Ship platform. The LCS has five unmanned surface and subsurface vehicles that will need to be controlled depending on three different mission packages. The MVCS Dam Neck team completed software Build 2.0.0 in March followed by qualification training which continued through April. The target release date is early May.

"The team said it makes no sense to have different controllers and five different radios on the ship. How are we going to handle this? Multi-vehicle control systems are the answer, and they came up with the idea in conjunction with the Mission Package Development Lab at NSWC Panama City and SPAWAR San Diego.

"This is an Internet service provider for unmanned vehicles. You bring the vehicle that is compliant with the MVCS architecture, you plug it into that architecture, and you don't need to bring your own radio and your own control system. All you need is a little bit of software. You can

ITMS

The Integrated Tactical Mobility System provides the small craft operator with a single system capable of interfacing systems, processing the data into a single data source, and displaying information in real-time.

The system architecture and design scales from a single station to hundreds of stations. Each station includes standard processors specially packaged for harsh environments. ITMS addresses the operator's needs for a common design and installation approach to situational awareness, navigation, communications, sensors and other craft systems.

ITMS provides built-in fault isolation, sensor monitoring, multiple source video display and capture, electronic nautical charts, integrated radar, electronic maneuvering board and radio control. Each station maintains full functionality with data and file synchronization. ITMS is a Microsoft Windows-based system that incorporates commercial off-the-shelf (COTS) and government off-the shelf (GOTS) software.

The ITMS software was designed for all weather operation using bezel button input. All screens contain large, easy to read text with day and night color configurations on enhanced sunlight and night vision compatible displays. ITMS can be easily installed on a standard laptop, and connected to the ITMS LAN to provide all the functionality of an ITMS station.

NSWC Dam Neck's location for fleet support is ideal: it is within 30 minutes of 50 percent of the Navy's largest fleet concentration area ...

control that system and send signals back to the mission module and into the core combat system. We are excited about that, and we think that it has applicability beyond LCS and beyond the Navy," Greene said.

As Greene continued to enumerate a seemingly inexhaustible list of NSWC Dam Neck accomplishments, too many to state here, he continued to point to the Dam Neck workforce as his source of greatest pride.

"We are active across the life cycle, so we do everything from the developmental work, the testing and evaluation, and into the life cycle management."

For more information, contact NSWC Dam Neck public affairs at nswcdnpao@navy.mil or (757) 492-6155, or go to the NSWC Web site at www.navseadn.navy.mil.

CHIPS

FROST – Future Readiness and Optimized Scheduling Tool

Predicting best-case or worst-case scenarios — and any scenario in between — for more accurate cost models and decision analysis

By Sharon Anderson

NSWC Dam Neck engineers recognized that making trend predictions for Navy electronics systems maintenance required data collection from a wide variety of sources. So to make tracking easier, they developed a Web-based application that tracks data in a customizable management and predictive tool, called FROST, Future Readiness and Optimized Scheduling Tool.

FROST is a collaborative effort between the Naval Sea Systems Command's warfare centers. FROST was initially created by combat system engineers to forecast inventory shortfalls and to identify requirements before they developed into problems.

"We try to predict ahead of time when we are going to have a problem," said Michael Gaintner, FROST project lead and systems engineer.

Originally, the team entered data in a huge Excel spreadsheet, but changing data was tedious, labor intensive and error prone.

"Excel couldn't handle the calculations anymore, so we made the first version of the Web tool — FROST. We added a few other features, like including 'harvesting' in our predictions. The first time a system would be taken off a ship, we would go out, grab some of the electronic components, and use them to support the systems that are still in the fleet. It cut down the inventory we were using, which means less warehouse fees and less purchases," Gaintner said.

There are several basic data inputs that go into FROST. According to Gaintner, the problem is that the information needed for forecasting is dispersed across different commands.

For example, NSWC Corona, Calif., has a database that provides data about parts failure. At NSWC Crane in Indiana, engineers are in constant contact with vendors to determine how long the vendors can support each part and the cost of new parts. NSWC Port Hueneme, Calif., keeps track of the parts inventory and is the performance-based logistics organization.

"The information needed to sustain Ship Self Defense System (SSDS) is dispersed. When it was a manual process and we would go to a new schedule, it would take us weeks to provide our program office with feedback. The new schedule could affect our ability to support the system. For every part, we had to contact all these organizations to get all the information," Gaintner said.

FROST now automatically collects, tracks and shares relevant information in one tool and automates the process of analyzing system supportability. It automatically alerts engineers and logisticians when a part needs attention.

"You may get an alert that pops up and tells you that five years from now you will have a problem with a particular part. This enables us to look for a solution now. We can be proactive instead of having to react with limited options. The earlier we

do it, the more options we have and the more efficient the solutions are," Gaintner said.

Since managing the parts and electronics that make up these systems is captured in FROST, data and forecasts the team collects can be used by managers to help determine the effects of scheduling and budgeting decisions.

"We have managers dealing with entire ships and systems. There is not a lot of information being rolled up from the parts to the entire system to tell them what effects their decisions are going to have on supportability.

"They come out with a new fielding schedule and they need to determine what effect the schedule is going to have on supportability. We are trying to roll up all this information, so we can tell them, 'If you move this ship out two years, we can expect these problems, and we can expect these costs.' We can make more informed decisions not only on scheduling, but also on planning and budgeting," Gaintner said.

FROST is PKI-accessible. It creates reports on-the-fly with the most up-to-date information.

"The moment data changes, we can generate a new report from the system," Gaintner said.

In addition to automated tasking, FROST developers are working on implementing a mathematical model called "Monte Carlo."

"Without going into too much math, using Monte Carlo enables us to apply a complex statistical process to see the most likely scenario. The most likely scenario in this case is that we'll have a problem in two years. We'll also see that there is a 10 percent chance that we will have a problem this year and a 30 percent chance of a problem next year.

"We can run through every possible scenario to make sure that nothing happens that catches us off guard. Standard systems that don't use this tool have to make a lot of assumptions that may not end up being true. Most of these systems assume that parts fail at steady rates: three parts fail this year, three parts fail next year, but it doesn't happen like that," Gaintner said.

The Monte Carlo model also allows analysts to treat inputs as variables and generate options or uncertainties (randomness). This flexibility can be combined with information, such as scheduling changes, budget constraints and parts availability and obsolescence, for more accurate and meaningful forecasting.

"You may be lucky for four years, nothing breaks, and suddenly five or six [parts] break at the same time. Part of the statistical process is that we can account for that. We also do a lot of statistics with vendor data. They say they are going to produce this part for the next three years and support it for four years after that."



The actual results often differ.

"When you base all of your projections on assumptions that vendor data is correct, you can get in hot water and make bad projections and bad decisions based on that. We have analyzed how often they [vendors] are accurate and how much variance there is, and we are building it into the new system," Gaintner said.

According to Gaintner, best-case or worst-case scenarios — and any scenario in between — can be supported with more accurate cost models.

"One of the things we can offer management that they have never had before is projection of sustainment costs based on individual electronics. If we are going to run out of parts for this processor in five years, we can predict what it is going to cost to solve that problem," he said.

In this regard, FROST connects the life cycle sustainment process together to increase overall efficiency. It allows engineers and logisticians to discover supportability problems at the earliest possible time, increasing their options, thus allowing high-quality, more affordable solutions. It also provides previously unavailable data to management for more cost-effective decisions.

A ship's availability is a huge factor in scheduling changes. A lot of planning goes into this part of the forecasting, according to Gaintner.

"The next goal is to use Monte Carlo to find the optimal fielding schedule for systems. Management can tell us all the constraints, whatever you need to consider, put it into the system, determine that there are 30 or 40 possible schedules that fit this, and let the system tell you which one is going to save us the most money," he said.

"It has been a great tool. Program managers have been able to use it to support COTS obsolescence initiatives," said Pamela Schools, former SSDS commercial off-the-shelf (COTS) obsolescence lead, who is now on the Strike Force Interoperability team.

Gaintner said he would like to add to FROST's capabilities.

"We would like to go further and have the system compute optimal refresh cycles."

FROST was developed through Program Executive Office Integrated Warfare Systems (PEO IWS) sponsorship and is used primarily for SSDS. But it is being extended to be able to handle other Navy systems.

The software, servers and hardware behind FROST are maintained at NSWC Dam Neck. It is designed to be used on a daily basis by the engineers responsible for sustaining SSDS.

"I taught myself to program and wrote the first version which is specific to SSDS. Now we are contracting out to build the next version. As soon as we created this basic picture, we realized that we could build on it and do other things," Gaintner said.

There are about 225 parts tracked for SSDS ranging in cost from \$200 to \$40,000. The team performs COTS obsolescence management for SSDS and the Advanced Combat Direction System, which is a major undertaking when dealing with COTS products, according to Gaintner.

A working prototype of FROST is in use. Version 1.0 is expected to be deployed in June 2008.

CHIPS

Navy Reestablishes U.S. 4th Fleet

Chief of Naval Operations (CNO) Adm. Gary Roughead announced in April the reestablishment of U.S. 4th Fleet and assigned Rear Adm. Joseph D. Kernan, who was serving as Commander, Naval Special Warfare Command, as its first commander.

U.S. 4th Fleet is responsible for U.S. Navy ships, aircraft and submarines operating in the U.S. Southern Command (SOUTHCOM) area of focus, which encompasses the Caribbean, and Central and South America and the surrounding waters.

Located in Mayport, Fla., and dual-hatted with Commander, U.S. Naval Forces Southern Command (COMUSNAVSO), U.S. 4th Fleet's reestablishment addresses the increased role of maritime forces in the SOUTHCOM area of focus and demonstrates the U.S. commitment to regional partners.

"Reconstituting the Fourth Fleet recognizes the immense importance of maritime security in the southern part of the Western Hemisphere and sends a strong signal to all the civil and military maritime services in Central and Latin America," said Roughead. "Aligning the Fourth Fleet along with our other numbered fleets and providing the capabilities and personnel are a logical execution of our new Maritime Strategy."

U.S. 4th Fleet, established in 1943 as one of the original numbered fleets, was given a specific mission. During World War II, the U.S. needed a command in charge of protecting against raiders, blockade runners and enemy submarines in the South Atlantic. U.S. 4th Fleet was disestablished in 1950 when U.S. 2nd Fleet took over its responsibilities.

Initially, the new 4th Fleet will be headquartered with COMUSNAVSO and take advantage of the existing infrastructure, communications support and personnel already in place in Mayport. As a result, U.S. 4th Fleet will not involve an increase in forces assigned in Mayport.

U.S. 4th Fleet will retain responsibility as COMUSNAVSO, the Navy component command for SOUTHCOM. Its mission is to direct U.S. naval forces operating in the Caribbean, Central and South American regions and interact with partner nation navies within the maritime environment. Various operations include counter-illicit trafficking, theater security cooperation, military-to-military interaction and bilateral and multinational training.

Rear Adm. Joseph Kernan assumed command of U.S. 4th Fleet in a ceremony June 21, 2008, on Naval Amphibious Base in Coronado, Calif.

For more information, go to U.S. Naval Forces Southern Command's Web site at www.cusns.navy.mil.



PACIFIC OCEAN (June 27, 2008) Chilean sailor Javier Pino Jeria shows U.S. Navy Ensign Shawn Calihan how to plot the ship's location during the Pacific phase of UNITAS 49-08. UNITAS is an annual exercise designed to increase cooperation and interoperability between the U.S. and South American navies. U.S. Navy photo by Mass Communication Specialist Seaman Omar A. Dominguez.

— Consolidated from stories posted on Navy.mil

Strike Force Interoperability

Navy officers and government engineers ensure combat systems are strike group ready and surge capable

By Sharon Anderson

Strike Force Interoperability Officer (SFIO) teams, consist of Navy officers and senior civil service project engineers with a strong technical pedigree in fleet operations using integrated and interoperable command, control, communications, computers, combat systems and intelligence (C5I) systems aboard U.S. Navy ships.

NSWC Dam Neck's SFIOs ensure that combat systems are integrated and interoperable within a carrier strike group or expeditionary strike group. Although SFIOs do not deploy on ships, they identify C5I issues within the strike groups for which they are responsible as established by U.S. Fleet Forces Command in May 2004.

"We analyze and monitor C5I equipment to identify interoperability issues and track their resolution," said Pamela Schools, who is a project engineer on the SFIO Team.

SFIOs primarily work with the strike group's N6 leadership who focus their attention on C5I support. The SFIOs help to identify, communicate and resolve interoperability and modernization issues key to strike group readiness and surge capability.

"There are three naval officers and three civilian project engineers here at NSWC Dam Neck. Each naval officer is teamed up with a project engineer, and together they are responsible for multiple carrier strike groups and expeditionary strike groups.

"For example, I am responsible for the USS George Washington and USS Theodore Roosevelt Carrier Strike Groups. I am also responsible for the USS Nassau and USS Bataan Expeditionary Strike Groups," Cmdr. John Vliet said.

"Within each one of those strike groups, there may be as many as eight or 10 Navy ships assigned, so what I just gave you are close to 45 separate ships, from aircraft carriers and big deck amphibs, to guided missile cruisers, destroyers and frigates.

"That is how we spread the division of labor within the SFIO organization. At any given time, any one of those ships could have an interoperability issue or a modernization issue, and then we go into action. We vet those issues to Naval Sea Systems Command (NAVSEA) 05W4 Strike Force Interoperability Program Office at the Washington Navy Yard and also to Naval Network Warfare Command (NETWARCOM)," Vliet explained.

Training on new combat systems is important for the ships' crews, as well as the SFIOs, according to Vliet.

"With today's rapid development of COTS [technologies] and other C5I systems, it would be an overstatement to say we know half of the technical aspects of all new systems available to the fleet. Having said that, it is imperative that SFIOs and project engineers be trained and stay current on the capabilities and limitations of these new systems.

"If it is difficult for the technical community to stay current on new systems, you can only imagine how difficult it is for a young Sailor aboard a ship, which is why training for the Sailors with reference to these new systems is imperative," Vliet said.

To ensure they are well prepared for the job, SFIOs and project engineers attend a weeklong C4I training seminar, sponsored by the Space and Naval Warfare Systems Command (SPAWAR). "These seminars are held quarterly in San Diego," Schools said.

"It gives you all the SPAWAR points of contact for C4I, but let's not forget combat systems," Vliet added.

The team also gets training from NAVSEA 05W4 and information from NDE, the Navy Data Environment, a source of information about ongoing modernization throughout the fleet.

"It is the authoritative data source for modernization and it has four or five parts. NM is the Navy Modernization piece, AMPS is the Afloat Management Planning System which NAVSEA 05W4 created to manage the C5IMP (Combat System and C4I installations and improvements), and there is a logistics module," Schools said. "SPAWAR has SPIDER (SPAWAR PEO Integrated Data Environment and Repository) which feeds programmatic data into NM and AMPS automatically."

"If you take one thing out of this interview, understand that our main interest, our focus and our main goal is the fleet ... "

- Strike Force Interoperability Officer Cmdr. John Vliet

The SFIO Team analyzes the ships' problems and works with NAVSEA to determine the best course of action for resolution.

"We analyze the modernization data on our respective ships and vet the issues through NAVSEA 05W4. If it is something we need to address, we address it. If there is an interoperability issue — that is where we come into play. We don't physically go down to the ship to fix it; however, we might go to a ship to discuss an issue. We push the right buttons to get the right people involved," Vliet said.

Interoperability issues are complicated due to the fact that each ship in the Navy has a different configuration, and even when differences are small, it still makes fixing problems difficult, according to Vliet.

"No ship is the same, so the testing at sea becomes complex. We try to identify and keep an up-to-date status on the testing and installations on the ships and make sure that we inform NAVSEA 05W4, the type commanders, for us, specifically NETWARCOM, and the fleet commanders about what is going on.

"Sometimes as systems are being installed on ships, they are still being tested at land-based test sites," Vliet said.

Vliet added that the only sure test for combat systems interoperability is at-sea testing.

"They discover new things on ships; it is just the nature of the business. You can't test everything in the lab; you have to get it out into the at-sea environment and flex the system."

The SFIO team is proud of the contribution they are making to fleet readiness, but they are continuously working on ways to improve, according to Vliet.

"If you take one thing out of this interview, understand that our main interest, our focus, and our main goal, is the fleet. I have been in the Navy for 27 years and most of that time at sea, I don't care how sensitive an issue is, it is going to be brought up on behalf of the United States fleet."

CHIPS

ASDS - Advanced Sensor Distribution System

A digital, real-time, efficient and cost-effective sensor distribution method

By Sharon Anderson

The Advanced Sensor Distribution System (ASDS) Laboratory, also known as the AN/SPQ-14(V) or ASDS lab, is a small lab with a big job. Simply stated, ASDS converts Navy tactical radar signals and radar video into a digital stream enabling ASDS radar distribution switchboards (SB-4229A(V)/SP) to distribute these signals to various consoles throughout NSWC Dam Neck to support test events and other fleet support initiatives.

NSWC Dam Neck is a Naval Sea Systems Command warfare center. It has served the fleet in its present location for more than 40 years. NSWC Dam Neck is the only NAVSEA warfare center located in Norfolk's fleet concentration area, although other NAVSEA employees work in the Hampton Roads area in the Carderock and Port Hueneme Warfare Center detachments, for example.

The ASDS program has been at NSWC Dam Neck since 1995. ASDS was developed as an upgrade to the older Radar Display and Distribution System (RADDS) or AN/SPQ-12(V). RADDS is the legacy system installed on more than 148 Navy ships.

The ASDS lab provides the distribution of multiple live Navy radars to combat systems. Additionally, system prototypes and upgrades are designed and tested at this site.

The ASDS project provides "cradle to grave" support to the Navy, providing services such as: life cycle maintenance; configuration management; system engineering; software development and maintenance; test and integration; and logistical support.

ASDS is installed on more than 48 ships, including aircraft carriers (CVN), amphibious command ships (LCC), amphibious assault ships (LHA/LHD), destroyers (DDG) and amphibious transport dock ships (LPD). ASDS is also slated for installation on all new construction LPD, LHA, LHD and DDG class ships.

ASDS consists of switchboards, con-

verters, amplifiers, decoders and displays. The converters, (CV-3989(V)1/SP), take analog data from Navy radar, combine it with ship data, and convert it to a 64-bit data stream called the RADDS Data Stream. The RADDS Data Stream is sent to the nucleus of the ASDS system, the switchboard, (SB-4229A(V)/SP).

The switchboard distributes the data stream to various users throughout the ship, including AN/UYQ-70 and AN/SPA-25G/H displays. Decoders are used to change the data format to support analog and digital users. Amplifiers are used to split signals to additional users.

The ASDS system is quite reliable (as deployed), but the lab staff is constantly challenged with technology obsoles-

Rick Sharp, ASDS project manager, and Luis DelValle, AN/SPA-25H project lead, with the AN/SPA-25H console. The first installation of the AN/SPA-25H to the fleet is planned for November 2008 for the newly named amphibious assault ship USS America (LHA 6).



cence. In addition to obsolescence, ASDS upgrades and new prototypes are driven by new technologies or requirements and usually a combination of factors, according to Rick Sharp, ASDS project manager.

"It's a bit of both, depending on the situation. For LRADDS, we have a requirement from the ships. For something like the AN/SPA-25H (a follow-on obsolescence upgrade to the current AN/SPA-25G Indicator Group), it comes about because of technology. Because of technology obsolescence we can't find a lot of parts. It was cheaper to go with a new design than it was to try to piecemeal every part in that system," Sharp said.

Obsolescence mitigation also provides opportunities for future enhancements and growth.

"Our next generation of sensor distribution (and follow-on to ASDS) is in the design phase now. This new system is a LAN-based design. We are working closely with the Aegis modernization team in

PEO IWS 1.0 to put the LAN Radar Data Distribution System (LRADDS) on cruisers and destroyers during COTS refresh (CR3).

"The newer system [LRADDS] does what ASDS does — and a whole lot more. This time around, we are adding a software scan conversion function and will be interfacing with the new Common Display System consoles. The genealogy of distribution is RADDS to ASDS and now to LRADDS," Sharp said.

Another obsolescence solution is working its way through the design and development phase at NSWC Dam Neck, according to Sharp.

The "obsolescence challenged" AN/SPA-25G Indicator Group uses 1980s tech-

nology that is in desperate need of updating. The AN/SPA-25H is completing a few remaining Integrated Logistics Support (ILS) items prior to full implementation. The new AN/SPA-25H was designed as an AN/UYQ-70 variant.

"There are thousands of AN/UYQ-70 consoles aboard Navy ships, and we were able to utilize those lessons learned in this effort. The first delivery for the AN/SPA-25H is in November 2008 for the LHA 6.

"We are in the planning phase for backfitting the AN/SPA-25H in FY09 and FY10 on nine ships. Those ships will have their AN/SPA-25G, Tactical System Interface Unit (CP-2294) and controller (CD-135) replaced with the AN/SPA-25H and a network switch, resolving the most pressing obsolescence issues they are dealing with," Sharp said.

The nine ships are: USS Nimitz (CVN 68), USS Eisenhower (CVN 69), USS Carl Vinson (CVN 70), USS Ronald Reagan (CVN 76), USS George H.W. Bush (CVN 77),

USS Tarawa (LHA 1), USS Nassau (LHA 4), USS Peleliu (LHA 5) and USS Blue Ridge (LCC 19).

"The AN/SPA-25H does everything the old one did and more. Using current technology, we are able to network multiple AN/SPA-25Hs together to get a common track picture for the operators," Sharp said.

Testing for the AN/SPA-25H has been completed, but has just begun for the LRADDS.

"We have most of the design and all of the testing and logistics ahead of us," Sharp explained.

Installation of the LRADDS system is planned for all cruisers and destroyers that are scheduled for modernization. The modernization, which is planned to run until 2021, is part of a larger Navy plan to modernize the fleet in basically two areas: hull, mechanical and electrical (HME) and combat systems (CS) upgrades.

"We have to deliver the first LRADDS system in March of 2009 for a lab. The first ship installation is [scheduled] in June 2010. We are doing three to six ships a year for almost 45 ships over a 10 to 11-year window. In addition to LRADDS, we are also installing the AN/SPA-25H at the same time.

"The cruiser modernization and the destroyer modernization work that we are doing is done out of Program Executive Office Integrated Warfare Systems 1.0. I support PEO IWS 2.0, the Above Water Sensors directorate. I am a NSWC Dam Neck employee that spends a little over one third of my time in Washington as a member of the IWS 2.0 team. I manage the RADDs, ASDS, LRADDS and AN/SPA-25 projects out of the IWS 2.0 shop at NAVSEA," Sharp said.

There are 13 government personnel on the team and seven contractors, according to Sharp, and they are out on ships several times a month.

"Any day we could get a call that there is a problem on a ship, which we would need to respond to. The nice thing is that the fleet is right here in our backyard so it is easy for us to respond. Obviously, it takes a lot more effort to support the West Coast," Sharp said.

Working with different configurations and both new and legacy systems is complex, but it is a requirement that the ASDS team can't get around because they must support both.

"AN/SPA-25H [technology] is somewhere in between. Some projects would like to take a technology leap, but for obvious requirement reasons we must still be able to interface with legacy systems.

"We wanted to take advantage of as much state-of-the-art technology as we could. We have come up with a solution that has allowed us to service all the legacy interfaces that we have, [and] at the same time, incorporated and taken advantage of all the technical advances," Sharp said.

Luis DelValle, AN/SPA-25H project lead, agreed with Sharp's assessment of the need to support both old and new technologies.

"We are internally using features and components that are being proposed for the future CDS, the Common Display System, as well as using and keeping some of the interfaces and requirements that we have with the older legacy systems. We are somewhere in between, and we have become a bridge between enabling us to go forward in the future but always maintaining and servicing our legacy interfaces," DelValle said.

As testament to DelValle's observation, the lab is populated with several generations of consoles including the new AN/SPA-25H. Legacy equipment is juxtaposed with the new. Cables, charts and equipment take up almost every inch of space, but the team is determined in their efforts and their service to fleet customers.

While NSWC Dam Neck has a 40-year legacy for fleet training and certifications, ASDS is one project more focused on providing reliable hardware and customer service support.

Whether or not the lab provides training depends on the customer and its requirements, Sharp said.

"Cruisers and destroyers have a requirement that we provide training material to their schoolhouse, and they take that and develop the curriculum. In the case of the AN/SPA-25H, it is going to come with a CD that you can put in any laptop or computer, and it will run computer-based training. There will also be training for the LRADDS system to support the customer."



For more information, contact NSWC Dam Neck public affairs at nswcdnpao@navy.mil or (757) 492-6155.

CHIPS

NSWC Dam Neck Awarded Wireless Grants

Improving battlefield command and control communications

NSWC Dam Neck was selected to receive a \$1.4 million grant from the Office of the Secretary of Defense to develop and deliver a mobile ad-hoc wireless network prototype for deployment in the tactical battlespace.

Roger W. Kuhn Jr., a Navy civilian network architect/information assurance engineer in NSWC Dam Neck's System Management Engineering and Analysis Branch (Code F33), will serve as a U.S. government trusted agent and will provide government oversight to this project to be executed by Fortress Technologies. Fortress, a secure wireless solutions provider, will deliver 10 prototypes of its ES520 Secure Wireless Bridges, with software modifications, to support advanced meshing capabilities.

Kuhn will be working closely with Fortress Technologies' Chief Technical Officer Magued Barsoum. Kuhn was notified Feb. 21, 2008, about the award.

"Within the 12-month timeframe allotted by this grant, we will rapidly develop, prototype and deliver 10 environmentally-ruggedized, secure wireless access bridges that support an improved form of tactical mobile peer-to-peer, or mobile ad-hoc network, (MANET) for deployment in the mobile, wireless tactical battlespace," Kuhn said.

The grant proposal, titled, *Secure, Robust Tactical Wireless "MESH" Network*, was selected for funding by OSD under the Quick Reaction Fund (QRF) program. The program, sponsored by OSD's Director of Defense Research and Engineering, "provides flexibility to respond to emergent DoD needs within budget cycles."

The Office of Naval Research (ONR) identifies the QRF as a program that takes advantage of promising technology breakthroughs that can be quickly field tested for an immediate impact on military operations. QRF grant recipients must deliver a military-specific prototype application within six to 12 months of being funded.

One aspect of NSWC Dam Neck's mission is to provide innovative capabilities by delivering force-level integrated and

interoperable engineering solutions to the maritime, joint, special warfare and information operations domains.

Kuhn identified the opportunity to seek an alternative to current Defense Department MANET developmental efforts.

“Current efforts involve adapting centralized scheduler architectures that are normally employed in a wired environment, such as Open Shortest Path First (OSPF)-based routing, which is inefficient in terms of network performance and survivability in a tactical, mobile wireless environment,” Kuhn said. “Hence, an alternative mobile mesh wireless protocol-based system needs to be developed and deployed ... specifically for a mobile, wireless battlespace.”

What this could mean for warfighters in theater is a reliable, robust, scalable, dynamic mobile tactical command and control (C2) system in which to operate.

Mesh networking is a way to route data, voice and instructions between nodes or devices attached to a computer network. It allows continuous connections and reconfiguration around broken or blocked paths by “hopping” from node to node until the destination is reached. A mesh network whose nodes are all connected to each other is a fully connected network.

Mesh networks differ from other networks in that the component parts can all connect to each other via multiple hops. Mesh networks can be seen as one type of ad-hoc network, but they generally are not mobile. MANET-ing and mesh networking are therefore closely related, but mobile ad-hoc networks also have to deal with significant problems introduced by the mobility of the nodes.

Kuhn, who is also a U.S. Coast Guard Reserve officer specializing in C4I, is known for his work in the wireless arena having co-authored the U.S. Coast Guard’s secure wireless policy.

In 2007, Kuhn received a Certified Wireless Network Expert designation — a certification that less than 100 people hold worldwide.

According to Kuhn, the Certified Wireless Network Professional, or CWNP, is the industry standard for non-vendor specific Wireless LAN (WLAN) training and professional certification.

In 2008, Kuhn received the WiMAX Forum RF Network Engineer designation (WFRE No. 411). The WiMAX Forum

is an industry-led, not-for-profit organization formed to certify and promote the compatibility and interoperability of broadband wireless products based on the harmonized IEEE 802.16/ETSI HiperMAN standard. IEEE is the acronym for the Institute of Electrical and Electronics Engineers.

In 2007, Kuhn brought to NSWC Dam Neck the command’s first ONR independent applied research (IAR) grant. Work on this \$1.6 million grant is a collaborative effort with NSWC Dahlgren Division. The proposal, *Application of IEEE 802.16 Technologies to the Global Maritime Domain Awareness (MDA) Battlespace* was approved by Dahlgren Division’s Science and Technology Council in July 2007.

When the CHIPS staff met Kuhn during an April 16th visit to NSWC Dam Neck, he and co-workers, Chris Weeks and Charles McCallister, were moving into a refurbished lab. They were enthusiastic about their new space and their projects.

McCallister’s expertise lies in radio frequency engineering. Weeks is an electronics engineer and the wireless lab manager.

“We are setting up a wireless lab that will support a tactical C2 technology/unmanned vehicle test range in the VA-CAPES (Virginia Capes) operational area [which is] adjacent to NSWC Dam Neck,” Kuhn said.

ONR is currently funding the adaptation of Wi-Fi technology for mobility within a metropolitan area network (MAN) for scalability. But the Dam Neck team is investigating broadband technology as an alternative for mobile C2.

Teaming with Barsoum, Kuhn came up with an idea of combining a set of routing protocols that specifically sup-

port a scalable, mobile, tactical, ad-hoc architecture. Engineers Chris Weeks, Roger Kuhn and Charles McCallister in the newly refurbished wireless technology lab at NSWC Dam Neck, Va. Kuhn is holding a wireless router. The team is working on two wireless research grants that they hope will result in a transformation in mobile, robust, wireless command and control communications on the battlefield.

port a scalable, mobile, tactical, ad-hoc architecture.

“There essentially are two developmental paths under the IEEE 802.11’s draft amendment which is the emerging standard for wireless mesh networking. You can go down the Ad hoc On-Demand Distance Vector (AODV) protocol path, which is what we are doing, or you can employ the Optimized Link State Routing (OLSR) protocol path. That is what ONR is doing.

“The problem is that wireless networks are flat, wireless LANs have limited network addressing, and you have intermediary or stop-gap routing protocols like Mobile IP.

“Mobile IP doesn’t lend [itself] to a seamless transfer, like a cell phone type of functionality. They tried to resolve that by using the OLSR protocol as a DHCP (Dynamic Host Configuration Protocol) relay agent to resolve that and instead of using Extensible Authentication Protocol (EAP)-based authentication, they are evaluating the employment of cryptographic-enhanced, Host Identity Protocol (HIP),” Kuhn said.

The Mobile IP communications protocol is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address to provide a routing capability between wireless LANs.

Extensible Authentication Protocol, or EAP, is a universal authentication framework frequently used in wireless networks and point-to-point connections. Although the EAP protocol is not limited to wireless LANs and can be used for wired LAN authentication, it is most often used in wireless LANs.

The Host Identity Protocol provides a



method of separating the end-point identifier and locator roles of IP addresses. It introduces a new Host Identity (HI) name space, based on public keys. The public keys are typically, but not necessarily, self-generated.

"After surveying current DoD C2 technology and unmanned vehicle development efforts, I had an epiphany: most mobile wired broadband technologies operate in the IEEE (U.S.) radio frequency C and S bands. DoD technologies employ these same bands," Kuhn said.

The Navy has a great deal of empirically-derived data about maritime propagation phenomena in the the S and C bands. That information will support Kuhn's ONR project.

"As a former Coast Guard weapons officer, I am familiar with radar-related RF ducting, Doppler shifts and other maritime RF propagation phenomena associated with temperature inversions, salinity of water, moisture content ...

"Conceivably, once you come up with a software-based radio with an internal frequency agility capability and an associated mathematical model based upon certain atmospheric and environmental conditions, you could tailor a software-based radio to function at its best while being subjected to ... atmospheric and environmental conditions," Kuhn continued.

"Additionally, given the infrastructure of conventional mobile broadband technologies like Mobile WiMAX, I foresaw the need of a self-scaling ad-hoc routing capability and that is how the second grant came about. The great thing about this protocol is it will be 'medium independent' [that means] it will work with IEEE 802.11, IEEE 802.16 and Free Space Optics."

FSO refers to the transmission of modulated visible or infrared beams through the atmosphere to obtain optical communications. Like fiber, FSO uses lasers to transmit data, but instead of enclosing the data stream in a glass fiber, it is transmitted through the air. FSO works on the same principle as infrared television remote controls, wireless keyboards or wireless personal digital assistant devices.

As we left the lab, Kuhn's attention was immediately drawn to the task at hand: completing lab set up and diving back into the work that may transform battlefield communications.

CHIPS

Remote Monitoring

SWE improves equipment operating condition feedback

The Remote Monitoring initiative under the Surface Warfare Enterprise (SWE) has resulted in significantly improved equipment monitoring for surface ship hull, mechanical and electrical (HM&E) equipment.

Through the combined efforts of Naval Surface Forces and Ship Systems Engineering Station (SSES) in Philadelphia, the Integrated Condition Assessment System (ICAS) has been updated to allow analysis via automatic downloading of ships' data to a central NAVSSES server. The combined improvements now deliver to the ship an Integrated Performance Appraisal Report (iPAR) of current equipment operating conditions within 24 hours.

The previous process for iPAR delivery used a manual approach and averaged 16 days to create and deliver this report back to the ship. The benefit of this improved process is that it allows ships to properly respond to "yellow" and "red" operating conditions on a timely basis before catastrophic equipment failures can occur.

These upgraded ICAS systems, currently on 36 of 76 ICAS-equipped combatants, consist of three added elements that include:

- ▶ Remote Monitoring Utility software that automates the download of data through the ship's Navy Information/Application Product Suite (NIAPS);
- ▶ A Configuration Data Set update to improve ICAS data accuracy and reduce unreadable or "gray" data cells; and
- ▶ An Auto Update Tool to allow remote download of future software upgrades.

As a result, these ships are now able to automatically download data to the Maintenance Equipment Library Server (MELS) at NAVSSES Philadelphia, which analyzes the data and generates the ship's iPAR.

The iPAR, which includes subject matter expert (SME) comments for recommended equipment checks, is then uploaded to the ship for HM&E material health visibility and assessment beyond the ship's alarms and control systems.

It also provides the same information to shore sources of support (SoS) for possible maintenance follow up. If a red con-

dition is noted requiring technical help from shore-based SoS organizations, the iPAR provides operating data which a SME can also access through MELS.

While the ICAS improvements to date have been significant, NAVSSES continues to refine and upgrade the system. A new enterprise Performance Assessment Report (ePAR) has just completed testing and is ready for use by SMEs and Class Squadrons (CLASSRON).

The ePAR report provides a stoplight-like condition report summary by specific system or group/class of ships. This report also provides SMEs drill down capability into specific red systems for analysis of more detailed operating conditions underlying the problem to be addressed.

As a result of these improvements, ICAS is now providing key remote monitoring lessons learned which represent a significant step forward in the Navy's way ahead to provide viable condition-based maintenance approaches to reduce repair costs and extend the life of a ship's systems.

These lessons learned provide another example of how the SWE is meeting its mission of optimizing warfighting readiness for combatant commanders.

Continuous process improvement allows the SWE to fulfill that mission in each core area: maintenance, modernization, logistics, manning and training.

The SWE is an enterprise committed to providing the most powerful, dominant, and adaptable surface warfighters and ships with maximum efficiency and careful stewardship of resources.

Commander, Naval Surface Forces is located in San Diego, Calif., and is headed by Vice Adm. D.C. Curtis, who ensures all of the Navy's surface ships are properly manned, trained, equipped and sustained to effectively support military operations around the globe.

Rear Adm. Kevin Quinn is the deputy SURFOR commander, located in Norfolk, Va. He is "dual-hatted" as the commander of Naval Surface Forces, U.S. Atlantic Fleet and Chief Readiness Officer.

Go to www.navy.mil/local/cnsp/ and www.swe.surfor.navy.mil/default.aspx for more information.

CHIPS

CWID Answers the Call for Future Capabilities

One nation threatens another in a volatile region of the world, and the scenario unfolds with a terrorist backlash in the continental United States on the global stage where Coalition Warrior Interoperability Demonstration technologies show their mettle.

Information sharing technologies, running the gamut from digital personal identification to suites for real-time global situational awareness, leveraged warfighter and first responder skills over a global network in June during CWID.

Based on predictions about the world after 2015, the Joint Chiefs of Staff refine requirements for "tangible joint force capability improvement" in the Capstone Concept for Joint Operations for making user-defined information and expertise available anywhere within the network.

Exploiting network connectivity between a dispersed joint force and coalition elements for information sharing, collaboration, coordinated maneuver and integrated situational awareness is just one of the areas that CWID tests.

CWID is the only forum that brings new and emerging information technologies into a global network environment with interagency and multinational partners.

Conditions since the Gulf War, with terrorist strikes on civilians and operations in Afghanistan and Iraq, led U.S. military planners to see that future conflicts may not always involve full-scale force on force operations.

Air Force Col. Vincent Valdespino, director for Command, Control, Communications and Computers, U.S. Joint Forces Command, said at a recent CWID conference, "We're talking about irregular warfare, about asymmetric warfare, CWID lets us look at emerging technologies to fight this type of warfare and enable winning the peace, enable civil affairs, cultural analysis and nation building."

Knowledge allows the joint force to see, understand and act before an adversary can.

With real-time information comes the ability to engage a broad range of solutions including economic, diplomatic and civil response on a global scale.

U.S. European Command, the combatant commander sponsor for 2006 to 2008, brings a natural emphasis on coal-

ition operations with close ties to NATO via its European headquarters in Stuttgart, Germany. Stephen Ewell, deputy director J-9, International Interoperability, Concepts and Experimentation, USEUCOM, has been instrumental in involving the DoD acquisition community more closely in the CWID process.

"We do CWID for operators, joint, interagency and coalition operators, to deliver capability," Ewell said.

Though CWID itself does not carry acquisition authority, CWID assessments, conducted during the demonstration, are compiled into a final report which provides focus for the acquisition community on demonstration output.

Technologies that make the CWID cut reduce risk, advance spiral development of existing technologies and put cutting-edge information sharing tools into the hands of warfighters in the near-term.

Assessment teams compile reports on warfighter utility, technical interoperability and information assurance from questionnaires, observation and network data collection.

CWID, held annually, was conducted June 9th through 19th out of four main U.S. network locations with more than 20 coalition partners in eight countries around the world. Defense Department, government, first response agencies and multinational counterparts all sponsor trials for CWID based on defined mission objectives.

Information technologies are recruited for the demonstration through a Federal Business Opportunity (www.fedbizopps.gov) published each spring. Promising trials are selected by fall, beginning an intense planning process to integrate them into the operational environment and onto the network for scenario play the following June.

The Defense Information Systems Agency is the lead agency, providing demonstration network engineering and daily support through the CWID Joint Management Office staff. USJFCOM oversees the event for the JCS and directs the management group with a charter to facilitate technology fielding in the near-term.

U.S. sites are: Homeland Security/Homeland Defense at North American Aerospace Defense Command/U.S.

CWID 2008

CWID evaluates technologies and capabilities for exchanging information among coalition partners, military services, government agencies, first responders and U.S. combatant commanders, especially this year's host, U.S. European Command (USEUCOM). Information sharing technologies leverage decision making and operational flexibility on the battlefield and during crisis response on the home front.

The five objectives of CWID 2008 are:

- Improve coalition and joint C4ISR architecture;
- Improve information sharing across the full range of military operations;
- Enhance cross domain and multiple security level information exchange tools;
- Enhance integrated logistics planning tools; and
- Enhance government agency interoperability.



On a tour of CWID, National Guard Bureau Director of C4, Maj. Gen. Alan Cowles, holds a prototype phone designed for satellite-based communications. The phone system or "infrastructure in the sky," a Marines Corps Warfighting Lab project, can help commanders track their troops on the ground. It brings connection times from 30 to 45 seconds down to just two. Photo courtesy of NSWC Dahlgren Division.

Northern Command, Peterson Air Force Base, Colo.; U.S. Army, U.S. Marine Corps and National Guard Bureau at Naval Surface Warfare Center, Dahlgren Division, Dahlgren, Va.; the U.S. Navy at Space and Naval Warfare Systems Command, San Diego, Calif.; the U.S. Air Force at Electronic Systems Center, Hanscom Air Force Base, Mass.; and the Warfighter Capability Demonstration Center at the Pentagon, which provides a virtual window into the coalition operational sites.

Go to www.cwid.js.mil for more information. CHIPS

A Trident Warrior 08 Journal

A situation report by the deputy director of Trident Warrior

By Brad Poeltler

The following are selected paragraphs from the daily SITREPs that were submitted to key senior officers to provide feedback on tempo and progress as we conducted Trident Warrior 08 experimentation. TW is the annual sea-based FORCENet series of experiments.

11 June

We intend to provide periodic updates during TW08 execution to keep you abreast of status and to solicit any real-time feedback to better meet our FORCENet experimentation needs.

As a reminder, we began TW08 with the concept development conference in November 2006. We designed the experiment to support fleet priorities, systems command technical support and Naval NETWAR FORCENet Enterprise (NNFE) requirements. We solicited technology nominations and then selected experimentation candidates from a broad range of government and industry sources.

We then began the detailed process of objective development, process diagram design, certification/accreditation, risk reduction lab-based testing, data collection and experiment design. This now brings us to the actual execution of the experiments. We start the main experimentation efforts on Monday [June 16]. We plan to execute about 100 separate experiments each day.

As a quick summary of the experimentation process: we will execute from June 9 until July 25 in the Southern California and Hawaiian operations areas. We will install, test and report on over 110 separate technologies or processes which have been installed in more than 40 separate commands including 19 U.S. and coalition ships.

We will issue a preliminary "quicklook" message immediately following the transit phase ending June 27, and then will send a supplement message following July operations. The Military Utility Assessment and final report will be ready in October.

13 June

Today, Commander, Space and Naval Warfare Systems Command Rear Adm. Mike Bachmann, who is also the NNFE chief operating officer, kicked off the distinguished visitor brief for an audience that included the commander of Amphibious Squadron 7 (CPR-7), commanding officers (CO) of USS Bonhomme Richard (BHR) (LHD 6) and CNS Almirante Riveros (FF 18), and representatives from the Navy Tactical Exploitation of National Capabilities (TENCAP) program and Office of the Chief of Naval Operations N6.

Of interest was a discussion on TW "leave behinds" with Capt. Neil Parrott, CO of the BHR. He petitioned for several of the installs, particularly the Navy Enterprise Records Management Solution, to remain. Unfortunately, ERMS and several other high interest technologies are installed on an experimental network and will have to be removed upon FINEX (exercise conclusion).

Commander of CPR-7, Commodore Rodney Clark, commented that perhaps the best leave behind benefit of TW was not

in a particular technology but the extensive system grooming conducted by the TW install team.

16 June

Today, we turned the experimentation level up to high. As the BHR and the USS Milius (MIL) (DDG 69) rounded Point Loma we were already testing more than 50 technologies in every one of the 12 FORCENet TW08 focus areas.

From an experiment battle rhythm perspective, each day we track events designed to measure and analyze data on each TW08 technology. Each evening we review the events of that day and adjust the next day's events to maximize the experimentation opportunities. As an example, yesterday we tracked over 300 separate events.

A technology that we are testing early is Hostile Forces Integrated Targeting System. HITS is designed to provide precision geolocation for targeting, utilizing air, surface and subsurface platforms by receiving and correlating signals from multiple security enclaves.

Today, we conducted over 40 geolocation trials against static shore-based and mobile maritime target platforms. HITS equipped sensors aboard BHR, MIL, an EP-3 aircraft and a submerged fast attack submarine utilized emissions in the ultra high frequency (UHF), very high frequency (VHF) and HF spectrums. Preliminary results indicated all geolocation trials were successful.

17 June

The networks on the BHR and MIL have stayed fairly stable and have not degraded any of our testing so far. We did, however, suffer a technical glitch testing the Floating Area Network. FAN is designed to provide a high-speed inter-strike group data network.

Because of installation restrictions we only could install FAN



SPAWAR Commander Rear Adm. Mike Bachmann and Commander of CPR-7 Commodore Rodney Clark at a distinguished visitor brief aboard USS Bonhomme Richard (LHD 6) June 13. The briefing officer is Lt. Cmdr. Doug Magedman from SPAWAR.

TW08 FORCEnet Focus Areas

- ▶ Network Design
- ▶ Cross Domain Solutions (CDS)
- ▶ Intelligence, Surveillance, Reconnaissance (ISR)
- ▶ Information Operations (IO)
- ▶ Wireless Technology
- ▶ Distance Support
- ▶ Naval Fires
- ▶ Command and Control (C2)
- ▶ Maritime Domain Awareness (MDA)
- ▶ Knowledge Management (KM)
- ▶ Coalition Communications
- ▶ Human Systems Integration

The Navy relies on Trident Warrior to help plan the future of FORCEnet



Royal New Zealand Navy liaison officer to TW08, Lt. Cmdr. Ralph Groube; N6 for Commander Amphibious Squadron 7, U.S. Navy Lt. Joe Moore; Naval Air Systems Command liaison officer to TW08, U.S. Marine Corps Capt. Tony Krockel; and Royal Australian Navy liaison officer to TW08, Lt. Cmdr. Kym Fisher.

19 June

TW08 coalition experimentation has participation from seven nations: Australia, Canada, New Zealand, United Kingdom, France, Chile and the Republic of Korea. Australian participation is centered on HMAS Anzac (FFH 150), en route to Hawaii. Canadian units include HMCS Ottawa (FFH 341), HMCS Regina (FFH 334), Maritime Forces Pacific and Canadian Forces Base Esquimalt, British Columbia.

New Zealand units include the New Zealand Maritime Operations Center and Joint Force Headquarters Wellington, HMNZS Te Kaha (F77) and virtual ships Waka and Kiwi. The United Kingdom is manning the virtual ship Daring in Portsmouth. The French Navy's virtual ship is participating from Toulon. The Chilean ship, CNS Almirante Riveros, and the Republic of Korea ship, KNS Munmu the Great (DDH 976), are also participating.

All units and nodes have established communications and network services utilizing the Combined Enterprise Regional Information Exchange System (CENTRIXS) community of interest, called Cooperative Maritime Forces Pacific (CMFP). CENTRIXS and Collaboration at Sea (CaS) accounts are using Sametime Version 8 core chat services with the Persistent Chat plug-in.

The following is selected TW08 technology with coalition impact:

Spatially Aware Wireless Networking (SPAWN) is a low cost, lightweight, phased array antenna. It was built by SPAWAR Systems Center San Diego and is sponsored by the Australia, Canada, New Zealand, United Kingdom and United States alliance, AUSCANNZUKUS, for command, control, communications and computers (C4). We are using a 802.11 radio, but the antenna can potentially be used with several other radios. The results have been extremely positive. This evening, we passed full motion video across a network connection in excess of 2.5 megabits per second at a range of 12 nautical miles.

20 June

In previous reports, the focus has mainly centered on the at-sea portions of TW 08; however, tonight's report highlights a few examples of TW08 ashore experimentation, in particular,

on BHR, MIL and USS Comstock (COM) (LSD 45), and the only opportunity to have all three in line-of-sight was this afternoon. Unfortunately, when the ships began the specific maneuvers, one of the critical FAN antennas aboard BHR failed. We were able to complete several distance and off-set tests, but the ability to obtain and then retain the network was not completed.

18 June

A quick addendum to last night's SITREP. Following the failure of the FAN antenna, the FAN technicians pulled apart the box and performed emergency surgery while the BHR, MIL and COM began their scheduled UNREP (underway replenishment).

Once advised the FAN antenna was working, CPR-7 re-tasked the ships to maneuver to the original FAN test formation following the UNREP. We accomplished an additional two hours of FAN testing and completed that experiment thanks to OUTSTANDING support from CPR-7, BHR, MIL and COM. Bravo Zulu and many thanks to all involved.

During last Friday's distinguished visitor brief, Capt. Parrot was particularly interested in the TW08 technology, ERMS. I would like to give a quick update. ERMS is enterprise software developed by the Department of the Navy Director of Records office to automate workflow functions for just about anything that requires routing within a ship. Today, ERMS was used to successfully create, chop, produce, and track through the chop chain, the BHR's operations summary report all the way from initial draft to final transmission as a naval message. We've received multiple requests from ship personnel to expedite this technology to the fleet.

experiments that directly support FORCENet capabilities at 3rd, 2nd, 7th and Pacific Fleet.

At 3rd Fleet, we are experimenting with Aqua Quiet Interlude Processing System, sponsored by Program Executive Office Integrated Warfare Systems. AquaQuIPs is a real-time, automated data fusion engine that receives national, theater and tactical sensors data and produces composite tracks into a clear and accurate maritime picture.

An “apples to apples” comparison between AquaQuIPs data and 3rd Fleet’s MOC data is nearly impossible because of different sensor inputs, different start times, and non-use of electronic intelligence by the 3rd Fleet MOC. However, AquaQuIPs tracks generally had many more hits per unit time than the 3rd Fleet MOC Global Command and Control System - Maritime for tracks detected by both systems.

At 2nd Fleet, we have installed and are testing Command Post of the Future. CPOF is a U.S. Army program of record currently deployed in Iraq and Afghanistan. It is also used by U.S. Marine Corps forces in theater. The primary server (with clients) is located at 2nd Fleet so that Maritime Headquarters with Maritime Operations Center (MHQ w/MOC) personnel can observe CPOF operations.

To support at-sea testing, CPOF is installed in BHR and MIL to assess the communications capabilities of a ground force and tactical ship. The primary goal of TW08 is to assess CPOF’s ability to operate in a low bandwidth afloat environment. Thus far, we have found that during periods of high communications disconnect rates CPOF has recovered well with a graceful rebuild, as the clients and servers re-established communications.

At 7th Fleet, we have installed, and will leave behind, an experimental asynchronous transfer mode (ATM) switch connecting the 7th Fleet piers in Yokosuka, Japan, to the Regional Network Operations and Security Center West via a high-speed network. This will provide a 50 megabits per second dedicated point-to-point circuit and will provide 7th Fleet’s flagship, USS Blue Ridge (LCC 19), with greatly increased bandwidth when pierside.

At Pacific Fleet we are experimenting with two cross domain enablers, High Assurance Platform (HAP) and Global Command and Control System-Integrated Intelligence and Imagery (GCCS-13). HAP provides the capability to simultaneously display three separate security enclaves on a single workstation. We were

able to launch Common Operational Picture (COP), chat and a Web browser on three domains, Joint Worldwide Intelligence Communications System (JWICS), SIPRNET and CENTRIXS CMFP, with little to no degradation in performance.

GCCS-13 is designed to provide transparent COP and imagery sharing across multiple domains. We demonstrated that GCCS-13 reduced the number of servers while maintaining separation; however, we also determined significant effort is required to correctly integrate GCCS Track Management System data fields.

21 June

Although our TW08 installed systems are onboard to do experimental technical research, there are two examples of providing real-time support to the BHR Surface Action Group (SAG) during this transit.

The first is Raven 1100 Intelligent Agent Security Manager sponsored by the Navy’s Networks, Information Assurance and Enterprise Services Program Office, PMW 160, who reports to the PEO C4I. IASM provides enterprise-wide network threat management, composite security analysis and centralized control for network security operations. It operates as a single-point of interaction with the ship’s network and interface structure for shipboard program of record systems in response to DoD Instruction 8500.2 IA implementation requirements.

Operationally, IASM provides network administrators with an intelligent security monitoring and assessment capability that displays possible intrusions or unauthorized use of networks instantly. IASM also provides detailed information about the incidents.

During the past three nights, the CPR-7 and BHR network managers utilized IASM to detect shipboard violations in the following areas: DoD blacklisted Internet access from a ship’s computer system; e-mails with a virus-infected attachment leaving the ship; malevolent embedded ActiveX within a Shockwave flash file; detection of unencrypted passwords used for non-DoD Web site access; connecting to an online game server; spyware and malware; surfing to Web sites with inappropriate content; and bypassing the ship’s proxy servers to surf the Web undetected.

Today, another example [of IASM capability] resulted from the lack of Internet connectivity aboard the COM due to SHF an-



USS Bonhomme Richard (LHD 6) gets underway from San Diego, Calif., June 16, and pulls into Pearl Harbor, Hawaii, June 22.

tenna blockage. SPAWN and FAN were utilized by CPR-7, COM and BHR to exchange large documents and files. The transfers varied from Word and PowerPoint documents to a 350-mega-byte SHF technical manual.

22 June

Tonight, there are three network related experiments I want to highlight. The first is the PMW 160-sponsored Integrated Shipboard Network System Next Generation Technology (ISNS NGT). As you know, the ISNS is the shipboard local area network and the heartbeat of network operations. Though the current architecture has gone through many improvements and upgrades, the latest technology, ISNS NGT, will offer consolidated services through blade servers in a virtual environment, while saving space, weight and power requirements.

The new architecture is the first evolution in consolidating command and control systems, as well as many other shipboard operational networks and the shipboard LAN.

During TW08, we are testing a shore-based installation at the Pacific Fleet MOC and a ship-based installation aboard the BHR. The improved capabilities focus primarily on enhanced network management, computer network defense and information assurance and security.

On the BHR there are three suites: two SIPRNET and a NIPRNET. The 29 virtual servers on NIPRNET will replace about five racks of hardware; the 40 virtual servers on SIPRNET will replace about eight racks. By resource pooling, not one of the 69 applications hosted have experienced any degradation or limitation. Using virtual servers maximizes processor usage and RAM utilization while reducing the hardware footprint.

Another PMW 160 experimental endeavor is focused on meeting the mandates of DoD Directive 3000.5, which states that integrated civilian and military efforts are key to successful stability operations ... "the DoD shall be prepared to work closely with relevant U.S. Departments and Agencies, global and regional international organizations, U.S. and foreign non-governmental organizations (NGOs) ..."

In response to this mandate, the domain name servers at Pacific Region Network Operations Center and aboard BHR were modified to allow any laptop, military or NGO, access to any Internet Web site. This allows NGOs access to unclassified Web browsing, chat and instant messaging via some sites that are not normally available to a shipboard network.

This NGO network was installed without any significant problems and has been effectively functioning from day one. Not only have the multiple users been able to read e-mail normally blocked by the NOC, the TW deputy director successfully connected his personal Apple computer — after the proper security scans were performed. The observer logs and survey have all recorded satisfaction in the ease of use and ability to access Web mail.

Lastly, aboard the BHR, PMW 160 is experimenting with the ability to provide roaming capability to send and receive e-mail via a BlackBerry device. We have installed multiple wireless access points on the bridge and 02 level. These were accredited for use based on 802.11i capability and Federal Information Processing Standard (FIPS) 140-2 certification. We also installed a BlackBerry Enterprise Server. BlackBerry devices use cryptographic kernel technology that is FIPS 140-2-validated.



USS Bonhomme Richard Executive Officer Capt. John Funk and Ban Nguyen from PMW 160 are pleased with the success of the BlackBerry communications experiment at sea.

We have distributed these devices to several members of the BHR crew including the CO and executive officer. The initial feedback has been outstanding. In fact, earlier this evening the XO, Capt. John Funk said, as he held up his BlackBerry, "On behalf of the U.S. Navy, I thank you."

23 June

As of close of business today we have completed the experiment testing aboard Bonhomme Richard and at the ashore locations. We have exceeded all of our expectations on the level of detail and the amounts of raw data we have collected. We now begin perhaps the most difficult phase of Trident Warrior, sifting through the vast amount of data and performing relevant analysis.

I would also like to explain the data collection and analysis (DCA) element in more detail. The TW08 DCA team is led by the Naval Postgraduate School, but includes experts from a wide range of organizations, including Naval Surface Warfare Center Corona Division, SPAWAR Systems Center San Diego, Pacific Science and Engineering Group, Inc., Air Force Research Lab, Office of Naval Research, the Center for Naval Analyses and Naval Reserve Program 38, for a total of nearly 60 personnel participating.

The data collection planning we have done for TW08 is the most complete and focused data effort we have done in any previous Trident Warrior. There are nearly 250 specific survey and observer instruments, all made accessible via a Web browser.

Observer forms for every experiment event have been produced. The entire effort of more than 100 technologies and over 2,000 individual events is managed using the Web-based Trident Warrior FORCENet Innovation and Research Enterprise. FIRE provides the source for analysis and provides an archive to all past Trident Warrior information.

We will be releasing the TW08 quicklook message within the next two weeks followed by the final report in 90 days. CHIPS

The Maturation of Cyber Crime: It's a Job

Cyber crime is fast-growing and lucrative ... and increasingly easier using sophisticated automated tools

By James M. Belt

The dawn was cold and gray as Joe slipped on his coat and swallowed the last bit of coffee. Last night's research was profitable for his bank account and beneficial to the company. He was glad he followed that tip from his buddy on a new toolkit. It didn't cost much and he more than got his money back with his bonus check.

Sometimes he longed for the good old days as a command line commando. But, now that he's more mature, he likes that the tools allow him to have a personal life with a predictable daily routine. He stepped through the door into the damp mist and headed for home ...

The protection of our networks has become much more difficult than in the past when threats focused primarily on manipulating electronic funds and skimming cash from the careless. Over time, our economy has accepted information as a new commodity that is valued and in demand.

In the past and still today, hackers might try to use a stolen or hacked credit card to buy hundreds of dollars of items for resale. But the more lucrative market today is the sale of credit card numbers and personal identities — information.

Credit card numbers with valid ac-

count information can fetch up to \$5 per account, and bank account numbers with valid account information can yield up to \$400 per account, depending on available balances.

The incentive has shifted from the more risky use of the card or account to the sale of information. Figure 1 summarizes the monetary value of this underground economy.

Along with the increase in return for hackers, there has also been an increase in demand for tools or toolkits that automate hacking and identify vulnerabilities for possible exploitation.

The best tools and newly discovered system vulnerabilities are auctioned off to the highest bidders online, creating a thriving market for "black hat" software programmers. The tools automate repetitive techniques and probes, freeing up the user to do other things, or the user can leave the machine unattended and return later to collect the results.

The tools also add precision in targeting systems and information. The ready availability of tools means a hacker no longer has to be an expert in computer languages, or interface through the command line. Some tools even provide an easy to use graphical interface that makes hacking a point-and-click exercise.

When Joe returned that night, he grabbed a cup of coffee before checking his terminal for the results. His trained eye quickly spotted anomalies in the printouts. Eureka! One of the reports identified several improperly configured servers and multiple network and user systems without proper patches.



He quickly went to his computer files and retrieved the account and password information he had gotten several weeks ago by pretending to be a technician on the help desk. He now has all the pieces needed to attack his assigned target.

Joe heard the bump of the office doors closing and the arrival of one of the apprentices. Her youthful exuberance and naivety reminded him of his younger days as an idealistic social activist hacker.

Nothing felt as good as tagging a Web site or using his skills for political statements. As he got older, he got smarter. He realized he was being exploited by causes for the monetary gain of a few, and quit for awhile, until he was tipped off about this gig.

Despite his disillusionment, he still gets a sense of youthful satisfaction from defeating a challenge, but now the rewards are so much more substantial ...

The motives of hackers have changed with the increased reliance on the Internet by government and commercial firms for sharing and storing information.

In the earlier days of the Internet, hacking attracted the curious and the thrill seekers. Hackers were more likely to be inspired by the 1983 movie *Wargames* than any desire to become rich. Most crimes were thefts of telephone service (and later, cellular service) from the phone company or attempts to alter or "graffiti" Web pages. Hackers were motivated primarily by curiosity and for the prestige bestowed by other hackers.

Hacker clubs such as Legion of Doom and Masters of Deception attained great notoriety during this time along with individuals such as Kevin Mitnik and Kevin Poulsen. These early cyber crimes cost

Figure 1. Underground Cyber Economy

Rank	Item	Percentage	Price Range
1	Credit Cards	22%	\$0.50-\$5
2	Bank Accounts	21%	\$30-\$400
3	E-mail Passwords	8%	\$1-\$390
4	Mailers	8%	\$8-\$10
5	E-mail Addresses	6%	\$2 per megabyte-\$4 per megabyte
6	Proxies	6%	\$0.50-\$3
7	Full Identity	6%	\$10-\$150
8	Scams	6%	\$10/week
9	Social Security Numbers	3%	\$5-\$7
10	Compromised Unix Shells	2%	\$2-\$10

- Symantec Corp. - September 2007

phone companies and businesses money, but there was relatively little monetary gain for the hackers.

Today, with the continuing maturation of Web 2.0 and its emphasis on information sharing, the routine use of networks for information transfer, business transactions and daily organizational needs, the rewards for success have changed. Figure 2 is an illustration of cyber-security motives and their impact.

The availability of sophisticated tools adapted to hacking, the decrease in skills needed for success, the high return of successful exfiltration of information with the low risk of detection have also broadened the threat profile from “kiddie” hackers to well-organized and financed organizations.

Present day hackers may have electronically stolen millions of dollars from bank accounts by transaction skimming and other scams before getting caught. Statistics are not collected on the money lost to cyber crime but the Government Accountability Office in 2005 estimated \$67.2 billion in annual losses for U.S. organizations due to computer crime.

Defending against network threats is a difficult, but not impossible task. Identification of threats or threat actions are complicated since adversaries, allies, governments and the private sector all operate in the same virtual space.

Defenders of networks are overwhelmed by the speed of transactions and the volume caused by the huge Internet user population. Many of the current practices, techniques and technical solutions have lagged behind the increase in user sophistication and the evolution of information sharing technology.

The ability to share information is progressing far more quickly than the ability to prevent unauthorized information sharing because the focus of the Internet evolution is to remove impediments to information sharing and access for users.

The threat to the Defense Department is increasingly unacceptable because exfiltrated unclassified information could lead to insight about current and future warfighting capabilities.

Information has become a strategic asset to commercial competitors and rogue states because the business of America is conducted on the Internet. Statistics show a huge increase in incidents involving personal, business and

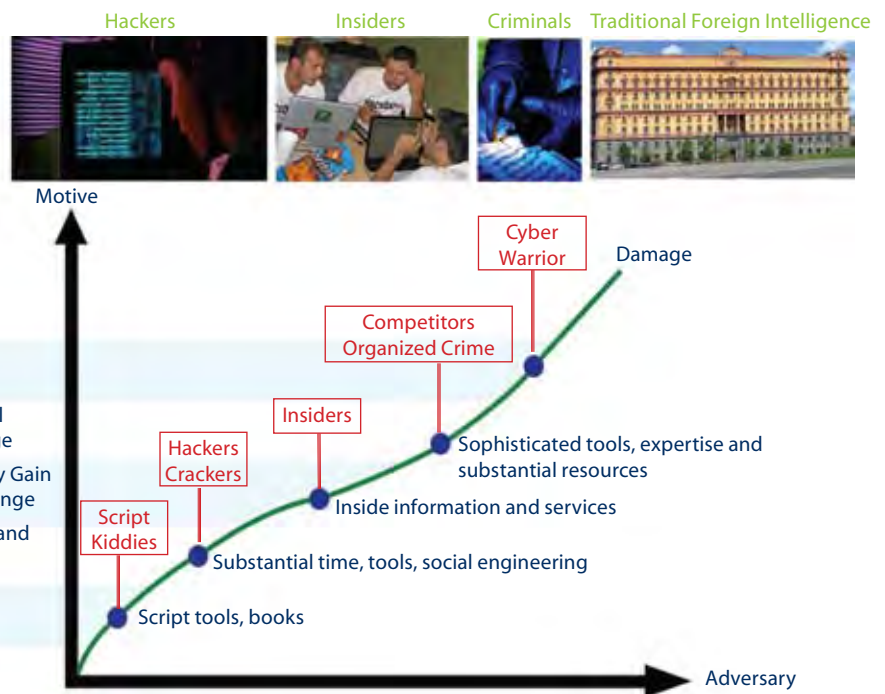


Figure 2.

government information. Figure 3 provides statistical data regarding the Internet threat.

After a few minutes, Joe was logged into the network on one of the compromised user accounts. Shortly after, he was able to exploit a common vulnerability in the network to establish a separate account with administrative privileges.

A quick scan of the system administrator console showed no active network monitoring engaged, just the usual auditing. That meant he could take as much time as he needed. It would be days or weeks before any review of the audit records would be conducted, if at all.

He used the help desk's own remote maintenance software to download the

data from the hard drives of pre-selected targeted computers. Before logging out, he installed a clandestine program that will operate in the background of the target machines to mine any future information. The program will also spread throughout the network in e-mailed documents to other users ...

Exfiltration, the unauthorized transmission of data from a system, is particularly difficult to detect since the user has no indication of data being stolen. Detection requires the recognition that transactions that appear normal, done in certain sequences and at different times, may indicate trouble.

Typically, most users aren't concerned

Figure 3. Internet Threat

53% rise in volume of Web site incidents

– Anti-Phishing Working Group Phishing Trends Reports November 2005 - November 2006
www.antiphishing.org/phishReportsArchive.html

784% rise in number of Web site scams

250% rise in targeted malware

– McAfee Avert Labs Blog
www.avertlabs.com/research/blog/?p=49

U.S. Computer Emergency Readiness Team incidents up 55% (FY07 versus FY06)

- 2,000 + detections per week
- 30% of malware library discovered in 2007
- 90% of new malware obfuscated
- 200,000 root kit installations in first half of 2007

As our computer systems become melded into the Global Information Grid, security of the DON's

"administrative" systems should be just as rigorous as the security applied to combat systems.

because the information they process is open and not proprietary or classified. The sense of security from this approach is being shattered by capabilities unleashed by the Internet and the powerful applications available for free.

Data mining software searches for key words or phrases, or uses other parameters to collect relevant information. This technique can download massive volumes of information, allowing the exfiltrator to leisurely search for new information or clues to link to DoD or proprietary commercial capabilities.

While any single piece of data may be unclassified or public, enough pieces put together may reveal sensitive information. For example, a data mining effort focused on an individual may find information in different places, such as date of birth, family members' names and relationships, address information (including old addresses).

From this information a profile of an individual can be built to allow the creation of accounts online and even determine a partial or complete Social Security number.

Similarly, in the military, compilation of unclassified data could reveal the existence of, and sometimes details about, sensitive or classified information or undertakings. In a simple example, a person could say in an e-mail that he will be unavailable to attend a meeting because he will be attending another meeting at an undisclosed location.

On another computer, orders are being prepared to send him to a named location and an American Express e-ticket is confirmed for a flight to an airport near that location. The timeframe overlaps the meeting he could not attend.

From this unclassified information, one can surmise that there is a sensitive meeting occurring on a classified subject at a specific place and timeframe. More searching through the unclassified data may ultimately reveal the subject, attendees, and possibly, an agenda. Exploitable but sensitive information is the "weapon of choice" in cyber attacks and exploitations.

Joe removed the DVD he created from his computer and carefully labeled it and put it in a case. He noted in his report where the information on the DVD was collected and a general description of its contents. He was thinking that with this big haul the analysts will have lots of fun going through the proprietary and sensitive information and sorting out personal identification information that can be sold.

He recorded the entire effort in his shift log. He placed copies of the report and DVD in an envelope marked "urgent" and put it in the drop box.

Joe thought it was ironic, as he put on his uniform jacket, that the same technology that allows him to collect this data makes his own network just as vulnerable to information theft, making "snail mail" the preferred method of distributing stolen information.

He paused at the door and looked back at his workstation. He kind of felt sorry for the administrators who will take the brunt of the blame once his work is detected. Joe spoke aloud, "Nuthin' personal, it's just a job," as if they might hear his apology. Then he went outside to begin his celebratory smoke break.

DoD is partnering with companies supporting the defense industry to improve the sharing of cyber security information. This allows better recognition of any interrelated actions that may be occurring across networks with sensitive defense data. Federal, state and local governments have been mobilized into national partnerships that work together to prevent damage to, and the unauthorized use and exploitation of, internal networks.

At the Department of the Navy, a cyber security task force is working to improve cyber security information exchange within the Department. The DON is also working to decrease its vulnerability by deploying data encryption software, improving network monitoring, reducing the number of Internet connections, and ensuring that it has eliminated the most commonly exploited vulnerabilities.

All users, developers and purchasers of DON systems play key roles in defending

the Department's networks. Below are some things users can do to remain vigilant in defending DON networks.

✓ Report anomalies such as unexplained installations occurring at start-up or an unfamiliar background program using up large amounts of resources.

✓ Help the private sector become aware of the problem. When working with contractors emphasize and discuss the security of sensitive government information on their networks.

✓ Collaborate with contractors to solve program security issues.


✓ Do not process information on public computers (e.g., those available for use by the general public in kiosks, hotel business centers, or the like), or computers that do not have access control.

✓ Transmit e-mail, text messages and similar communications using technology such as closed networks, virtual private networks (VPN) and public key infrastructure (PKI). Encrypt all wireless connections.

✓ Transmit facsimiles only when the sender has a reasonable assurance that access is limited to authorized recipients.

✓ Do not post information to a Web site which is publicly available or has access limited only by domain or IP restriction. Information may be posted to Web sites which control access by user ID and password, user certificates, or other technical means, which also provide protection via use of secure sockets or other equivalent technologies.

As our computer systems become melded into the Global Information Grid, security of the DON's "administrative" systems should be just as rigorous as the security applied to combat systems.

James Belt provides contract support to the DON CIO Information Assurance Team. 

DICE

DoD's Interoperability Communications Exercise

If you aren't prepared — you're rolling the dice

By Sharon Anderson

Since 1988, the Defense Department's Interoperability Communications Exercise has been the only DoD exercise whose primary purpose is to certify systems for joint interoperability.

This year, the Joint Task Force Civil Support (JTF-CS) hosted the civil response portion of DICE at its base of operations at Fort Monroe, Va., March 24-28. Briefly stated, the JTF-CS goal is to reduce the civil responders' risk of operational failure.

But mobilizing and coordinating the vast resources of federal, local and state governments, as well as the DoD, private industry and nongovernmental agencies, in responding to domestic catastrophes, are far from simple. At the same time, enormous improvements have been made at all levels in disaster response, according to exercise participants.

"We have come a long way. The notion that some might have that we have not learned the lessons of 9/11 or Katrina, or even lessons of Hurricane Dean this past year, or the California wildfires, are just not well-founded in fact," said retired Coast Guard Vice Adm. Roger T. Rufe, who is now director of the Operations Directorate in the Department of Homeland Security.

"We are generations better than we were in Katrina. We are safer today ... The nation needs to understand that."

Referring to the communications failures during Hurricane Katrina relief operations, FEMA's assistant administrator for Disaster Operations, Mr. Glenn Cannon agreed, "We have the ability now to communicate with people and places, which never existed prior to Katrina."

JTF-CS

The JTF-CS is a standing joint task force composed of active, Reserve and Guard members from the Army, Navy, Air Force, Marines and Coast Guard, as well as civilian personnel, and is commanded by federalized Army National Guard Maj. Gen. Daniel E. "Chip" Long Jr.

Established in October 1999, JTF-CS is a subordinate unit of U.S. Northern Command, a unified combatant command formed in October 2002 to plan, organize

and execute both homeland defense and civil support missions. When directed by the president or the Secretary of Defense, NORTHCOM provides defense support of civil authorities, including consequence management operations.

JTF-CS staff emphasized the critical role of civil support in domestic incidents in terms of speed and unity of effort between all the responders to provide a synchronized response.

Experts in their specialty areas, staff members anticipate, plan and integrate NORTHCOM chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) consequence management operations. The team trains according to the maxim, "Not if ... but when," because their efforts are always part of a larger, in-parallel response with other government and nongovernmental agencies.

DICEVILLE

In Hampton, the JTF-CS worked alongside operators and subject matter experts from DHS, the Federal Emergency Management Agency, NORTHCOM, and various local, state and federal inter-agency partners, including the cities of Norfolk, Virginia Beach and Hampton, the American Red Cross, Customs and Border Protection, 35th Signal Brigade, Civil Air Patrol, Federal Aviation Administration, the National Guards of Virginia and West Virginia, and others.

The exercise tested communications capabilities such as radio to cell phone at the first responder level, information

sharing at the operational level and long-haul satellite communications, and reach-back testing at the strategic level.

To demonstrate these capabilities, NORTHCOM and JTF-CS sponsored a media tour of "DICEVILLE," a series of vehicles, trailers and tents which housed some of the communications tools tested.

Some of the senior representatives from the participating agencies also took the tour March 27.

In addition to Rufe and Cannon, other representatives included Commander North American Aerospace Defense Command (NORAD) and USNORTHCOM Air Force Gen. Victor E. Renuart Jr.; then Director, Command and Control Systems NORAD-USNORTHCOM J6 Navy Rear Adm. Kendall L. Card, who is now commander of Expeditionary Strike Group 3; Commander of U.S. Marine Corps Forces Command Lt. Gen. Joseph F. Weber; Maj. Gen. Long; and director for Communications Systems, JTF-CS, USNORTHCOM, Air Force Lt. Col. Theodore P. Henrich.

"All the people that are out there on the DICE field are working together, sharing ideas, they are networking, they are getting to know each other, they are passing out business cards. The next time we need to go out to react to a crisis, they are going to know each other, know what each other's capabilities are, and we will be better off," Henrich said.

Participants commended the DICE structure because it provides an environment for communicators to practice "inter-talk-ability."

Ft. Monroe, Va. (March 21, 2008) – Senior Airman Matthew Keen, Senior Airman Lonnie Stringer and Airman 1st Class Cody Hart of the 54th Combat Communications Squadron set up a communications antenna in preparation for the start of DICE 2008. U.S. Navy photo by Petty Officer 3rd Class Jennifer Wolfe.



The network tested at DICE 08 comprised communications systems currently in use (or about to be fielded) and was established and manned by the actual owners and operators of the equipment. System developers and industry partners were also on hand to resolve interoperability issues that could degrade performance.

Because DICE employed a robust joint architecture along with the actual operational personnel to install, operate and maintain the equipment, the exercise environment was characteristic of those used by the civil response community during real-world operations.

Communications in Civil Support

DICE used advanced communications technology, but participants focused on response procedures to display a common operational picture and share operational-level information in response to a scenario that included a nuclear detonation in New Jersey resulting in a CBRNE incident.

"I think one of the important things that you realize, for emergency response is [that] communications are the backbone. If communications fail, then the mission can fail and if this mission fails, people can die," Cannon said.

Some of the capabilities demonstrated included mobile command and control units from the FBI, Virginia Emergency Response Support, Army and National Guard, and FEMA. The FEMA Mobile Emergency Response Support trailer-sized detachment is used for tactical logistics and communications support. There are six located throughout the United States.

The 34th Civil Support Team and 35th Civil Support Team demonstrated a vehicle with a deployable satellite antenna, handheld radios, in fact, everything needed for communications on-the-fly. A vehicle of this type was sent to Puerto Rico in response to Hurricane Dean and in support of the Department of Transportation for the bridge collapse tragedy in Minnesota.

"Almost every vehicle out here has a gateway that allows disparate radio systems to talk to each other. We are on the cutting edge of technology and shifting to where everything will be voice-over IP. People on a cell phone can talk from their office and speak to the incident commander at the scene of the incident, that's being tested here today. The good news is that it works," Cannon said.

Despite dramatic improvements in emergency response, agency participants agreed that exercises like DICE are still



One of the mobile communications vehicles exhibited at DICEVILLE.

needed because of problems that may develop when trying to integrate new technologies, legacy systems and changing response partners.

"We just saw a company from Fort Bragg using the next generation technology integrating it into the old technology. You cannot abandon the existing technology. It would take \$40 billion to replace that in our country in terms of public infrastructure," Cannon said. "You can't do that. You have to have a way to make what local fire, police and EMS (emergency medical services) guys have today to talk to all these other responders without replacing it. That is where these interoperable missions become so critical."

DICE also enables agencies to test new procedures resulting from the hard lessons learned in past relief efforts.

"We have come a long way since Katrina and, of course, it will continue to develop and improve with exercises and opportunities like you see here. I was at Katrina, I had three cell phones and a hard line into my office and at one point, I could not communicate with anyone," Long said.

The National Response Framework

Because the nation has faced an unprecedented series of disasters and emergencies, the national response structures have evolved and improved to meet these threats. The National Response Framework reflects those improvements and replaces the former National Response Plan.

Joint Task Force – Civil Support

JTF-CS is a standing joint task force comprised of active, Reserve and Guard members from the Army, Navy, Air Force, Marines and Coast Guard, as well as civilian personnel, and is commanded by a federalized National Guard officer.

The purpose of JTF-CS is to save lives, prevent injury and provide temporary critical life support.

While hoping the need never arises, JTF-CS stands ready to aid the designated lead federal agency, most likely FEMA, in charge of managing the consequences of a CBRNE, or chemical, biological, radiological, nuclear or high-yield explosive, accident or incident.

JTF-CS is the only military organization dedicated solely to planning and integrating DoD forces for consequence management support to civil authorities in such a situation.

JTF-CS at a glance

- *Deployment of JTF-CS is at the direction of USNORTHCOM, and on authority of the Secretary of Defense, only after a governor requests federal assistance from the president, and after the president issues a Presidential Disaster Declaration. This would only occur at the request of civil authorities when local, state and other federal resources are insufficient to meet the emergency;*
- *JTF-CS selects personnel based on their expertise and provides additional training to prepare them for executing consequence management operations;*
- *JTF-CS interacts with many federal, state and local agencies in accordance with the Stafford Act;*
- *DoD does not assume control of the response and always works in support of the lead federal agency in charge of the overall effort.*

The National Response Framework establishes a comprehensive all-hazards approach to enhance the ability of the federal government to manage domestic incidents. The framework, which became effective March 22, 2008, identifies the key response principles, as well as the roles and structures that organize national response. It describes how communities, states, the federal government and private-sector and nongovernmental partners apply these principles for a coordinated, effective national response.

“Part of what FEMA does every day, part of the National Response Framework, is to make sure that locals can speak to each other. All the grant funds that we send to local governments to support their communications have to be part of state-approved plans that are then reviewed by FEMA regions,” Cannon said.

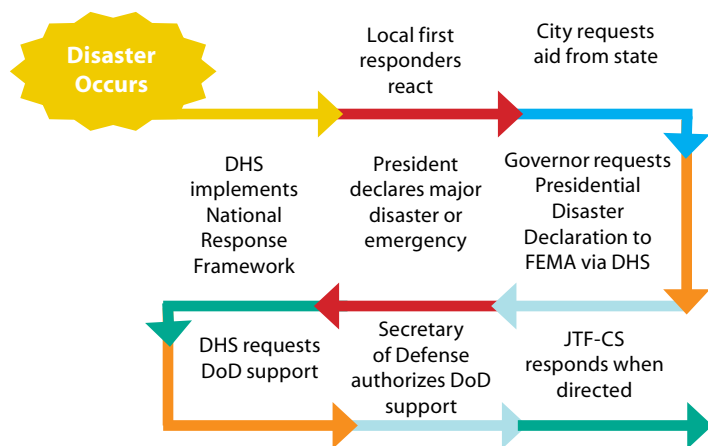
“You won’t get dollars any longer just to buy hardware, you have to be partners. The National Response Framework, this exercise, and the national communications plan, are all pieces of the federal government’s unified response to an emergency.”

DoD Support to Civil Responders

USNORTHCOM’s civil support mission includes domestic disaster relief operations that occur during fires, hurricanes, floods and earthquakes. Support also includes counter-drug operations and managing the consequences of a terrorist event employing a weapon of mass destruction. The command provides assistance to a lead agency when tasked by DoD. Per the Posse Comitatus Act, military forces can provide civil support, but cannot become directly involved in law enforcement.

Gen. Renuart explained the process for states to request Defense Department assistance. He said the first military responder is always the National Guard, but any response begins with local responders.

“First and foremost, all events will begin locally. It doesn’t matter how big it grows. As you see the seriousness of the event de-



DoD Civil Response Process. The first military responder is always the National Guard, but any response begins with local responders, such as firefighters, law enforcement and emergency medical personnel. Detailed federal guidelines, both statutory and regulatory, govern the organization, funding and operation of the National Guard, as well as Department of Defense assistance in the event of an emergency. Although the formal request for DoD assistance must go through all the appropriate levels for approval, providers in concert with other agencies, such as FEMA, DHS and USNORTHCOM, are simultaneously planning their relief response.



Responding to media questions at the DICEVILLE demonstration: federalized Army National Guard Maj. Gen. Daniel E. “Chip” Long Jr.; retired Coast Guard Vice Adm. Roger T. Rufe, now director of the DHS Operations Directorate; NORAD-USNORTHCOM Commander Air Force Gen. Victor E. Renuart Jr.; and FEMA’s assistant administrator for Disaster Operations, Mr. Glenn Cannon.

velop, then municipal leadership and state leadership will make a determination that some form of military support is needed. Normally, the governor will pull National Guard teams in.

“There is a relationship among the states, the EMAC (Emergency Management Assistance Compact) that allows mutual aid, Guardsmen from other states, or to pull in civilian responders through FEMA, to give more muscle and capacity,” Renuart said.

Detailed federal guidelines, both statutory and regulatory, govern the organization, funding and operation of the National Guard, as well as Department of Defense assistance, in the event of an emergency.

“There is a prescribed process, the state requests a declaration from the president for disaster response and that enables funding to flow to allow DoD to provide the support. That sounds like a lengthy process ... but the reality is that we can see what the fire chief sees almost immediately because of exercises like this. So we can begin to ask ourselves in DoD, what might that state need and begin to marshal that at the same time,” Renuart said.

“In many cases, and the [Minneapolis] bridge is a good example, it took a series of about four phone calls from the governor to the Secretary of Transportation to the Secretary of Defense.”

The general discussed the specialized assistance that the DoD can provide that often doesn’t exist at the local or state level.

“During the hurricane season this past year, Hurricane Dean was threatening the Texas coast. The state of Texas has a very well-developed hurricane response plan, but one of the areas where they had a requirement for support was in evacuation of unique medical patients, some critical care, some very aged. That capacity doesn’t exist in large numbers in an individual state. DoD was asked to provide capability to move some of those critical care patients.

“In Minnesota, when the bridge collapsed, the state had a very good capacity to respond to the structure failure and in the first response to those injured. However, the state, and truly anywhere in the federal government, you did not have capacity to put divers in the water to operate in that environment to help recover the remains of those killed, so DoD was asked to provide Navy salvage divers to go in there,” Renuart said.

Both Renuart and Cannon talked about how pre-scripting

consequence management has led to quicker and better coordinated response efforts.

"In 2006, we had 44 pre-scripted mission assignments with four other federal agencies — DoD being one of them — the main one. Today, we have over 240 with 31 federal agencies. That is a tremendous difference in a year and a half's time. We don't want to wait until we are in the middle of the event to call our friends at DoD and say, now we need some help," Cannon said.

The comprehensive domestic response structure relies on continuous information sharing and contact among support providers for crisis planning. Providers emphasized that procedures are planned collectively so that each agency can respond to an emergency without hesitation.

"We look within each of the 10 FEMA regions [for] the kinds of events that could occur within that region that you can somewhat predict, not the timing, but at least the type of event. Then we begin to try to identify those shortfalls in capacity that may exist among the states or among the various federal partners and look out into DoD to see how we might help fill that gap," Cannon said.

Although the formal request for assistance must go through all the appropriate levels for approval, providers are simultaneously planning their relief response.

"There is a process involved, but underneath that, we have the agencies talking to each other in real-time almost as the event occurs. You can look at floods in the Midwest in the last few days — FEMA, DoD and the states were all talking to each other about what might be needed if the flooding level began to expand beyond what was predicted," Cannon said.

Inter-talk-ability

While interoperability between agencies and response times improved tenfold, improvements required a cultural shift in how agencies were organized to provide emergency support.

"At this moment, interoperability technologically is not all that difficult; it's the culture of people communicating with each other. I was, at one time, in charge of a major metropolitan police department, and the FBI wanted to come up on my radio system. I did not want the FBI on my radio system, unless I asked them to be on my radio system," Cannon said. "Those kinds of issues you have to resolve and deal with.

"We realized that our internal communications needed to interoperate well. So today, I have FEMA staff stationed out at NORTHCOM. Every one of our FEMA regions has a defense coordinating officer in that region, it facilitates that communication, and it does it the moment there is a beginning of a sign that something is occurring," Cannon continued.

"We are breaking down those cultural barriers so that we can talk when we have to talk to each other."

JTF-CS – www.jtfc.northcom.mil
USNORTHCOM – www.northcom.mil
FEMA – www.fema.gov
DHS – www.dhs.gov
EMAC – www.emacweb.org

Navy ERP Achieves Initial Operational Capability

A major milestone in the Navy Enterprise Resource Planning program was achieved May 12 in ERP's acquisition life cycle. The attainment of initial operational capability (IOC) signals a significant step in bringing Navy ERP, the Navy's integrated business management system, to 88,000 users across the service when fully implemented.



Calvin Newby, head of testing for Navy ERP, and Terry Mitchell, test team member from NAVAIR, work on the extensive test program executed by the Navy ERP program, part of the rigorous requirements necessary for the program to achieve initial operational capability.

The Navy ERP program brings total asset visibility and financial transparency to Navy business operations as part of the Navy's transformation of its business affairs.

The system, now in operation at the Naval Air Systems Command (NAVAIR), integrates management functions in program management, finance, workforce management, supply and maintenance into one system that standardizes and modernizes Navy business practices.

The program constitutes the Navy's adoption of best commercial business practices as it employs a commercial off-the-shelf (COTS) system that is in use in hundreds of private, commercial concerns.

The Navy conducted four pilot programs to assure that the unique requirements of the Department of Defense and Navy could be successfully supported by a commercially-based system. Lessons learned testing from the pilots allowed the Navy ERP program office to develop the system that will meet the Navy's requirements while increasing the effectiveness and efficiency of its business operations.

"Achieving IOC is a significant and well-deserved accomplishment for the Navy ERP program and a transformational step forward for the Navy Enterprise," said Rear Adm. Tim Flynn, Program Executive Officer for Enterprise Information Systems (PEO EIS). "The IOC milestone recognizes the dedication and tireless energy of the Navy ERP team in bringing this essential capability to the warfighter."

Release 1.0, now operating at NAVAIR, serves as the foundation of the Navy ERP system, and encompasses financial, program management and workforce management capabilities. In October of this year, Release 1.0, will be rolled out to the Naval Supply Systems Command and is scheduled to be implemented at the Space and Naval Warfare Systems Command in October 2009.

Release 1.1, which is currently under design, will be the Navy's *Single Supply Solution*, combining the operations of retail and wholesale supply support for the Navy. This release is scheduled for implementation at the Naval Supply Systems Command in February 2010.

"We are extremely pleased that IOC has been reached. This program has been a very complex undertaking, requiring the best of the remarkable talents of our program team. This IOC declaration affirms the transformation of the Navy's business practices is on track to achieve great things for the Navy," said Valerie Carpenter, acting program manager for the Navy ERP program.

The Navy ERP program uses a product produced by SAP, and is the largest ERP implementation in the Department of Defense — and among the largest implementations ever accomplished.

Navy ERP is a Department of the Navy PEO EIS program. Go to www.spawar.navy.mil, for information about the PEO EIS.

CHIPS

CHIPS

Department of the Navy Architecture Federation Pilot

The Defense Department recognized that the current approach of attempting to develop monolithic integrated architectures has not worked well. Consequently, DoD has developed a concept of architecture federation ...

By Brant Frey

The Defense Department knows that the structured analysis associated with architectures is essential to transform its platform-centric environment to a net-centric environment. This change will eliminate silos of data and information, thus making information visible and accessible to all authorized users.

However, the DoD recognized that the current approach of attempting to develop monolithic integrated architectures has not worked well. Consequently, DoD has developed a concept of architecture federation.

The Architecture and Interoperability Directorate of the office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) published the Global Information Grid (GIG) Architecture Federation Strategy version 1.2 in August 2007 (available on the Department of the Navy CIO Web site; search for Enterprise Architecture). It outlines the basic concepts and principles underlying architecture federation.

The DoD strategy has been kept at a high-level to allow each service to develop a tailored implementation plan. Allowing each component to tailor an implementation plan is consistent with the spirit of the federation approach. It endeavors to provide a minimum set of rules and standards from the higher echelons within the DoD while allowing maximum flexibility at subordinate echelons.

This article outlines a portion of the DON's implementation of the DoD federation strategy. It approaches DON architecture federation from the perspective of developing a repeatable process that, when applied to any number of architectures, produces a consistent result. The DON EA Federation Pilot Report 1.0, scheduled for release this summer, will outline processes, essential inputs to these processes, expected outcomes, and the rules required to achieve consistent success.

Architecture federation serves in part as a process for relating or aligning subordinate and parent architectures via the mapping of common architecture information. At the same time, federation provides an organizing construct that allows uniqueness and autonomy throughout the enterprise. These aligned architectures are subsequently located and linked through an architecture management service, allowing consistent search and discovery.

This alignment and discovery provide critical insight into the enterprise, improving interoperability and reducing overlaps and gaps. The ability to maintain line-of-sight for strategic missions and goals to the systems that instantiate those objectives is achieved. This enhances not only the ability to view duplica-

tive or overlapping systems, but also the ability to identify those systems that need to be developed to fulfill a desired capability gap.

The DON views architecture federation as consisting of five central elements that govern the process and the methodology of federation: tiered accountability, categorization, semantic alignment, reference architectures, and search and discovery, as illustrated in Figure 1. Together these elements provide the framework for effective federation of DON architectures.

Architecture federation techniques recognize that the re-



Figure 1.

sponsibility for architecture development is shared at several echelons or what the DoD federation strategy calls tiers. Tiered accountability establishes a hierarchy of architectures whereby subordinate architectures inherit characteristics from the higher level architectures in a parent-child relationship. The basic concept behind tiered accountability is to architect down to a minimum amount of detail at each tier to establish clear touch points between the tiers. This concept is shown in Figure 2.

To deal with the complexity and diversity of the enterprise,

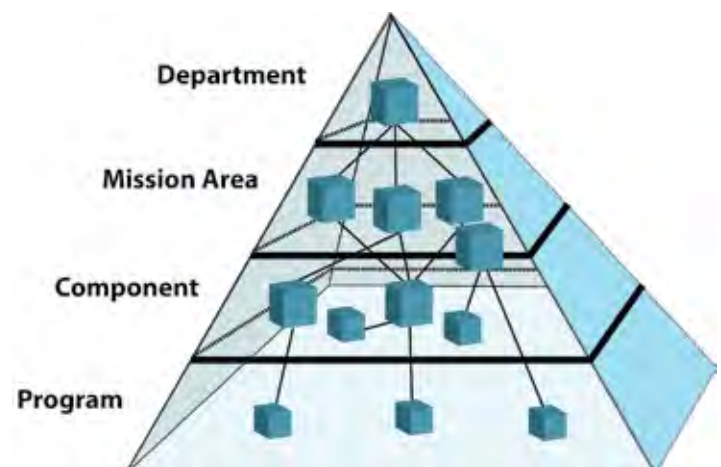


Figure 2.

Any successful federation effort is dependent upon making architecture artifacts visible and accessible to analysts, planners and decision makers at all levels.

this concept sets the stage for dividing the enterprise into manageable components. These components can be described and documented by the communities that are most closely associated with them using a set of standard rules and practices.

Ideally, only a small set of rules, common terms and standards are inherited from the parent architectures to maintain consistency throughout the enterprise and effective high-level guidance from each higher tier.

The DON's federation process provides a method for linking or aligning subordinate and parent architectures via the mapping of common architectural information. This concept advocates subordinate architecture alignment to the parent architecture. For alignment, the operational activity model (OV-5) node tree, which describes the activities that are normally conducted in the course of achieving a mission, capability or a business goal, serves as the basis for federation and acts as a reliable touch point between architectures.

This is based on the belief that activities are of an enduring nature. Capabilities will change over time as will the processes and systems that instantiate those capabilities. As activities are aligned throughout the enterprise to a tiered taxonomy, the ability to trace capability development in systems can be effectively realized.

The subsequent ability to direct, change, challenge or administer architecture development is guided from above rather than below. Consistent with the idea of tiered accountability, a series of DON level reference architectures and DON mission-level reference architectures (detailed in Figure 3), which are effectively aligned to high-level capabilities, can serve as the parent taxonomies for program architectures to utilize.

The semantic alignment of activities to a parent or reference architecture is achieved by using a four-part grading system that qualifies the strength of the relationship between activities. These

mapping relationships are qualified as equivalent to, part of, similar to, or no relationship.

The activities and the relationships are then captured in a federation tool called the Federation Log. To facilitate both search and discovery, the process developed will leverage this consistent methodology to capture the taxonomy output of the federation process.

The "FedLog" is a standard means of capturing the output of the federation process while offering a searchable and discoverable document that will facilitate reuse of the federation effort and serve as an architecture analysis and quality control tool.

Any successful federation effort is dependent upon making architecture artifacts visible and accessible to analysts, planners and decision makers at all levels. As part of the DON federation strategy, there is a focus on making the products accessible and visible through the use of GIG Architecture Enterprise Services.

The GAES would work in conjunction with other DON repositories such as the Naval Architecture Repository System (NARS) and the Systems Command Ar-

chitecture Development and Integration Environment (SADIE) to provide a search and discovery service that would allow an authorized user access to relevant architecture products.

Employing an architecture service alleviates the need for the DoD to create a single massive repository. Instead, architectures can be registered in the DoD Architecture Registry System (DARS), indicating that their products are contained within service-level repositories.

Using a federation approach, the DON expects to achieve the following results:

- Decompose the DON enterprise into logical mission segments based on traditional mission areas, horizontal tiers and the echelon level at which the architecture must exist;
- Demonstrate clear program alignment with mission architectures, as well as alignment with the DoD-level architectures;
- Use the federation techniques to identify gaps and overlaps in existing architectures;

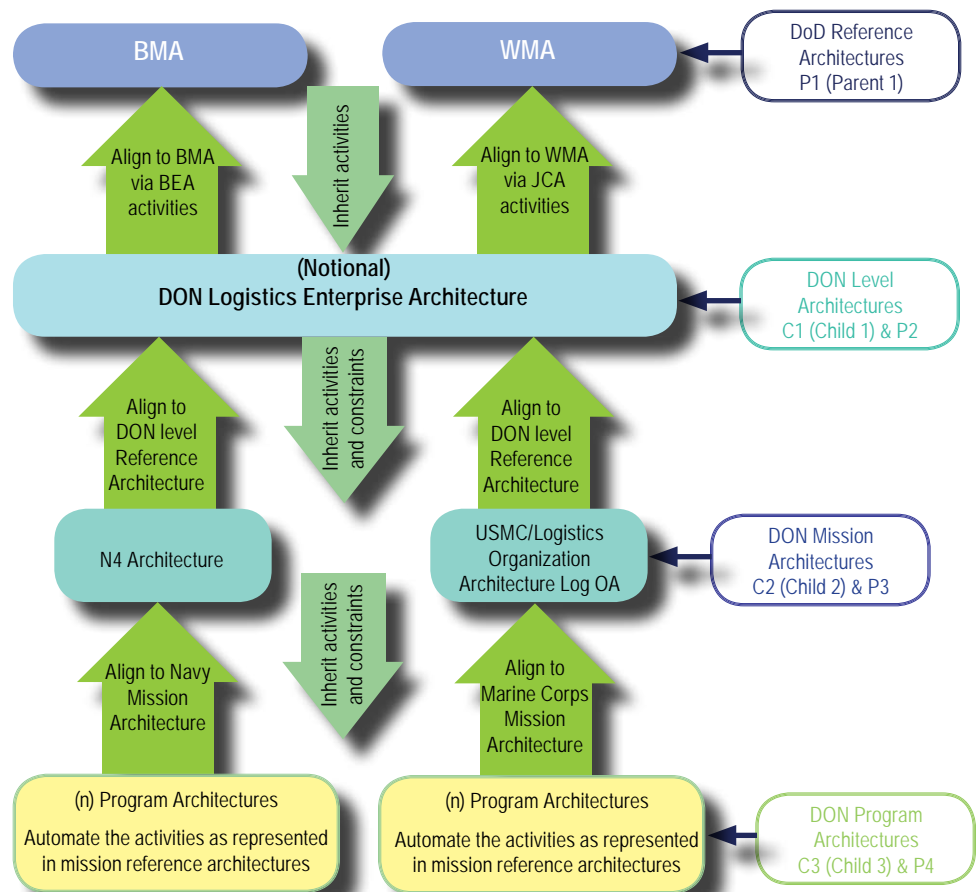


Figure 3.

- Provide a basis for each program to demonstrate how it contributes to naval and joint missions;

- Identify strengths in current systems and their contribution to required naval capabilities;

- Leverage existing architecture investments and reuse the artifacts as a starting point for creation of the larger federation;

- Increase insight into the interactions and dependencies among DoD/DON missions, organizations and systems;

- Improve architecture information sharing;

- Improve investment decisions; and

- Establish enterprise boundaries.

The federation process and model were tested through a pilot program using both a Navy command and control architecture and a Marine Corps logistics architecture that aligned to both the Business Enterprise Architecture and the Warfighter Mission Architecture.

The federation process is independent of any particular enterprise hierarchy but will work as long as a defined tiered structure and a tiered accountability construct are established.



In April 2008, the Booz Allen Hamilton team working with the DON CIO was presented with a Department of Defense Enterprise Architecture Achievement award — a first from the DoD. The award recognized significant contributions in advancing enterprise architecture for the DoD.

Web links:

DON CIO – www.doncio.navy.mil

ASD(NII)/DoD CIO – www.defenselink.mil/cio-nii/

Brant Frey provides support to the DON CIO Enterprise Architecture team.

CHIPS



– Artist's conception of a WGS satellite in orbit

Navy transitions to Wideband Global System

By NETWARCOM Public Affairs

Operations Coordination and Execution Lead Capt. Kevin Johnson, at Naval Network Warfare Command, recently announced the transition of Pacific fleet communications to the Wideband Global System (WGS-1), the first of a series of six new generation communications satellites that will dramatically improve NETWARCOM's ability to provide timely and accurate information and decision superiority to the fleet.

"This is a tremendous first step in improving our communications, both afloat and ashore. It will not only improve our tactical communications but will also allow us to conduct our logistics and other routine communications in a more timely manner and allow Sailors more flexibility to complete online training courses and communicate with their families," Johnson said.

Each WGS satellite provides more communication capability than the entire Defense Satellite Communications System (DSCS) constellation and has been eagerly anticipated by Navy forces in the Pacific theater. Follow-on WGS-2 and WGS-3 will provide improved communications capability in the Indian Ocean and Atlantic.

The WGS program augments, and will eventually replace, the existing DSCS which provides super high frequency (SHF) wideband communications. The reconfigurable antennas on WGS satellites will enhance fleet operations by increasing the commander's ability to tailor coverage areas to match operational scenarios.

Navy carrier and expeditionary strike groups will use WGS to provide high-capacity connectivity between ships and into the terrestrial portion of the Defense Information Systems Network (DISN). Ships operating in the Western Pacific will have the first opportunity to use these new satellites. USS Fitzgerald (DDG 62) was the first ship to access WGS-1 during its recent transition to operational status.

The WGS satellites are key elements of a system that is expected to provide a significant increase in global communications capabilities for the fleet. These satellites provide communication capacity, connectivity and flexibility for Navy forces afloat and ashore.

The WGS constellation will maintain interoperability with existing and programmed X-band and Ka-band satellite terminals. WGS supports the Navy's warfighting information exchange requirements, enabling execution of tactical command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR); battle management; and combat support information.

WGS also augments the current Ka-band Global Broadcast Service (on UHF follow-on satellites) by providing additional information broadcast capabilities.

"We'll be closely monitoring the transition to WGS to ensure we are using it to its fullest capacity and are eagerly awaiting WGS-2, WGS-3 and the rest of the Wideband Global System constellation," Johnson said.

NETWARCOM is the Navy's type commander for networks, information operations, space and intelligence, and the central operational authority responsible for providing ready information professional, information warfare and intelligence forces.

For more information, go to the NETWARCOM Web site at www.netwarcom.navy.mil.

CHIPS

Key tactical data link systems clear operational testing

NGC2P, MIDS on ship programs prepare for fleet introduction

By Steven A. Davis and Mike O'Gara

The Navy's Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I) announced the successful testing of two critical components of its planned upgrade to the Tactical Data Link (TDL) system aboard Navy ships.

The Next Generation Command and Control Process (NGC2P)/Common Data Link Management System (CDLMS) and the Multifunctional Information Distribution System (MIDS) on Ship (MOS) each achieved positive results in recent testing conducted by the Navy's Operational Test and Evaluation Force (OPTEVFOR).

The tests were conducted over several weeks and involved elements of the Navy, Marine Corps, Air Force and NATO. The MOS system accumulated more than 430 operating hours over a 19-day period aboard USS Tarawa (LHA 1), both in port in San Diego and at sea in the local operating area.

The NGC2P/CDLMS system accumulated more than 100 hours over a five-day period aboard the cruiser USS Port Royal (CG 73) and destroyer USS Hopper (DDG 70). Both systems were found to be operationally effective and operationally suitable.

"The effectiveness of our operating forces is largely determined by their ability to receive and process information, and then use that information to protect themselves and deliver their weapons accurately — 'put rounds on target,'" said Chris Miller, who heads the PEO C4I organization. "These successful tests are a major step forward in enhancing that capability for our warfighters."

Tactical Data Link

Tactical Data Link systems transfer information quickly and securely between military assets. Information can be sent via an orbiting satellite, an aircraft operating overhead or a system of ground links. These systems allow ground troops operating in Afghanistan, for example, to transmit near real-time information to a Navy ship operating in the Persian Gulf.

The existing TDL system is the Joint Tactical Information Distribution System (JTIDS), a network radio system used by the U.S. armed forces and its allies to support data communications, principally in air and missile defense. JTIDS is one of the family of radio equipment that compose the JTIDS/TDL J system, commonly referred to as Link 16, a highly survivable radio communications data link that provides reliable situational awareness for fast-moving forces.

Link 16 data communications standards and technology were developed in 1975, with the first JTIDS terminals installed on Air Force AWACS aircraft and at U.S., U.K., and NATO ground-control facilities. Smaller Link 16 terminals, called MIDS-Low Volume Terminals (LVT), were developed to equip U.S. fighter aircraft, specifically the F/A-18 Hornet.

The MOS system is the next generation Link 16 TDL terminal and is designed to replace the older JTIDS terminals on newly constructed Navy ships. MOS was developed to meet the Navy's continued need for a Link 16 terminal. It is based on the MIDS-LVT Link 16 receiver-transmitter, but includes additional software to allow the system to interface to the ship's combat system.

The NGC2P/CDLMS system is designed to enhance the ability of Navy ships to be made aware of incoming threats. The system also allows Navy ships to strike targets over the horizon by providing improved connectivity, enhanced throughput and extended range of TDLs, including Link 16.

OPTEVFOR released the NGC2P operational test report Feb. 21, 2008. The report evaluated the NGC2P (version 3.4x), with Joint Range Extension Application Protocol (JREAP) C capability, to be operationally effective and suitable for fleet use on all U.S. Navy Model 5 combat systems-equipped ships.

JREAP-C enables Link 16 tactical data to be transmitted over digital media and networks not originally designed for tactical data exchange. Formatted tactical digital messages (J-series) are embedded inside JREAP messages as data fields within available commercial and government protocols using Transmission Control Protocol and User Datagram Protocol, both of which are the core protocols of the Internet protocol suite and are commonly used over satellites and terrestrial links.

NGC2P

NGC2P is the follow-on to the C2P program initiated in 1982 that converged three separate data links into a single system interface. That system is used today in the fleet aboard aircraft carriers, cruisers, destroyers and large amphibious warships.

NGC2P employs a satellite data link for the exchange of information. The satellite link reduces the reliance on airborne link relays, and will relieve current constraints on battlefield deployment due to line-of-sight and network saturation limitations in large combat theaters of operations.

NGC2P leverages JREAP-C, which will provide forces greater range enhancements and improve the Navy's and Marine Corps' ability to operate with joint forces. The JREAP-C capability provided by NGC2P is also used by the Aegis Ballistic Missile Defense system as a mission-critical communication link.

Each system must clear a final hurdle before being introduced to the fleet. NGC2P is expected to receive full-rate production approval this summer and will then be installed aboard all Navy combatant ships by 2012.

The final step for the MOS system is the award of a production contract, also scheduled for this summer. It will be installed on new construction ships.

NGC2P is managed by PEO C4I's Command and Control Program Office (PMW 150), which oversees pre-planned product improvement of the C2P. The function of NGC2P is to enable platforms to accurately process and exchange tactical data with Navy, joint and coalition forces over any combination of TDLs to achieve a common tactical picture.

The NGC2P is designed to be extensible and flexible to meet the mission requirements of a constantly changing warfare environment. The NGC2P provides critical support to the Navy transformation elements by providing improved connectivity, enhanced Link 16 throughput and extended range to the TDLs.

Connectivity and extended range enhancements will be sup-

ported in current and future NGC2P builds incorporating Link 11, Satellite Link 11, Link 16 and Satellite Link 16 and through the incorporation of JREAP Appendix A and Appendix C, Link 22 and Link 16 line-of-sight Dynamic Network Management capabilities.

JREAP-C is a significant improvement supporting beyond line-of-sight and multimedia ultra high frequency (UHF), extremely high frequency (EHF) and super high frequency (SHF) Link 16 capabilities that are interoperable with joint services.

Testing is essential to success

Extensive developmental testing was conducted to ensure a successful operational test at sea aboard USS Milius (DDG 69) and in port aboard USS Lake Erie (CG 70) with support provided by the Space and Naval Warfare Systems Center (SSC) San Diego Combined Test Bed lab over a three-year period. Testing events grew in both fidelity and complexity to include a variety of Navy ships underway supporting carrier strike group operations.

The successful CDLMS technical evaluation was conducted during the bilateral Annual Exercise (ANNUALEX) '07. This week-long exercise is designed to enhance the United States' and Japan's ability to better respond to the defense of Japan or any regional crisis in the Asia-Pacific region.

The evaluation was coordinated by the test team lead, Aaron Hubbard, in SSC San Diego Code 535, aboard the USS Kitty Hawk (CV 63) and executed with contractor team members aboard USS Shiloh (CG 67) and USS Stethem (DDG 63).

The operational testing included risk mitigation testing and alignments by the Link 16 In-Service Engineering Activity and the CDLMS Software Support Activity in port onboard USS Port Royal (CG 73) and at sea onboard USS Hopper (DDG 70).

The operational test was conducted at sea onboard Port Royal, Hopper, with support by Tarawa, and the SSC San Diego Combined Test Bed lab.

Future enhancements to the CDLMS program include added ballistic missile defense improvements, implementation of Net-Enabled Weapons message processing capability and expansion of IP ports to communicate directly to Global Command and Control System - Maritime and the shipboard combat system.

This successful testing was part of the Space and Naval Warfare Systems Command's continuing effort to deliver effective capabilities to the warfighter.

"NGC2P enables platforms to accurately process and exchange tactical data with naval, joint and coalition forces over any combination of Tactical Data Links in order to achieve a common tactical picture," explained Paul Bobrowich, PMW 150 principal assistant program manager for tactical command and control. "It is designed to be extensible and flexible to meet the mission requirements of a constantly changing warfare environment."

For more information about SPAWAR and the PEO C4I, go to www.spawar.navy.mil.

Steve Davis is a media officer/security and policy review manager in the office of public affairs and corporate communications for SPAWAR.

Mike O'Gara is the joint test and evaluation team lead for tactical C2 systems at SPAWAR Systems Center San Diego and was test manager for both NGC2P and MOS.

CHIPS

Records Management Tool Aids Disposition Decisions

By the DON CIO Communications Team

A new records management disposition tool is available to assist users in their search for the applicable life cycle management policies and procedures for all types of naval records. This tool complements the Secretary of the Navy Manual M-5210.1: "Department of the Navy Records Management Program, Records Management Manual."

This easy-to-use tool allows users to search the manual's Part III, "Retention Standards for Naval Records," by either keyword or standard subject identification code (SSIC). Entering a keyword returns all the records containing that keyword, along with the SSIC and applicable chapter in the manual. For example, entering the keyword, "training records" returns all 42 records with a description containing that keyword.

The tool also enables users to easily find the applicable Federal Records Center (FRC) that will maintain custody of the records. Select the state or region in the drop-down menu, and the tool will provide the name, address and phone number of the FRC. Appendix A of the manual provides information on packing and shipping records to the FRC.

To learn more about Records Management, there are four Web-based training courses available on Navy Knowledge Online (NKO):

- Records Management in the DON: Everyone's Responsibility
- DON Records Management: Advanced Topics
- TRIM Context via the NMCI (Entry Level)
- TRIM Context via the NMCI (Advanced)

To access these courses, log on to NKO at www.nko.navy.mil. Under Learning, select Navy e-Learning, select Browse Categories, select Department of the Navy (DON) Training, and select the DON Records Management training subcategory. Once the course is completed, a course certificate can be printed through the transcript window of the NKO e-learning account.

CHIPS

LIFELines

Since 1999, the LIFELines Services Network has been the Navy Department's official quality of life Web site for providing a treasure trove of self-help and support information for our Sailors, Marines and their families. There are literally hundreds of articles on issues ranging from personal finances and basic life skills, to tips on relocation and transition assistance.

A lot of time, thinking and capital went into launching and keeping LIFELines afloat and we don't want to waste a resource of this caliber.

I strongly encourage you to pass the word about this valuable tool throughout your respective commands.

LIFELines' motto is it's "the place to go when you don't know where to start." I've seen it and it's true!

Take a few minutes and visit LIFELines today at www.lifelines.navy.mil.

– Rear Adm. Frank Thorp
Navy Chief of Information



CAN YOU HEAR ME NOW?

SOLAR FLARES AND THEIR EFFECT ON DOD EQUIPMENT

By Dr. Paul M. Kintner, Professor of Electrical and Computer Engineering, Cornell University, Ithaca, NY with introduction by James McCoy, Naval Air Systems Command, NAS Patuxent River, Md

Introduction

According to recent reports from the National Oceanic and Atmospheric Administration (NOAA), solar flare activity is increasing in frequency and is poised to present detrimental effects to critical Department of Defense communications-electronics (CE) equipment.

The purpose of this article is to briefly introduce the general technology-minded reader to the detrimental effects of solar flare activity and begin a dialogue by which the professional acquisition community can begin to plan mitigation methods that will reduce or completely negate the impending, damaging impact of solar flare activity on DoD's CE equipment.

The Department of the Navy Chief Information Officer, Office of the Chief of Naval Operations and Naval Air Systems Command's Electromagnetic Environmental Effects Division have already begun to examine this not so well-known phenomenon by opening the dialogue with prestigious universities such as Cornell University.

Cornell University has established a space weather research group dedicated to uncovering the harmful effects of solar flare activity, and they are working toward the development of successful mitigation methodologies.

Overview of Space Weather

Space weather begins at the sun. The sun exhibits an 11-year cycle of sunspots that are visible manifestations of an increased solar magnetic field. The last sunspot maximum (peak of activity) was in 2000, and the next one is expected in 2011.

The maxima are somewhat broad and last three to five years. During the sunspot maximum, the solar magnetic field is disrupted by solar flares (extremely large

explosions) emitting solar ultraviolet light, x-rays, energetic particles (million-electron-volt protons), coronal mass ejections (high temperature plasma gases which give a ring-like appearance around the sun or any other celestial body), and a "stormy" solar wind.

Certain larger flares produce solar radio bursts of broadband noise from 10 megahertz to 10 gigahertz that may directly affect Global Positioning System (GPS) receivers on the dayside of the Earth. Although larger solar flares produce solar radio bursts, a one-to-one relation between the size of a solar flare and the intensity of a solar radio burst does not exist.

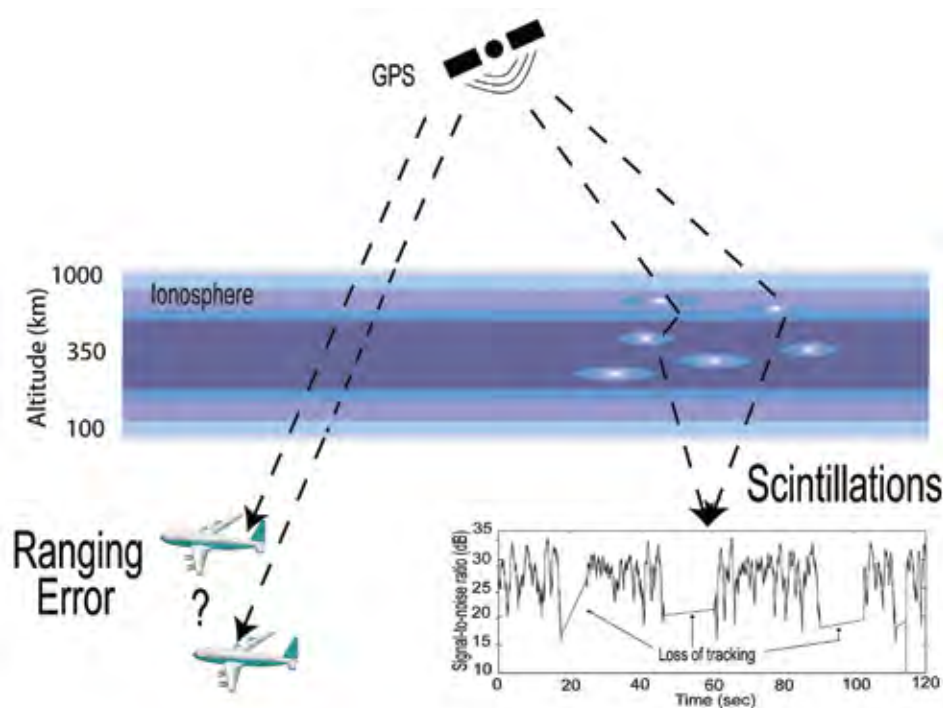
Coronal mass ejections and stormy solar winds frequently reach the Earth, if

they originate on the part of the sun facing the Earth. These ejections arrive as supersonic shock waves, frequently carrying high-energy particles.

Because the solar wind is fully ionized, it first encounters the Earth's magnetic field. The high-energy particles can directly reach the upper atmosphere over the north and south poles, endangering transpolar air flights.

Depending on how the solar magnetic field captured in the solar wind encounters the Earth's magnetic field, a magnetic storm may develop. In a magnetic storm the Van Allen radiation belts (the charged plasma particles surrounding the Earth) are rearranged, creating a doughnut that carries a ring current of 100 kiloelectron-volt plasma around the Earth.

Figure 1. Schematic of ionospheric effects on GPS signals. On the left is a ranging error produced by the slowing of GPS signals in the ionosphere. On the right are amplitude scintillations produced by destructive interference of scattered signals.



The Department of the Navy Chief Information Officer, Office of the Chief of Naval Operations and Naval Air Systems Command's Electromagnetic Environmental Effects Division are examining the effects of space weather on Defense Department communications-electronics equipment.

This current creates a magnetic field opposite to the Earth's magnetic field at the surface of the Earth. The disturbance magnetic field may amount to 1 percent or more of the Earth's field, thus it is called a magnetic storm.

The radiation belts pose a hazard to medium Earth orbit and geostationary Earth orbit spacecraft because of spacecraft charging that may cause static discharges in delicate electronics in the short run and solar cell power reduction from radiation damage in the long run.

They are also potentially fatal to astronauts if exposed directly to the radiation. During these storms the rearrangement of the Earth's magnetic field and creation of the ring current drive disturbances in the ionosphere as well.

The ionosphere is the uppermost part of the atmosphere produced by solar ultraviolet light ionizing the thermosphere at about 350-kilometer altitude. It plays an important part in atmospheric electricity and forms the inner edge of the magnetosphere. It has practical importance because, among other functions, it influences radio propagation to distant places on the Earth and to signals between satellites and the ground.

An important aspect of the solar cycle is that the average solar ultraviolet light increases substantially at solar maximum. Since solar ultraviolet light produces the ionosphere by direct ionization and heats the thermosphere, the ionosphere is denser and thicker during solar maximum.

Hence GPS signals are more strongly affected by the ionosphere during solar maximum. For example, ranging signals will have larger errors and experience large/rapid amplitude and phase fluctuations (scintillation), leading to larger navigation errors or, in extreme cases, temporary failure to navigate. See Figure 1 for an illustration of this phenomenon.

Ionospheric space weather can be roughly organized into three categories: equatorial latitudes, mid-latitudes and high latitudes. At equatorial or tropical latitudes, it frequently will affect GPS signals with the intensity modulated by the solar ultraviolet light intensity, as noted above. However, the occurrence of ionospheric weather in the tropics is usually suppressed by solar and magnetic storms.

At mid-latitudes, ionospheric weather is dominated by magnetic storms. Large storms move the aurora (brilliant display of bands or streamers of light observed in the night sky, particularly in polar regions) equatorward over the United States, and all magnetic storms have the potential to move equatorial plasma poleward and create thicker ionospheres.

At high latitudes, the northern lights, as well as high density ionospheric structures called "blobs," occur frequently but usually do not have a major impact on GPS signals.

Mitigating Space Weather Effects on GPS Receiver Operation

The first step in mitigating the effects of space weather on GPS signals is monitoring. Scintillations and rapid changes in total electron content (the number of electrons in a one meter cross-section between the receiver and the transmitter) produced by the ionosphere have unique signatures that can be used to detect their presence.

Scintillations are a combination of destructive and constructive interference produced when small scale density irregularities in the ionosphere scatter electromagnetic signals. Similar phenomena can be observed when looking through jet engine exhaust.

In transiting the ionosphere, electromagnetic signals, such as GPS signals, slow down and the excess time lag introduced is proportional to the total electron content. Without monitoring, anomalous receiver performance cannot be properly diagnosed. For example, monitoring is helpful in distinguishing ionospheric scintillations from a flock of birds roosting on or near a receiving antenna.

Second, you can predict when space weather will occur. There are a variety of aids to help in this effort. NOAA's Space Environment Center Space Weather service is useful for both nowcasting and forecasting magnetic storms and solar flare activity.

Satellites, (located upstream at the L1 Lagrangian point — where the Earth's and the sun's gravity cancel each other), monitoring the solar wind can yield predictions up to an hour in advance.

Solar imaging satellites can detect the onset of coronal mass ejections, yielding substantially earlier predictions. These observations are being combined with models to predict the effect on the Earth's magnetosphere and ionosphere.

Third, we can design better GPS receivers. Current receivers are not designed for a scintillating environment nor are their performance evaluated in the presence of scintillations. They are not able to detect or report whether a GPS signal is scintillating. The noise bandwidth of a GPS receiver's frequency or phase lock loops is not optimized for a scintillating environment.

GPS software receivers may be particularly useful in this application since their operation can be flexible. The receiver tracking loop bandwidth can be increased when the signals are robust and decreased when the signals are scintillating.

Finally, remember that GPS signal scintillations are not the only space weather effect on GPS signals. Solar radio bursts reduce the signal to noise ratio by increasing the noise ratio, which can threaten GPS receiver operation. Fast-moving ionospheric gradients can produce rapid signal phase changes that endanger the receiver's ability to track GPS signals.

Dr. Kintner is a professor of electrical and computer engineering at Cornell University in Ithaca, N.Y. Kintner received a bachelor of science degree in physics from the University of Rochester and a Ph.D. in physics from the University of Minnesota.



Benefits gained from Combined Endeavor 2008 as varied as the nations involved

By Texas Army National Guard
Master Sgt. Brenda Benner
CE 08 Public Affairs

Armenian armed forces Lt. Col. Khachatur Yeritsyan, signal department chief, conducts a compressed file transfer protocol test during Combined Endeavor 2008 in Baumholder, Germany, May 5, 2008. More than 35 participating nations use the exercise to plan, prepare and practice using a full range of communications, equipment, policies and procedures prior to deploying for NATO missions and emerging, real-world crisis situations. U.S. Air Force photo by Tech. Sgt. Corey Clements.

Regardless if military communication specialists are participating in their 14th Combined Endeavor communications interoperability exercise or their very first, their achievements, simple or complex, are crucial for the continued development of the craft of military communications for their nations and coalitions.

"When nations come to Combined Endeavor, they bring their best and brightest communicators," said U.S. Army Lt. Col. James Pugh, CE 08 exercise director. "We bring together people in a secure, low pressure environment to work out serious technical challenges. The reason we do this is no nation deploys anywhere in the world as a single entity. There's always a partner nation there."

During the past 14 years, thousands of military communicators from more than 40 nations honed their skills at CE. They used what they learned at CE to update, and in some cases, completely modernize their nations' military communications systems. Each nation can point to success stories of innovative high-tech ideas and multinational cooperation they share with one another and with communication specialists back in their homelands.

"Operations have forced us as communicators to come together and learn how to bring each nation's organic assets to the mission so we can rapidly build communication networks that provide the command and control the leadership requires," Pugh said.

Helping warfighters communicate with each other during operations is the core mission of the military communicator. Blue Force Tracking (BFT) technology, which enables commanders to see the exact location of friendly forces miles away from the ac-

tion in the command center, is at the forefront of battlefield operations. This year, the Norwegian and Finnish delegations were among those testing the interoperability of their BFT systems here.

"This is the first time we have Blue Force Tracking at Combined Endeavor," said Norwegian army Maj. Steinar Svalstad, Norway's delegation chief. "This is the system we use in Afghanistan daily. We have to make sure we can exchange data with other countries."

The Finnish team is tracking its 25 members all over Lager Aulenbach military compound using Global Positioning System-equipped push-to-talk enabled cell phones to prove the concept is working, according to Finnish Defense Forces Maj. Jarkko Karsikas, Finland's delegation chief.

Testing the interoperability of new technologies isn't the only type of testing conducted at CE.

"The systems we put in place here at the workshop are used overseas as well," said Irish Defense Forces Commandant Rossa Mulcahy, Ireland's delegation chief. "They ... provide safe and secure environments for our troops on the ground and also provide them with welfare links back home."

Mulcahy said the testing of various links such as video teleconferencing and the tactical system satellite are vital to keeping forward deployed commanders and those back in Ireland constantly updated.

The Irish delegation also benefits from the invaluable experiences provided by taking leadership roles in this multinational exercise and by working with communicators from other nations they may encounter in operations, according to Mulcahy.

"We've taken the lead on the [information technology] side with PKI encryption, so that's been a big learning curve for my guys," said Mulcahy. "They've risen to the challenge, achieved all of their goals ahead of time. We've got everyone in our regional group up and running on PKI."

Many delegations use CE training for guidance on the latest state-of-the-art equipment and procedures when building their own communication infrastructure.

Much has changed since 1999, when Moldovan communicators attended their first CE workshop with an analog switchboard. This is the 10th year Moldova par-



From left, German army Tech Sgt. Kevin Kuessner, Austrian Capt. Wolfgang Mader and French Capt. David Sajus test video teleconferencing capabilities with other nations during Combined Endeavor 2008 in Baumholder, Germany, May 5, 2008. U.S. Air Force photo by Tech. Sgt. Corey Clements.

ticipated in CE and they've moved from obsolete Soviet-era technology to testing the interoperability of a nationally developed e-mail server and PKI solution, according to its delegation chief Moldovan army Lt. Col. Andrei Sorochin.

"We have learned a lot," said Sorochin. "I'm very proud to tell you during the transformation of our national army the first thing we did was transform our communication system. All the ideas that we have — and what we've already implemented — was [were] taken from CE. Our voice-over Internet Protocol technology, our PKI security, all the software, the mail server and the client software are all based on CE experiences."

Austria has modified its communications systems deployed to Kosovo based on many improvements from past CE exercises.

"Actually, we built a new one out of the major parts of the old one," said Austrian army Lt. Col. Engelbert Ponemayr, delegation chief for Austria. "[We] had new software releases and implemented additional interfaces and gateways."

According to Ponemayr, Austria acts as the regional group leader to prepare for European Union – Battle Group 2012, providing all the signal equipment required by a brigade-level element.

"That's new for us," Ponemayr said. "We started the planning a couple of years ago. Now we're trying out [to check] if our preparations are correct. That's the reason we are a lead nation here."

As the scope and participation within CE increased from its 10-nation roster during 1995 to more than 40 nations today, each year brings first-time observers or participating nations into the CE family. Such is the case with Afghanistan, Serbia and Montenegro.

The Afghan delegation is thankful for the initial CE experience for the Afghanistan National Army Signal Group, according to Afghan army Col. Nazar Mohd Safi, his country's delegation chief.

"We will learn new technology," Safi said. "There's now a computer network in Afghanistan with thousands of users. Having a computer network and using it was just an imagination for us. Now it comes true. We use these services with help from the Americans."

Combined Endeavor Snapshot

Combined Endeavor, the annual, U.S. European Command (USEUCOM)-sponsored exercise is "in the spirit of" the Partnership for Peace (PfP) C4 integration and interoperability exercise. CE 08 is where coalition nations test and practice a full range of communications, equipment, policies and procedures prior to deploying for NATO missions and emerging real-world crises.

Now in its 14th year, Combined Endeavor ran from May 1-14. This year's event also marked the end of 10 years in which the exercise has been held at the military compound at Lager Aulenbach in Baumholder, Germany.

Over the course of CE 08:

- 1,380 communication interoperability tests were conducted by 40 nations, NATO and SEEBRIG.
- Between 160 and 180 tests were conducted and documented daily, with each day beginning at 6:45 a.m. and running often until after 7 p.m.
- A total of 442 support personnel, the bulk of which belonged to the German Joint Support Service, and 1,055 communications specialists participated.

Combined Endeavor has had participants from PfP nations, NATO nations, non-aligned nations and multinational organizations. Participation is voluntary and occasionally, nations are unable to participate in certain years due to deployments or other scheduling conflicts.

Participants in CE 08 include: Afghanistan, Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Kyrgyz Republic, Latvia, Lithuania, Macedonia, Moldova, Montenegro, NATO, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, South-Eastern Europe Brigade (SEEBRIG), Spain, Sweden, Switzerland, Tajikistan, Turkey, Turkmenistan, United Kingdom and United States.

Safi's CE goals include high frequency radio testing with the U.S., Albania, Azerbaijan and Sweden and creating a field command center on-site to establish communication with his command center in Afghanistan.

More than 40 participating nations use CE 08 to plan, prepare and practice using a full range of communications equipment, policies and procedures prior to deploying for NATO missions and emerging, real-world crisis situations such as the evacuation of Lebanon and response to natural disasters.

More than 1,200 interoperability tests within the areas of single-channel radio, voice and video services, information assurance, spectrum management and many other areas were conducted at CE 08, adding to a database of more than 13,000 tests conducted at CE since 1995.

CE 09 will be held at Kasara Barracks in Banja Luka, Bosnia and Herzegovina, where the focus will shift to distributed testing across three or more test sites.

For more information about Combined Endeavor, go to the Combined Endeavor Web site at www.combinedendeavor.net/.

Work continues on multinational common operating picture at CE 08

By U.S. Air Force Staff Sgt. Brian Hill
CE 08 Public Affairs

The idea to have a single digital display of relevant operational information shared by many nations and organizations in real time is becoming closer to reality at Combined Endeavor.

Traditionally, when coalition partners wanted to share their operating pictures with each other, doing so required installing a separate system requiring additional training and having yet another screen to monitor in the operations center.

Through the ever-increasing capabilities provided by the Multilateral Interoperability Programme, or MIP, timely and accurate information on the positions of friendly and enemy troops, and the positions and status of important infrastructure, such as bridges and roads, can be made available to commanders, said Tony Mansfield, command, control, communications and computers system engineer at the Marine Corps Tactical Systems Support Activity at Marine Corps Base Camp Pendleton, Calif.

"The aim is to achieve international interoperability of command and control information systems at all levels from corps to the lowest appropriate level, in order to support multinational, combined and joint operations and the advancement of digitization in the international arena," he said.

"Within our [U.S. Department of Defense] services, we're all sharing [a common operating picture]," Mansfield said. "Now we're sharing that with multiple nations."

The MIP is the standard for data exchange. And a standard is important because the data can then be shared in each nation's own system.

"It's a big advantage to individual nations," Mansfield said. "Because it requires no special training — they're using their own system. The MIP specifications [are] a powerful interoperability tool."

Countries at Combined Endeavor 2008 using their own system and linked together through the MIP include: Afghanistan, Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Hungary, Ireland, Lithuania, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Ukraine, United Kingdom and the United States.

According to Sgt. Michael Hendren, C4I systems analyst, having this common interface specification makes a common operating picture possible and minimizes problems that can arise when different commanders have different pictures of the state of the battlefield, including friendly fire incidents.

"With all the joint ops going on, it's very important to be able to share information," he said.

The MIP came about in 2001 by merging two separate programs: the Army Tactical Command and Control Information System (ATCCIS) and the former MIP. The former MIP was established in 1998 by the project managers of command and control systems in Canada, France, Germany, Italy, the United Kingdom and United States.



Latvian soldiers hoist a satellite onto a truck in Baumholder, Germany, April 30, 2008, so they can test connectivity with their home base during exercise Combined Endeavor 2008. DoD photo by U.S. Air Force Tech Sgt. Corey Clements.

Multilateral Interoperability Programme

The MIP specification is a managed interface between C2 information systems. When incorporated into a system, it enables interoperability of information between any other system that also incorporates the specification. Battlespace data are transferred as information. The meaning and context of the information are preserved across national boundaries precisely and without any ambiguity.

The information exchange requirements that MIP inherited from the Army Tactical Command and Control Information System encompasses the spectrum of joint and combined land operations. Thus MIP meets the requirements of the Land Component Commander of Allied Joint Combined Operations (including Article 5 and Crisis Response Operations). Systems may be wholly different from each other and need not necessarily conform to any hardware or software standard.

Typically, systems will be acquired through national or NATO acquisition programs, and their architecture will conform to the national or NATO policy prevailing at the time.

In a community of MIP-enabled C2 systems, nations, command levels and organizations can share:

- Situation awareness;
- Orders, plans and intentions; and
- Capabilities and status of friendly and enemy forces.

This is the MIP we all know today.

– www.mip-site.org

Military Coalition Frequency Management

By retired Albanian Armed Forces Lt. Col. Ulsi Meta

All military forces need uninterrupted access to the radio frequencies of the electromagnetic spectrum to meet vital communications requirements. The highly mobile nature of military operations and their logistics support require wide use of the spectrum for high-speed voice, data and image communications.

Because of the differences in technological capabilities of the participating countries, many of the communication needs in coalition operations can only be met with the use of radio systems. Military communications equipment are recognized as a force multiplier, and this is why unimpeded spectrum use is one of the conditions for successful military operations.

Despite the continuous reduction of forces, especially after the 1990s, the military need for access to radio frequencies has not decreased due to the high mobility of joint forces operating together, the need for quick responses to crises, and the increased number of missions, which all require precise, real-time information.

The variety of military operations (combat, humanitarian and peace-keeping) has increased and the need for frequencies usually increases based on the number and types of activities, not the number of forces. Military equipment is designed to work using the entire traditional, harmonized military spectrum.

Thus complete understanding of frequency management is mandatory to fulfill all the acquisition requirements for equipment that relies on the electromagnetic spectrum to operate. Further complicating matters, is that military systems work in different bands and several frequencies.

But as long as the electromagnetic spectrum is evaluated during planning as an element of the assets list and the operational electronic architecture, military forces can request the bands of the spectrum they will need to use. However, to manage frequencies, military forces face many challenges.

Technology using spectrum is in high demand. The success of certain applications, such as mobile radio-telephony, equipment using low emitting power, and digital media, increased the needs for commercial and private citizen use, as well as military needs. This often results in a tendency to decrease the military's access to frequencies by civil authorities.

Spectrum management, by its nature, is a complex, difficult activity. The terminology, legal and technical considerations, national, regional and international regulations, and bilateral and multilateral agreements might confuse anyone not well-versed in the issues surrounding spectrum use.

Operational forces often do not see the incompatibilities and interferences between their own systems and other systems. This dictates the need for trained, specialized personnel as part of the military force to advise commanders and staffs at all levels to effectively manage spectrum use. Effective, continuous training for frequency administrators is an important factor in improving frequency management.

Authorities at different levels of command and control have the responsibility to ensure access to the spectrum required for their systems. But often, they do not have the necessary knowledge for military frequency management. That is why specialized frequency management personnel are so important. They should have the responsibility for developing all the necessary administrative and technical planning for effective spectrum use.

Electromagnetic spectrum requests must be based on national priority and the national security structures. Because the civil authorities, who manage radio frequency use, often do not understand national security communications needs, they often don't follow or consider developments in the national security structures. So the military should actively engage with civil authorities to define clear objectives and priorities for its internal and international spectrum needs.

An essential aspect in frequency management is education on policies, agreements, and NATO procedures and standards. All members participating in a coalition should be familiar with the policies, agreements and standards of their partners. This is necessary to achieve interoperability between communication and information technology systems.

Military frequency management has a dynamic nature. It is related to adjustment and implementation of time concepts for the spectrum, taking into consideration allocation and spectrum usage according to currently available and future systems requirements. This involves periodic evaluation of current and future spectrum needs. The evaluation should aim for more exact definitions of spectrum resources and more effective ways to share spectrum with other nongovernmental users.

To ensure better and interference-free usage, the military, through its structures, should take responsibility for monitoring military frequency bands, cooperating and exchanging data with other authorized governmental spectrum management institutions and nongovernmental users, to identify and detect unauthorized transmissions and illegal interference.

Combined and joint operations are still a major challenge for frequency managers. The cooperation of two or more forces together, with different training needs and supporting organizations, but without appropriate frequency planning, invites failure of command and control communications. The success of combined and joint operations, in an alliance or coalition, is closely connected to the interoperability of communications and information systems.

Without careful coordination and management of spectrum bands, we can experience what communicators call "frequency fratricide." Spectrum use in these operations more than ever has shown the need for coordination between forces of different countries and within the country where they operate. Spectrum management must consider standardization and interoperability within the coalition, in accordance with deployment sites, regions and national and international regulations.

There are software tools that can assist in effective frequency management. These applications support spectrum administration and coordination, as well as both centralized and decentralized frequency management.

Military frequency management is based on policies, guides, procedures and technical manuals. The preparation, harmonization with international, regional and national regulations and adherence to technological developments make spectrum management an unrelenting task that requires time and painstaking planning.

Frequency managers must face these challenges and try to solve them to operate successfully in joint and coalition operations.

Ulsi Meta is in the J6 of the General Staff of the Albanian Armed Forces. Go to the USEU-COM Web site for more information about coalition operations at www.eucom.mil. **CHIPS**

C4I Project Management in USFK

Professional training coupled with a systematic approach delivers successful C4I capabilities on time and on budget

By Navy Lt. Cmdr. Stephen Bowman

In today's high-tech world, a project manager must use a variety of skills to develop, execute and implement a successful project. The planning process for complex command, control, computers communications and intelligence (C4I) projects can be a major undertaking when you examine the many factors that must be considered.

At Headquarters U.S. Forces Korea (USFK), Yongsan, Seoul, Korea, Air Force Col. Frederick W. Mooney, deputy assistant Chief of Staff, C6, Combined Forces Command (CFC) and assistant Chief of Staff J6, is responsible for providing C4I systems and services for all operational requirements of the joint USFK and combined CFC commands in armistice and war. This means that Mooney is responsible for providing reliable communications support for the entire Korean theater of operations.

But while communication systems are in place, there are always major technology projects in the works. Those communications projects represent the largest portion of the USFK annual budget. This year, the J6 spent more than \$31 million for C4I projects.

Project Management Tools

Every project, large and small, must be tracked and managed to the finest detail. But because the average tour length in Korea is 12 months, long-term projects often have multiple project managers over the project's life, which can sometimes cause problems with continuity and ability to deliver capabilities on schedule.

To mitigate this problem, the project management office developed a comprehensive, systematic approach to project management. Looking at many options and considering budget and training timelines, the PMO decided to use Microsoft Project. MS Project allows you to control project work, resources, schedules and finances in one integrated tool.

With many different types of projects in the J6, getting the project scope right is usually the first challenge faced by the project manager. After brainstorming sessions to identify the mission and scope of the project, the project manager can start using MS Project. The initial process involves entering all of the project tasks and estimates, dependencies, deadlines and constraints. After the tasks and limitations are entered, the resources for the project can be added to the database.

With the resources identified and tasks defined, MS Project can help the PM develop a work schedule that can be optimized for efficiency and cost effectiveness.

MS Project is also flexible; it produces progress reports tailored to the needs of the PM and senior leadership.

Professional Training

As more and more managers become trained in MS Project the command hopes to see better long-term tracking of projects. Using MS Project also allows

a smoother transition between project managers. Once the project has been mapped out in MS Project, the actual day-to-day management is really simple.

Because MS Project offers so many features that can help effectively manage a project, training is required for project managers to realize the full benefits of the software's capabilities. To this end, recently, 18 military officers and civilian personnel completed training in three certification levels: White Belt for those new to MS Project; Orange Belt for experienced project managers; and Blue Belt for multi-project and program managers.

According to Army Maj. Ivan Montanez with USFK J36, a student in the classes, the training increased his understanding of the process that the J6 uses to manage operational projects. He said the training was comprehensive, and he used the analogy of drinking from a fire hose to express the sheer volume of features covered in the MS Project training.

Army Maj. Earl Freeman, another student, is the chief of the project management branch in the J6. Freeman had a lot to say about how the use of MS Project helped him to manage successful C4I projects. Freeman said the reports that MS Project produces enhanced his ability to report project status up the chain of command.

Freeman, who is responsible for assigning managers to projects, as well as for overall monitoring for all USFK projects

Army Maj. Earl Freeman and Navy Lt. Cmdr. Stephen Bowman discussing a project management workflow diagram.



for the PMO, said that the features of MS Project have improved his ability to manage multiple projects.

In addition to the software training, Freeman, and about 20 other J6 action officers, attended project management classes for certification as a Project Management Professional.

The PMP certification is issued by the Project Management Institute (PMI), the world's leading not-for-profit association for the project management profession. To obtain a PMP certification, which is internationally recognized, much preparation and the successful completion of a four-hour exam are required.

The PMP classes cover many approaches to management fundamentals, but they are covered in a broad sense so that they can be applied to any sort of project, in any country, throughout the world.

A commitment to professionalism is shown by the J6 budget for project management training: J6 has spent \$100,000 on training this year and more than \$200,000 in the last three years.

Manageability

By breaking up a project into manageable phases, the PM can frame a general plan to tackle a project, no matter its size or complexity. A PMP divides a project into five phases: initiating, planning, executing, monitoring and controlling, and closing. Each phase is then further subdivided into processes specific to the phase.

By asking questions early in the project planning, solutions to potential problems can be addressed and corrected at a much lower cost than if they were to be addressed later in the project. This systematic approach to problem solving greatly enhanced the efficiency by which the J6 can bring a project to completion.

Many of the management subjects taught in the PMP program are not new to military students. Over the years, military training has embraced many topics related to leadership and quality management.

At Yongsan, many civil service C4I professionals can also be found proudly wearing their PMP certification pins. The current leader of the Regional Chief of Information Office (RCIO), Mr. Trinidad Capelo, is a qualified PMP, and he uses a PMP approach in the development of RCIO projects as well. Capelo is also the

local PMP preparatory class instructor.

Army Lt. Col. Shelly Matautia, chief of plans and resource management, said the focus in the J6 has been on process improvement. For the last three years, she has been managing a decreasing budget while the number of projects have increased. But by using project management fundamentals, she has been able to direct funds into critical projects based on well-defined requirements.

J6 projects and requirements are validated by the J3, which provides operational direction for all Republic of Korea (ROK) and U.S. forces assigned to and under the operational control of USFK.

By opening the project management training to J3 action officers, we have gained even more efficiencies as the project management strategy is adopted. Matautia believes we have made a great start in the future of project management and that we will need to be proactive in seeking even better processes to manage our decreasing military budget.

While we will continue to train new personnel on the software, the volume of trained experts on the staff enables new personnel to learn from their coworkers as well. By creating templates of specific types of projects, new projects can be initiated in less time and by using templates, processes become repeatable and more efficient.

A good example of a successfully completed project involves the power and air conditioning upgrades for the Northern Node Control Center (N2C2), the J64 N2C2 Integration Lab and Command Post Tango, CP TANGO. The N2C2 is the network control facility which provides primary connectivity to the Combined Enterprise Regional Information Exchange System–Korea. CENTRIXS-K is used for information sharing and collaboration, as well as transport.

The N2C2 formerly had only 15 minutes of electrical back-up power when commercial power was lost. The N2C2 integration lab did not have sufficient power for the current let alone future equipment that needed to be tested, and CP TANGO required additional equipment to upgrade the network. Without power enhancements, the facility was unable to support future technology upgrades.

The project was complex involving the use of several contractors and subcontractors, as well as the U.S. Army Korea

Command's department of public works.

Operational schedules and the work of the contractors had to be carefully synchronized. At the same time, network outages had to be minimized. Digging permits were required and had to be processed and approved. Most of the materials had to be procured in the United States, and shipment and customs clearance had to be carefully managed to coincide with the arrival of the installation team.

In early May 2007, a J6 project manager was assigned and numerous meetings were conducted with the project stakeholders. A work breakdown structure (WBS) was developed, which detailed 100 percent of the work defined by the project scope, the deliverables, in terms of the products to be completed, and the forecasted schedule for completion.

Installation began on schedule in early July 2007 and work was completed Aug. 1, 2007. While issues arose during the installation, they were quickly resolved by the PM working with the team and stakeholders. The result was a much more robust set of facilities supporting the USFK networks in Korea. A similar project is currently underway at the J6 facilities in Daegu. It is also under the management of the PMO and will be completed in January 2008.

Mooney is applying the project management approach to a theater strategic vision for all future projects in the Korean theater. He recently held a "strategic off-site" to gather inputs from senior communicator leadership in Korea. The output from the day of strategy sessions will be used to shape the future of communications project for years to come.

Mooney commended the efforts of the more than 50 officers from each of the services that attended the conference. The conference also included senior government civilians and contractors working on communications and intelligence systems. Mooney often proclaims that as "staff officers" each must embrace the work and produce results.

Clearly, the USFK J6 is producing results using great project management processes.

Lt. Cmdr. Steve Bowman is a project manager on the U.S. Forces Korea J6 staff. For information about USFK, go to www.usfk.mil/usfk/index.html. For information about the PMI, go to www.pmi.org/.

CHIPS

The Army's Central Technical Support Facility

System integration and interoperability to meet warfighter needs

By Army Maj. Shawn Murray

Today's warfighters trust when they operate their vehicles or set up tactical operations centers the command, control, communication, computer and intelligence (C4I) systems inside will interoperate. Full interoperability of military systems is critical to America's success in the war on terror and for operations into the future. Ensuring interoperability of net-centric systems is the job of the Army's Whitfill Central Technical Support Facility.

The CTSF is the Army's strategic command responsible for supporting interoperability engineering, executing Army Interoperability Certification (AIC) testing, and maintaining configuration control software for all operational through tactical level Information Technology/National Security Systems (IT/NSS).

The CTSF also supports warfighters' digital needs while they are deployed. In short, the CTSF's capability is key to ensuring the interoperability of Army and joint digital systems on battlefields now and into the future.

Located at Fort Hood, Texas, the CTSF was organized in 1996 under an organization now called the Program Executive Office Command, Control and Communications Tactical (PEO C3T). It was originally designed to provide a location for the rapid integration, testing and deployment of the Army Battle Command System (ABCS), which was designed to digitize the Army's battle command and control capability.

As digitization of the Army's warfighting capability has grown and matured, the CTSF's mission has expanded to integrate and test more than 200 net-centric systems. The number is expected to grow in the near future as more Army systems become network-enabled.

In July 2007, the CTSF organized under the Army Materiel Command's CECOM-Life Cycle Management Command.

The facility employs approximately 200 military and government civilian workers. It provides facilities for more than 400 additional government and civilian workers from several program executive offices in

a teaming environment that accomplish- es Army interoperability, integration and certification.

The CTSF campus covers more than 264,000 square feet, of which more than 40,000 square feet are dedicated to integration of software and AIC testing.

Because of its reconfigurable design, the integration and test facility can support a wide range of tactical network architectures (many simultaneously), from individual vehicles all the way to theater-level. According to Col. Steven Drake, director of the CTSF, the facility's mission "is to provide a unique, innovative and scalable environment, with skilled and dedicated personnel, using qualified synergistic processes in order to support the DoD's net-enabled strategic vision."

Drake says the mission is accomplished by "executing configuration management, systems engineering support and certification testing for Army and joint C4I providers."

As the Army continues to develop new net-centric capabilities, the CTSF stands ready to integrate and test C4I products for interoperability. The CTSF's vision is to become a customer-valued organization

ensuring the best net-centric C4I capabilities are available to U.S. Army, joint and coalition warfighters, Drake said.

AIC testing is a part of developmental testing occurring prior to a Milestone C decision. It gives the Army Staff, the Assistant Secretary of the Army for Acquisition, Logistics and Technology, and the warfighter the confidence that equipment fielded is interoperable and integrated with the other systems on the tactical network.

AIC testing at the CTSF immerses a system under test in an holistic tactical environment to ensure its ability to interoperate with other networked systems. Certification testing is done on behalf of the Army Chief Information Officer (CIO/G-6) to meet Title 40 responsibilities that mandate that no system, application or hardware will be used on the Army's tactical network until it has been tested and certified by the Department of the Army G-6.

To accomplish its mission, the CTSF has three main departments under the Technical Division to provide system integration and interoperability. These departments are Configuration Management (CM), Systems Engineering and Integration (SE&I) and Test. The departments conduct AIC testing synergistically to provide the warfighting community the best-tested tactical hardware and software possible.

The CM Department's staff not only



The CTSF is the Army's strategic command for supporting interoperability engineering, executing interoperability certification testing and maintaining configuration control for all operational and tactical level Information Technology/National Security Systems (IT/NSS). Right: CTSF test operators keep watchful eyes on monitors during software interoperability testing. Above: Test operators check cable connections as they prepare for software tests. Photos by David G. Landmann.

ensure the configuration management for the AIC test floor, but also ensure configuration control of the Army's fielded software baseline.

Each year, the CM shop produces more than 250,000 CDs and DVDs containing approved baseline software to ensure only approved software is used by Soldiers in the field.

CM also maintains a geospatial map library consisting of digital maps used by Army tactical computer systems, ABCS data products and approved baseline software, thus ensuring every map displayed in these tactical systems is the most accurate available.

The SE&I Department provides direct technical support to test and certification activities, as well as to software developers in their integration efforts. Not only do department engineers verify that new software and data products are compliant, but they also provide network engineering support to Army training events and unit deployments.

Additionally, CTSF SE&I provides support to engineering assessments of new and developing C4I products. The assessments are conducted within the CTSF's realistic tactical architectures that allow developers to test engineering releases of products in a non-attribution environment.

The SE&I Information Assurance branch works with all sections to provide an IA assessment during formal AIC baseline tests and Information Assurance Vulnerability Alert (IAVA) patch testing to update fielded software.

The CTSF Test Department is organized to provide Army and Joint AIC testing. Staffed with test officers, operators, operations research analysts and technical writers, the department provides the Army with the expertise and experience necessary to conduct the most complex interoperability software testing available within DoD today.

Interoperability requirements used for AIC testing come from the Army Training and Doctrine Command (TRADOC) capabilities managers (TCM), PEOs and formal requirements documents. From these requirements, program managers and TCMs develop mission threads which describe the flow of information through a multi-echelon architecture.

The test department uses these mission threads to create test cases which



Facility ensures quality of deployed systems Staff members from the Battle Command Network Support Directorate assisted the 1st Brigade Combat Team, 4th Infantry Division as it prepared for deployment to Iraq at the National Training Center, Fort Irwin, Calif., in August. The BCNSD is located at the Central Technical Support Facility, Fort Hood, Texas. Photo by Richard Mattox.

embrace an end-to-end approach to look at the cause and effect of information flow through a system in a networked environment.

As part of the overall test process, the CTSF has implemented a rigorous test-fix-test process executed prior to entering into a formal test. This process provides the program manager and the test officers the time to prove the software's interoperability as well as the mission threads before entering formal AIC testing.

This methodical, measured approach to testing maintains configuration control, yet allows software fixes and additional software drops to facilitate development of interoperable functional code in a shortened timeframe.

As the Army continues to conduct more of its operations in a joint environment, the CTSF will provide testing to meet the Joint Staff's mandate for Joint Technical Architecture (JTA) compliance. Many of the mission threads used today already either start or end in the joint arena.

To ensure complementary testing that is not redundant, the CTSF has a formal Memorandum of Understanding with the Joint Interoperability Test Command (JITC) to allow the sharing of data and test resources between the two organizations.

This allows Army systems to meet JTA compliance without duplicating effort. As part of this MOU, the CTSF has also recently added JITC liaisons to better integrate our communities.

The employees of the CTSF provide unparalleled, uncompromising, consistent and responsive support to the warfighter.

The investment the Army has made in the CTSF to ensure interoperability for warfighters has become a shining success and a beacon for the DoD in its attempt to develop interoperability across all services and warfighting domains.

While much work has yet to be done to achieve the DoD vision, the Army's CTSF stands ready to be an integral part of the plan to accomplish this goal. With its vast experience and dedicated workforce, the CTSF is meeting AIC integration challenges and has the resources to ensure Army interoperability in a joint environment.

As the Army's only facility to test theater-level system of systems products in a net-centric environment, the employees of the CTSF provide unparalleled, uncompromising, consistent and responsive support to the warfighter.

Maj. Shawn Murray is the deputy technical director of the Central Technical Support Facility, Fort Hood, Texas. Murray holds a bachelor of specialized studies in educational military history from Ohio University. His military education includes the Infantry Officer Basic Course, Armor Officer Advance Course and Army Acquisition Basic Course. He is Level III certified in test and evaluation and is member of the Army Acquisition Corps.

CHIPS

Commander Second Fleet Implements ITIL

Customer focus and continuous process improvement lead to effective management of Navy networks

By Second Fleet Public Affairs

After nearly eight months, Communications and Information Systems (CIS) personnel at Commander, Second Fleet are nearing the end of their implementation of a brand-new process to govern the Navy's information networks.

The idea for using the Information Technology Infrastructure Library (ITIL) came about after a joint task force exercise showed that there was a critical need for such a program.

The ITIL framework of "best practice" guidance focuses on key areas of successful organizational effectiveness: customer satisfaction, service delivery and support, application management and security management.

ITIL provides a methodology for integrating and aligning IT and organizational/business goals and implementing continuous process improvement.

"When we first realized this problem we immediately sent two personnel to a [ITIL] Foundations course sponsored by Naval Computer and Telecommunications Area Master Station Atlantic which showed immediate benefits in the alignment of processes.

"The ITIL framework works such that it will show benefit and can be established at the individual command level, which will tie into other instances easily for operations," said Information Systems Technician (IT) Senior Chief Carl Schlitt.

Under the leadership of Capt. Diane Webber, 2nd Fleet's Director for CIS, one major section of the project was to build a process-oriented framework for better management of 2nd Fleet's information networks.

After the framework and ITIL courses were completed, the 2nd Fleet ITIL implementation began in September 2007, with a one-year Plan of Action and Milestones and goal of finishing in August 2008.

With the combined efforts of Windward IT Solutions contractors Russ Herrell and Chuck Mitchell, and 2nd Fleet staff members completing ITIL training for Practitioner-level, the second-level for ITIL certification, the program was on its way to full implementation.

"The program started with a full-court press of key personnel receiving Foundations training and development of roles and responsibilities," Schlitt said.

"The Foundations training made it readily apparent that there was a viable solution to the current issues being dealt with in the Navy's IT infrastructure, and more specifically, here at COMSEC-ONDFLT," he continued.

ITIL is being implemented at 2nd Fleet in phases. Each phase, Incident Management, Problem Management, Configuration Management, Change Management and Service Level Manage-

Top: June 9, 2008 - Mr. Robert G. Castner, project coordinator of Maritime Headquarters with Maritime Operations Center (MHQ w/ MOC), and Information Systems Technician 2nd Class Jonathan Calhoun try troubleshooting a problem with help from Information Systems Technician 2nd Class Peter Newcomb at Commander Second Fleet Combat Information Systems Service Desk. Bottom: Mr. Mike Coleman, a satellite communication planner asks for assistance from IT2 Jonathan Calhoun at Commander Second Fleet Combat Information Systems Service Desk. U.S. Navy photos by Mass Communication Specialist 1st Class Moises M. Medel.



ment, implements a specific process. These processes are integrated to ensure successful IT governance.

The first phase, which implemented the Incident Management process, required a large cultural shift within the IT community itself. Many IT organizations operate in a reactionary survival mode most of the time. COMSEC-ONDFLT looks to focus on proactive service delivery which tends to stay ahead of problems. In today's dynamic network environment, not all challenges can be anticipated. But ITIL provides the processes to minimize the downtime associated with those challenges.

A larger cultural shift will take a longer period of time throughout the entire staff, but will be made easier by the evident benefits of being able to rapidly accept, understand and accomplish the mission with high change rates.

"We saw immediate and rapid benefits such as faster and more complete incident management," Schlitt said. "This allowed for users to be restored to service much more rapidly."

Another benefit was the ability to more accurately track IT man-hours and plan for balancing workloads more effectively.

"The service desk function makes it much easier to track my resources," said Information Systems Technician First Class Anaya Carter, who is the ITIL incident manager, "both people and computer systems alike."

The program also contains high quality tracking for the assets and the relationships of the infrastructure which helps in scheduling preventive maintenance, and reducing overall downtime.

Information Systems Technician Second Class Jonathan Cal-

houn, who is part of the change and release build team, sees the ITIL program as “a good way to rapidly implement changes without endangering the live environment.”

“The hardest part of the implementation is the concept of ownership,” Schlitt said. “Our COMSECONDFLT program is built so that we leverage the enlisted ranks to act as the managers of the various processes. This required quite a bit of training and significant coaching to gain individual project ownership.”

The CIS team is currently implementing the Continual Service Improvement process. The baseline process is in place and active, and is now being validated and updated as the staff learns and adapts to its changing mission criteria.

Information Systems Technician Third Class Ross Ebbinghaus sees value in the fact that “I have policies backing me up which makes good sense, and the incident process allows me to know what I’m doing and when.”

“ITIL is at the core of how we run the networks and other IT assets here at COMSECONDFLT,” Schlitt said. “Several Navy organizations are implementing ITIL, and the NGEN CONOPS [Next Generation Network concept of operations which will replace the Navy Marine Corps Intranet] just signed uses an ITIL framework as well. We hope many other Navy organizations will join us in implementing their own ITIL framework.”

Key to sustainment of a successful implementation effort is the commitment from management and ownership by the IT team.

One of the most important processes put in place is continuous improvement and the COMSECONDFLT CIS team is already thinking about how to keep their new process-driven approach current over the long haul.

“It is more important to build a good process and train your people to use it, than to try and buy and use tools to manage your networks,” Schlitt continued.

“ITIL focuses on people and processes, then seeks to take those best practices and automate those it can for a better, more efficient IT Infrastructure.”

For more information, contact COMSECONDFLT public affairs at (757) 443-9850 (ext. 47127). CHIPS

Create a Digital Dashboard to Share Management Information

Decision aid tools can help bring faltering projects back on the road to success

By Mary Hoffken and Steven Krumm

A digital dashboard is a software tool that presents summarized management information in easy-to-understand visual displays based on key performance indicators. Simple automotive-type “gauges” and “stoplight” colors are often used to distill complex data into meaningful and actionable information. Typically, users can “drill-down” to detailed information by clicking on the gauges to access graphs and tables.

A digital dashboard is used at Surface Combat Systems Center (SCSC), Wallops Island, Va., by senior leadership, managers, staff and key customers. Sharing the same (nonsensitive) information across the command ensures reliability and consistency in making decisions, preparing briefings and responding rapidly to data calls.

This article focuses on the practical approach used by SCSC for creating a digital dashboard which may be helpful to your organization in designing this management decision aid.

First, you need to determine what information senior leaders, managers and staff require. Don’t underestimate the importance of this question or your dashboard project may start off in the wrong direction. At this stage, it is best to forget about automation and shiny bells and whistles, and instead, focus on the information that is important to the success of your organization.

For example, SCSC performs vital work focused on: Program Executive Office Integrated Warfare Systems program development, life cycle engineering, fleet operator and combat information center team training, and in-service engineering. So statistical data displaying projects regarding this work are provided in the SCSC digital dashboard.

At SCSC, we started with the reports that management already received. Monthly customer support metrics, combat system readiness metrics, system usage and forecasts hours, facility electrical usage, and department financial information were initially placed on the dashboard.

For example, the dashboard has an electrical usage Web page, which shows the command’s five-year progress toward meeting Navy energy reduction goals.

Next, determine how to distill data into summary information. Decide how your data can be aggregated and calculations performed which will result in meaningful and actionable metrics.

These metrics should not just quantify organizational outputs, but should characterize how efficiently and effectively your organization is operating to provide products or services to your customers. If your organization does not have results-oriented metrics, you need to work on how to realistically and accurately measure organizational performance before

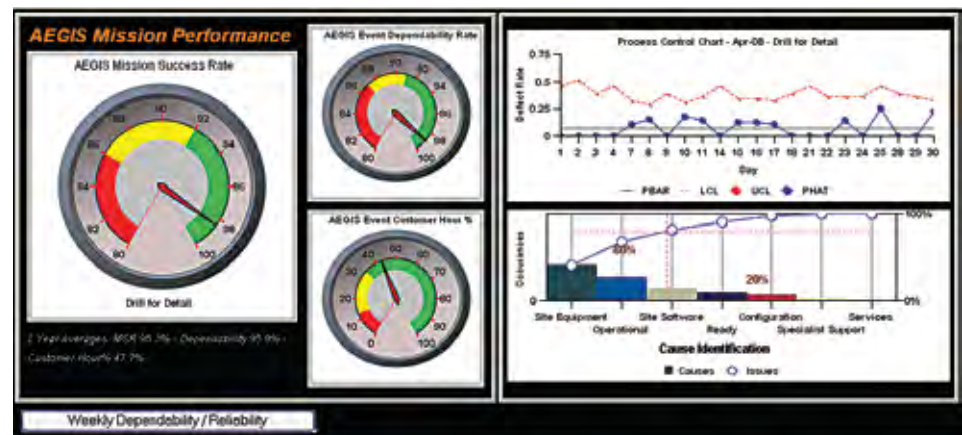


Figure 1.

you can decide how you will display this information on a dashboard.

A successful long-term dashboard project is dependent on the quality and availability of data. The most important metrics are useless if the data used to calculate them are inaccurate or outdated.

Once you have determined the information that is important and a way to measure performance, the next step is to select a software package. SCSC conducted a market survey to find a Web-based software package that automates data collection and distribution.

A weighted multi-criteria decision matrix was used to evaluate criteria important to SCSC to investigate a dozen dashboard software packages.

The criteria used were: must be Navy Marine Corps Intranet (NMCI) approved, cost-effective, can support a variety of data sources, drill-down capability, graphics capability, ease of design and flexibility, robust reports generation and a multiple dashboards capability.

The vendors of the top candidates were invited for an on-site demonstration. SCSC finally selected Visual Mining's NetCharts Reporting Suite approved for use on the NMCI by the Department of the Navy Application and Database Management System (DADMS) identification numbers 43337, 43338 and 43339. Cognos PowerPlay (DADMS No. 24955) also scored high but was considered more suitable for larger organizations.

Once you have established metrics and selected the dashboard software, it is finally time to design the dashboard. The software SCSC selected included a designer tool for rapid project development.

This tool acts like a wizard, leading the user through sequential steps, thus reducing code writing and directing the design process so the dashboard Web pages can be produced quickly.

Each dashboard starts with a project folder. Next, the data set is created, the information source for graphs and tables. Establishing a connection to a database or other source for a data set is made using an Open Database Connectivity (ODBC), Java Database Connectivity (JDBC), XML or even comma separated values (CSV) file connection.

Structured Query Language (SQL) is used to select the fields and criteria. Microsoft Excel is a good data source for small data sets, but relational databases,

like Microsoft Access or Oracle, are better if you have a large volume of data.

Another important feature of the data set is the ability to use variable substitution in the SQL statement. This allows the user to enter display criteria and interact with the dashboard and not just view static information.

Once you have a data set, you can create graphs or tables to display the information on the dashboard. Selection of the type of graph or chart is important because this is the way you communicate complex information so that it can be understood quickly.

For example, Figure 1 shows a typical dashboard gauge used to display monthly SCSC combat system facility event dependability. The stoplight color segments on the dial represent management success goals. In this case, two standard deviations are used as the boundary between green and yellow, and three standard deviations are used for the yellow to red boundary.

The drill down feature to see the values on a graph, or to select an attribute to show the information from another viewpoint, is an important function. The designer needs to balance the value of the information with the level of effort to maintain the different drill levels.

We learned that when displaying financial and technical information, to provide a drill down to the actual numbers in a table and to listen closely to managers' questions so access could be tailored to the need for specific information.

The last step in your project is to create the Web pages for the dashboard. There should be consistency throughout the Web pages in the method of navigation, page layout, colors and font selections.

You can use samples from the dashboard software, or browse the Internet

for examples of dashboard formats that you like. Think about the features that are appealing on the examples you find and how you could use them to display your information.

Don't forget maintenance and training when developing your dashboard project plan. Ideally, your dashboard will have a live data source connection, but if it uses static information, you need to plan who will be responsible for updating the data and how often.

Some training may be necessary to familiarize users in the mechanics of how to access, navigate and enter display criteria in the dashboard. More importantly, managers and staff need to understand how they can use the metrics on the dashboard.

The significance of this is demonstrated by SCSC's maturation in the Malcolm Baldrige Command Inspection criteria. In 2002, the focus was on *what are your metrics*, but by 2006 the emphasis became *how do you use metrics*?

A dashboard is an excellent way to share key performance indicators with managers and other stakeholders. A successful dashboard project should focus on the information needed, what metrics will provide that information and leadership buy-in.

Only then should the development team think about software selection and dashboard design. The development team also needs to consider dashboard maintenance and training.

Steve Krumm is the Surface Combat Systems Center Combat Systems Technology division head.

Ms. Mary Hoffken is a senior systems analyst with Lockheed Martin Information Systems and Global Services and the developer of the SCSC dashboard project.

CHIPS

NAVYForMoms.com

In March, Navy Recruiting Command launched NAVYForMoms.com in response to research that found New England-area parents have questions about what life in the Navy is like, and are searching for no-nonsense, first-hand answers.

NAVYForMoms.com puts potential Navy parents in touch with parents of young men and women who already are serving. This online community gives prospective Navy moms a place to gather accurate information, share stories and gain support from their peers.

The site continues to grow quickly, averaging more than 20 new members each day. Members have formed more than 180 groups, from Boot Camp Moms to "A" School Moms to Moms of Navy Daughters. In less than three months, members have uploaded more than 6,000 thousand photos and added hundreds of new discussion topics to the site. The recently-launched Web site NAVYForMoms.com celebrated the arrival of its 2,000th member May 21. For more information, visit www.NAVYForMoms.com.

CHIPS

SPAWAR Employees 2008 Winners

of the

Dr. Delores M. Etter Top Scientists and Engineers Award

SSC Charleston's 2008 Top Navy Engineer

By Susan Piedfort

Space and Naval Warfare Systems Center (SSC) Charleston's Ken A. Crawley was selected a Top Navy Engineer by the acting Assistant Secretary of the Navy for Research, Development and Acquisition, John Thackrah.

Crawley was one of seven SPAWAR employees honored in the competition, which included nearly 60 submissions.

The award recognizes Crawley's work with advanced antenna and radio frequency (RF) systems, particularly his contribution to the Expanded Maritime Interdiction Operations (EMIO) communications system. The system provides high speed data and voice to crews boarding vessels of interest while underway.

Crawley improved the antenna and radio system to greatly reduce service interruption and provide reliable communications between staff on the host vessel and the boarding party. The award citation noted that the electronics engineer's efforts "have made the task of interdiction much more effective and safer for our warfighters."

SSC Charleston supports the EMIO program by providing ship-to-ship line-of-sight (LoS) communications to boarding parties. The system design utilizes commercial-type wireless network systems to provide easy implementation and interoperability with common commercial network and computer systems.

Designing a dependable wireless link to operate between moving vessels on open seas offers challenges beyond those of a normal terrestrial link. A terrestrial LoS microwave link does not move, although path loss can vary over time due to ducting effects.

Engineering a successful data communications link over land is straightforward, even when including static water segments between the two terrestrial endpoints.

A maritime LoS microwave link is en-



Ken A. Crawley in Fallujah, Iraq.

tirely different. All of the difficulties and losses inherent in a terrestrial link are present, plus the relative positions of the two end points of the link vary and the variability of the transmission medium between them also varies.

Maritime LoS microwave links are also different with respect to terrestrial microwave equipment design and the data processing software algorithms for negotiating the best modulation waveforms. These are optimized for the highest data rates under static conditions.

Commercial off-the-shelf (COTS) solutions are not optimized for continuous renegotiation of the variables presented in a maritime environment. As a result, the path must be engineered with the greatest signal margins possible to keep the maritime effects at a minimum.

Also, COTS antennas are designed with the assumption that they are bolted in place and will not move in relative position. Maritime antennas are displaced in three dimensions simultaneously and quickly.

Crawley was called upon to review the implementation design, test the RF components and overall system operation, and recommend system improvements to ensure communications reliability to meet mission requirements.

After research and practical testing at SSC Charleston's Sullivan's Island lab facility and in on-water testing, Crawley proposed improvements to the system to increase effectiveness and reliability in a wide range of conditions.

Initial testing showed that variable sea conditions greatly affect the reliability of the link and additional signal gain must be designed into the system to achieve

minimum requirements for distance and data rate.

Most notably, wave induced rolls expected during interdiction operations will exceed the vertical beam angle of the original antenna system.

Antennas are optimized to provide the highest transmit/receive focus (gain) in a particular direction or elevation based on the designed use of the system. Generally, the higher the gain an antenna provides, the more directional the beam.

The radiation pattern of the antennas installed on the vessels provided effective communications when both were mounted vertically, but as the vessel rolled, the antennas tilted from vertical resulting in reduced signal amplification.

Crawley's test and evaluation process resulted in several recommendations, including adding amplifiers to both the vessel of interest (VOI) system and the host vessel to keep the system design "symmetrical."

He also recommended replacing the antenna on the VOI system to increase the vertical beam width and adding another antenna for use in higher sea states, and selecting an RF transmission line with the lowest loss practicable. Crawley also provided procedures and training to the boarding team to install the VOI antenna as near vertical as possible.

These improvements provided a system that worked acceptably in varying sea states under which actual operations occur. The continuous contact and large volume of data the boarding teams will have access to will not only increase the effectiveness of operations, but also reduce operational costs and potentially save lives.

Referring to RF engineering as an "art form," Crawley attributed his success with the EMIO system to "... education, experience, motivation and humility. Lack any one of these elements and you will fail," he said.

"RF engineering has colors that are the electromagnetic spectrum, each behaves differently. Often a textbook solution, or a product brochure solution, will fail because there are complications that lie outside of the problem statement," Crawley said.

Crawley's work in RF propagation/antenna design in SSC Charleston's communications department has taken him around the world. He also performs an-

tenna and RF system performance review and testing to identify system deficiencies and recommend performance enhancements to improve systems to meet operational requirements.

He was selected SSC Charleston Engineer of the Year in 2002 for a telemetry relay he designed, built and installed in Antarctica. During a six-month tour in Iraq in 2004, he established the SSC Charleston office in Balad, locating a site and negotiating with the Army and Air Force for its use. He and Jim Watson of SSC Charleston's Pensacola site, along with some willing Iraqis, cleared Operation Desert Storm war debris from the site.

In 2004 he, along with fellow "SPAWARriors" Don McCormick and Dean Glace (who has since retired from SSC Charleston), received a patent on a high efficiency, compact antenna assembly. Crawley has also filed a patent for a tactical AM broadcast antenna.

"This is wonderful recognition of your contributions to both [the] Department of the Navy, as well as DoD," said SPAWAR Commander Rear Adm. Michael Bachmann in a note to the SPAWAR honorees in the competition.

Crawley, and other SPAWAR award winners from SSC San Diego, James Finneran, Dr. John Meloling, Paul A. Miller, Hoa G. Nguyen, Dr. J. Scott Rodgers and Mihajlo Tomic, were honored in a Pentagon ceremony May 29.

During the presentation Crawley was lauded for providing "... warfighter[s] with a reliable tool they can count on for information and force protection during dangerous operations at sea. Your efforts have improved the product, saved money, and ensured greater success in assigned operations," his award citation noted.

The Department of the Navy has more than 35,000 scientists and engineers pursuing research, development, acquisition and sustainment.

The Dr. Delores M. Etter Top Scientists and Engineers Award was established to honor those who reached superior technical achievements and to promote continued scientific and engineering excellence.

For more information about SPAWAR, go to the SPAWAR Web site at www.spawar.navy.mil. **CHIPS**

SSC San Diego's 2008 Top Scientists, Engineers and "Emerging Innovators"

By Joanne Newton

Six Space and Naval Warfare Systems Center (SSC) San Diego employees were honored with the 2008 Dr. Delores M. Etter Top Scientists and Engineers Award by acting Assistant Secretary of the Navy for Research, Development and Acquisition, John Thackrah, in a ceremony at the Pentagon May 29.

The Navy Top Scientist and Engineer of the Year Award was established to honor superior scientific and technical achievement and promote continued scientific and engineering excellence. The title was officially changed to the "Etter Award" during the ceremony to honor previous ASN RDA, Dr. Delores Etter, who initiated the award during her tenure.

The ceremony recognized 35 Department of the Navy scientists and engineers and 11 "emerging investigators," individuals with less than 10 years of government service who show unique promise for future excellence.

In addition to Space and Naval Warfare Systems Command, other honorees represented various commands across the Department of the Navy, including the Naval Research Laboratory, Naval Sea Systems Command, Naval Air Systems Command, Naval Facilities Engineering Command and Marine Corps Systems Command.

Mr. Thackrah said, "There are extremely talented people out there in the Department of the Navy and their efforts are making a difference in the war on terrorism. I am humbled by the opportunity to honor them."

The following SSC San Diego employees were recognized for their achievements.

- James Finneran, Hearing Evaluation in Marine Animals
- Dr. John Meloling, High Frequency Antenna Technology
- Paul Alan Miller (emerging investigator), Advanced Unmanned Underwater Vehicle Control Software
- Hoa G. Nguyen, Explosive Ordnance Disposal Robots
- Dr. J. Scott Rodgers (emerging investigator), Photonic Processor
- Mihajlo Tomic (emerging investigator), Non-Acoustic Autonomous Surveillance Systems

James Finneran

James Finneran directs and manages a program that investigates the hearing abilities and effects of sound on marine mammals. His research is essential to establishing impact criteria for wild animals, developing de-confliction guidelines for the fleet's Marine Mammal Systems operating near active acoustic sources, and understanding the effects of man-made sound on marine life.

In 2007, Finneran developed techniques and equipment to quickly evaluate the hearing thresholds of marine animals by measuring auditory evoked potentials. Auditory evoked potentials are characteristic changes in an animal's electroencephalogram that are synchronized with a sound stimulus. An electroencephalogram represents electrical activity in the brain and is used to diagnose neurological disorders. Auditory evoked potentials reflect the effects of sound on the neurological activity within the auditory pathway.

Finneran's peer-reviewed papers were the first to describe the use of the multiple Auditory Steady-State Response (ASSR) technique to measure hearing thresholds in marine animals. The multiple ASSR technique is a type of evoked potential measurement that allows simultaneous testing at multiple frequencies and enables full hearing characterization in as little as five minutes.

In 2007, Finneran published the results of a landmark study using the multiple ASSR



James Finneran

technique to measure temporary threshold shift (TTS) in a bottlenose dolphin. TTS is a temporary loss of hearing after exposure to intense sound. The data is crucial to defining ways that Navy sonar may affect marine mammals, and how the animals recover from such effects.

The ASSR technique will advance the collection of hearing data from other marine mammal species not maintained in captivity. For some species, such as beaked whales, opportunistic tests on stranded animals may be the only means of obtaining information on their hearing capabilities.

Balancing the need to conduct at-sea training with the responsibility for environmental stewardship is a critical challenge facing the Navy. At present, all major exercises and at-sea testing and evaluation of mid-frequency active sonar are under legal challenge by state governmental and nongovernmental groups alleging that active sonar harms marine life.

Navy efforts to properly predict and mitigate the effects of active sonar are hampered by a profound lack of knowledge on the hearing abilities of marine mammals and the potential effects of underwater sound. For example, although there are over 128 different marine mammal species, direct information on hearing ability is available for only 28, and no information is available for baleen whales. There are questions about what marine animals hear and what sounds can cause hearing loss, physical harm and behavioral disturbances.

Finneran's development of hearing test methods establishes a scientific basis for acquiring key information to eliminate existing data gaps, helps ensure the Navy's compliance with environmental regulations, ensures fleet readiness, and provides a scientific basis for defending Navy at-sea training currently under litigation.

Dr. John Meloling

"It's a great honor to receive this award. I was very impressed by the people and projects selected. This is a tribute to all those working at the Navy commands, warfare centers and laboratories," said Dr. John Meloling, head of the Applied Electromagnetics Branch. He successfully led a multi-disciplinary team to design and demonstrate high frequency (HF) antenna technology for the Navy's new guided missile destroyer DDG-1000-class of stealth ships.

This is the first technology of its kind which was developed to meet strict antenna and radar cross-section (RCS) performance. An object's RCS performance depends on its size, reflectivity of its surface and the directivity of the radar reflection caused by the object's geometric shape. The broadband antenna performance is achieved by using a novel composite material configuration within the antenna, resulting in a mismatch loss-limited and not material loss-limited.

Procurement of the first two ship sets of antenna systems will begin in January 2010. The innovative HF antennas developed and demonstrated by Dr. Meloling will allow stealth ships to



Dr. John Meloling

communicate effectively, while maintaining a low radar signature, and resulting in greater ship survivability. The HF band is critical to interoperable communications with coalition forces and is expected to be a focus for ships of the future, including the next generation missile cruiser — CG(X).

Paul Alan Miller

Paul Miller is a lead project engineer for SSC San Diego's Unmanned Maritime Vehicles (UMV) Laboratory. During 2007, he developed innovative algorithms for the first-generation Hull Unmanned Underwater Localization System (HULS), a ship hull inspection system for detecting mines on the hull of a ship.



Paul Alan Miller

Miller was responsible for developing and testing prototype autonomous unmanned underwater vehicle (UUV) navigation and control software used to validate key vehicle behaviors related to mine countermeasures. He demonstrated advanced and innovative engineering skills in developing a prototype operating system for an autonomous UUV. The nine-month effort concluded in a successful demonstration of underwater hull search techniques at AUVFest 2007, an event sponsored by the Office of Naval Research.

Sponsored by Explosive Ordnance Disposal, the UMV Lab supports development and validation of performance parameters for autonomous UUVs used to locate mines or improvised explosive devices on a ship's hull. Miller analyzed the requirements to successfully perform hull searches and defined them in terms of autonomous underwater vehicle behaviors.

To execute those behaviors he wrote more than 75,000 lines of code (more than 95 percent of the software) while personally leading the fast-paced developmental effort. During the development cycle he researched and applied theoretical algorithms to provide innovative solutions and solve technical obstacles in the areas of vehicle simulation, navigation, ray-tracing, 3-D plane fitting, acoustic imaging, sensor integration, and interactive real-time vehicle data display using fiber-optic communications.

Miller designed and implemented a comprehensive vehicle control model that realistically simulates the vehicle's operating environment, navigation sensor performance and real-world degradation of key sensor data. His simulator significantly reduced expensive in-water test time and allowed refinement of software code based on continuing research.

Miller worked closely with several commercial vendors for underwater sensors who added improved performance and new capabilities to their existing sensors. All of the vehicle control software capabilities were successfully demonstrated in an operational environment.

Miller's work with advanced vehicle control algorithms was published in four technical papers and presented at two professional conferences in 2007. His research and development efforts support the Navy's anti-terrorism and force protection initiatives by addressing the need to detect mines placed by enemy combatants on ship hulls, piers and pilings. His advanced vehicle control architecture and supporting algorithms are the

basis for continuing research by commercial vendors who are capitalizing on his work to improve their ability to meet the Navy's hull search and mine countermeasures requirements.

Hoa G. Nguyen

Hoa Nguyen is the supervisor of SSC San Diego's Unmanned Systems Branch. He was the project manager for an effort to extend the operational range of explosive ordnance disposal (EOD) robots in theater. A Joint Urgent Operational Need Statement from U.S. Central Command was issued in 2006 in response to emergent problems occurring in theater. The radio-control range of EOD robots was being significantly reduced, limiting EOD operations.



Hoa Nguyen

During a 12-month, off-site tour at the Naval Sea Systems Command's Naval EOD Technology Division last year, Nguyen served as the technical lead for a multi-service effort to enable EOD robots in theater to compatibly operate with Counter Radio-Controlled Improvised Explosive Device (RCIED) Electronic Warfare (CREW) jammers. He planned, organized and led joint development and testing efforts by 16 organizations from government laboratories, defense agencies and industry. This accelerated research, development, test and evaluation effort led to the procurement and retrofitting of advanced radios on more than 1,000 EOD robots in theater.

Dr. J. Scott Rodgers

Dr. Scott Rodgers is a recognized expert in the field of integrated optics and nanophotonics. His research investigates how light propagates through materials, how these materials may be engineered to manipulate light, and how to use photonics to increase performance and reduce the size, weight and power needs of future Navy systems.



Dr. Scott Rodgers

Rodgers is the project manager and principal investigator for a photonic processor, with numerous applications within the Navy, which will provide a smaller, less expensive and more efficient way to do radio frequency (RF) spectrum analysis.

The photonic processor is a postage stamp-sized RF spectrum analyzer that can simultaneously analyze large portions of the RF spectrum, 2 to 20 gigahertz, with 100 percent duty cycles on all bands. The components needed to realize the photonic processor have been refined and combined in novel ways allowing a resolution of less than 100 megahertz.

Compared with technology expected to be available in 2010, this system will provide the performance equivalent to a system that would consume 1,000 watts, weigh 200 pounds and cost approximately \$2 million, at a fraction of the cost, size, weight and power.

Navy applications for this device include the use of optical beam steering and optical signal processing for navigation; optical interconnects for integrated sensors to detect biological, chemical and nuclear material; and optical logic and RF filters for combat systems applications.

Mihajlo Tomic

Mihajlo Tomic's work is instrumental in the progress of the Deployable Autonomous Distributed System (DADS) project as it moves forward in the Navy's acquisition process.



Mihajlo Tomic

Tomic is considered an expert in research and development of magnetic tracking algorithms utilizing Helium3 (He3) total-field magnetometers in non-acoustic surveillance systems. His ability to develop and leverage revolutionary technologies and practical at-sea experience contribute to the development, construction and testing of multiple next generation systems within time and budget constraints.

Tomic understands the responsibility of forming relationships with industry and academia with the goal of positioning SSC San Diego for future projects. In 2007, he submitted a proposal to the Office of Naval Research for a survivable undersea system and is a recipient of an independent applied research grant to fund the development of a wireless magnetometer network.

Tomic's contributions to He3 magnetometer technology resulted in performance characterization of linearly deployed total-field magnetometers and quantifying performance gains of ultra low noise magnetic sensing technology.

His research was the first to answer critical questions about the requirements for linear deployment of magnetic total-field sensors. His work resulted in a reduction of system complexity and overall cost, in addition to increased detection range.

Tomic took a lead role in planning, deploying, testing and recovering experimental magnetometers in a foreign joint at-sea test with scientists and engineers from the United States, Canada, Norway and the North Atlantic Treaty Organization Undersea Research Center. Tomic represented SSC San Diego during the experiment, at organizational meetings and project reviews summarizing magnetometer results from the sea trials.

Tomic developed data processing algorithms that resulted in a drastic reduction in analysis time. In addition, conclusions drawn from the experimental data sets were the foundation of a new magnetic to acoustic data fusion methodology, reducing autonomous system false alarm rates.

"I am truly proud to have this award named in my honor," Dr. Etter said. "It was nice to see all of these familiar faces again here at the Pentagon, especially those award winners ... They are doing great work."

Editor's Note: The Senate Armed Services Committee met June 26 to consider the nomination of Sean J. Stackley to be the Assistant Secretary of the Navy for Research, Development and Acquisition.

Fleet Readiness Center Southwest Lauded for Energy Saving Programs

By Jim Markle

The Secretary of the Navy joined the Department of Energy (DOE) in Washington, D.C., recently to recognize Fleet Readiness Center Southwest's (FRCSW) fiscal year (FY) 2006 energy cost-saving programs.

This was the first year FRCSW was selected for the DOE's Federal Energy and Water Management Award, and the fifth consecutive year FRCSW earned the "Gold" level of achievement within the Secretary of the Navy's energy conservation program, signifying a "very good to outstanding" program.

FRCSW is Commander, Naval Air Forces' West Coast aircraft repair depot intermediate facility specializing in the support of Navy and Marine Corps aircraft and related systems.

FRCSW was one of eight Navy facilities recognized by DOE under the energy efficiency and water management category. The awards honor superior achievement in three additional categories including renewable energy sources, energy security and reliability, and energy-efficient mobility.

More than 100 nominations from federal agencies throughout the government were submitted to the DOE Federal Energy Management Program, but only 25 facilities and individuals were recognized with the award.

"Every year I submit an annual energy and water management report for the facility to the Navy; it's a fiscal year requirement. Then, the Navy evaluates each facility for specific performance criteria. SECNAV recognizes its commands for their achievements, but further nominates facilities demonstrating energy and water efficiency achievements to the DOE," said Lucy Sapien, FRCSW energy and water conservation manager.

The command reduced its FY 2006 energy usage by 9.34 percent, a savings of more than \$500,000, Sapien noted.

Sapien said the completion of eight projects helped enhance energy efficiency and were key to the FY 2006 savings. The improvements were made possible through congressional energy funds which are allocated DOD-wide, she said. The cost of the projects was \$2,216,768 with projected annual savings of more than \$450,000 and 10,000 million British thermal units (MBTU). A MBTU is an energy measurement for steam, electricity or natural gas.

Two of the projects involved buildings 469 and 250.

"We upgraded the central plant, which basically is the building's heating, ventilating and air conditioning (HVAC) system," Sapien said.

Energy improvements to Building 469 included installation of Turbocor chillers. The chillers use a chlorofluorocarbon-free coolant and require no oil or lubrication. They feature the "Hartman Loop," a computerized program that augments the HVAC system of the building. The program reads and balances equip-

ment temperature and energy usage and adjusts them to optimize the most efficient use, Sapien said.

New chilled water and water variable pumping systems were installed to increase efficiency in HVAC cold water circulation and the building's hot water delivery system.

A Turbocor chiller retrofit was also installed in building 250, and the Siemens Technology energy management electronic control system was upgraded. The Siemens system monitors and controls a building's mechanical and electrical systems including lighting, heating and air conditioning.

Upgrades were also installed in buildings 94, 378, 466 and 472 to minimize leakage from compressed air sources. The move not only increased efficiency and reliability of equipment, but also generated approximately \$20,000 in annual savings, Sapien said.

FRCSW employs an Energy Management Team, led by Sapien, that oversees existing and future energy conservation projects and identifies project funding sources. The team includes three representatives from facilities and two from environmental. It reports to the FRCSW Executive Steering Committee at least twice annually. Membership will soon expand to include legal, comptroller and safety representation, she said.

"Now that we're going on to some bigger projects, we'll be getting into some contractual issues. And that's where the comptroller and legal [representatives] will be instrumental. And for safety and environmental, we have issues like asbestos, which may need to be addressed.

"A lot of the projects we do are facility improvement measures, such as improving a building's structure, equipment, lighting or implementing new technology. So, we coordinate our efforts with the Industrial Production Support department as well as the building owners and occupants," Sapien said.

The next phase of energy projects is expected to begin this summer and include Turbocor chiller and other HVAC upgrades to buildings 378 and 472.

Several hi-bay buildings are slated for improved lighting, and building 460 will be the first to get "Daylighting" technology, a new lighting and skylight technology, Sapien said.

The new skylight technology diffuses natural light, prevents solar heat gain and creates a calibrated, controllable and aesthetically pleasing light throughout the work area.

In the lighting industry, "high bay" (also called hi-bay) and "low bay" (lo-bay) lighting refers to a skeletal framework used in industrial construction, which forms an interior subspace called a "bay," which in turn marks the space as "high bay" or "low bay."

Approximately \$700,000 in annual utilities savings from the projects will be earmarked to pay for the improvements, Sapien said.



Hold Your Breaches!

By Steve Muck

All Department of the Navy personnel should continue to increase their level of awareness about properly safeguarding personally identifiable information (PII). To learn more about properly safeguarding PII, go to <http://privacy.navy.mil>.

The following is a synopsis of a recently reported loss or breach of PII that highlights common mishandling mistakes made by individuals within the Department of the Navy. Incidents such as this will be reported in each subsequent CHIPS magazine to increase PII awareness.

Names have been changed, but details are factual and based on reports sent to the DON Privacy Office.

On March 19, 2008, a group of private citizens discovered six boxes of paperwork at a remote, off-base location near a rifle range. Personnel files, affecting approximately 250 active duty personnel, including training records, general correspondence and W-2 tax forms were found.

The contents, which were found among what appeared to be trash, were partially burned, soiled and water damaged. The remoteness of the location and the way in which the boxes were found reduce the likelihood that PII data were used to steal identities of Department of the Navy personnel. However, because there was a loss of control over documents containing sensitive and high-risk PII data, all affected personnel were notified.

Lessons Learned:

- W-2s can and should, whenever possible, be accessed electronically rather than stored in hard copy form.
- Wherever possible, delete Social Security numbers and sensitive personal information from any list, database or e-mail before transmission or storage. SSNs are a critical element for the bad guys to use in stealing personal identities.
- Routinely review files and destroy PII by making it unrecognizable when it is no longer needed. This is especially important in areas that handle a large volume of PII like personnel offices.

Safeguard and label privacy sensitive information!

Steve Muck is the DON CIO privacy team lead.

CHIPS



If you are not watching what you throw away
someone else probably is.

Privacy information ...
if you collect it; you must protect it.



For more information visit <http://privacy.navy.mil>

CNO Visits MRAP Facility at SSC Charleston

// I am about to make your day; the Chief of Naval Operations will be at your facility at 1100. I need you to set up the facility and be ready to brief him. //

By Lt. Brian E. Phillips

April 2, 2008, brought the most unexpected, yet most exciting, encounters of my career. At approximately 0945 I received a call from the Mine Resistant Ambush Protected (MRAP) program manager. On the other end of the line the voice said, "I am about to make your day; the Chief of Naval Operations will be at your facility at 1100. I need you to set up the facility and be ready to brief him."

My initial reaction was a big gulp followed by a shot of adrenaline, realizing that I had to condense a normally intense preparation cycle into only one hour. The briefing material was developed, so I had the team put up all the storyboards and quickly sweep up the facility. Within 20 minutes, Capt. Red Hoover, then the commanding officer of Space and Naval Warfare Systems Center (SSC) Charleston, was on-site helping to prepare for the unexpected visit by ensuring all details were covered and that the facility was ready for inspection by the highest ranking officer in the U.S. Navy.

This quick visit was similar to how the MRAP program has progressed since its inception: faster than humanly possible. The MRAP program went from inception to full-rate production in a little over a year. That is about five times faster than most traditional acquisition programs of this type.

The MRAP family of vehicles provides operating forces multiple mission-role platforms capable of mitigating the effects of improvised explosive devices (IEDS), underbelly blasts and small arms fire threats, the greatest casualty producers in the global war on terrorism.

The MRAP platforms include a suite of government-furnished communications equipment to help warfighters in a variety of ways. SSC Charleston oversees the integration and installation work of the communications suite after the vehicles are accepted from the manufacturers. The MRAP team also performs interoperability testing and coordinates transportation of the vehicles from South Carolina to the Middle East. While many vehicles were transported by air initially, most are now sent by ship. SSC Charleston teams also work in theater, plugging in the radios and performing final preparations to the vehicles before they are turned over to warfighters.

CNO Adm. Gary Roughead, arrived promptly at 1100 and was quick to congratulate the team for success in meeting the nation's demand signal to ramp up production to 50 fully integrated vehicles with a full complement of command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems.



Chief of Naval Operations Adm. Gary Roughead, Lt. Brian Phillips and SSC Charleston acting Technical Director Charlie Adams.

The CNO not only learned all the details of what it takes to integrate the vehicles, but he also shook as many hands as possible and delivered as many personal "thank-yous" as he could for all the hard work done.

This visit also gave the CNO the opportunity to look over the facility and observe a joint program in action, which he was very excited to see. Many of his questions focused on how the services were able to balance requirements and ensure interoperability. Overall, he was very impressed with how, in a highly compressed timeframe, the services teamed to develop the best product at pennies on the dollar compared with original estimates.

To put the accomplishments of the MRAP program in perspective, this effort is the first of its kind, and it was able to increase production by 10 times in only four months. The MRAP vehicle development and acquisition ramped up more rapidly than the Jeep in World War II. This is especially noteworthy considering that the MRAP is a much more complex vehicle.

As the CNO departed his final comments to Capt. Hoover were about how the success factors and lessons learned in the MRAP program needed to be shared with all programs across the DoD. He was highly impressed with the workforce, leadership, facilities and with SPAWAR as an agency. The visit was a resounding success in that it showcased the high quality work we do here at SSC Charleston, and it allowed the CNO to see engineering duty officers in action and highlight their value to the Navy.

Lt. Brian E. Phillips is the MRAP vehicle Lean Six Sigma deployment champion.

Editor's Note: Capt. Bruce Urban assumed command of SSC Charleston in June. Philip H. Charles assumed duties as SSC Charleston's technical director in July. CHIPS

The Lazy Person's Guide to Botnets



By Retired Air Force
Maj. Dale J. Long

Cyberspace: the Wild West of the 21st century. The world is migrating information, commerce, governance and leisure activities into cyberspace in a shift that parallels American expansion into the Western frontier in the 19th century, only much faster and with many more people. This cyberspace migration has many of the problems that the early settlers encountered: con artists, bandits, claim jumpers — and outright warfare.

In response, the U.S. military is moving from merely operating in cyberspace to cyber-warfare operations, and we are once again exploring unfamiliar territory, particularly in terms of how we employ various technologies, procedures and behaviors. Earlier parallels include the introduction of telecommunications as a means of command and control and the development of large-scale military airlift operations.

In the first case, introducing radios and other long-distance communications devices into the C2 environment allowed us to share more information between larger numbers of people over great distances. However, radio and other communications technologies changed the operational dynamic by, among other things, allowing control of local operations by people thousands of miles away from the action.

Likewise, the Internet enables a functional increase in communications several orders of magnitude beyond what mere radios added, with equivalent levels of change in how we operate.

Military airlift was, at first, not much more than a way to get a small number of supplies to small groups out in the field — until the Berlin Airlift. Over the 18 months of the Berlin Airlift, military operations, doctrine, technology and procedures changed to keep a major city resupplied by air, revolutionizing military operations.

In cyberspace we face both challenges: employing disruptive technologies that change how we operate in the real world while exposing us to the relatively new, uncharted frontier of cyberspace. When we added airpower to the battlefield, we had to learn to think in three dimensions instead of two. In cyberspace, thinking in three dimensions is not enough. Our threats and opportunities will require thinking in at least four or even five dimensions.

Still, some things will remain constant. Whether it's controlling weapons with artificial intelligence or launching online attacks in cyberspace, it all really comes down to command and control. And where do we look to find the latest and greatest in computer-mediated warfare?

Well, I usually start in Zippy's basement.

Robotic Warfare

Last time we visited Zippy he had a small semantic misunderstanding with his robotic butler, Alfie. When I called to discuss cyber warfare, he was very excited about showing me his latest artificial intelligence project: Charlie. I was primarily interested in botnets, but first I had to see Charlie, artificial intelligence represented by a holographic computer simulation. I knew I would not get anything else out of Zippy until he demonstrated Charlie, so I descended into his basement lair to see the show.

The 3-D holographic display was state-of-the-art. It showed a small city scene with several buildings and a large wheeled machine that looked a bit like a large tank sitting in the middle of a four-way intersection. Meet Charlie," Zippy proudly said. "He's just a simulation at the moment, but we're mostly concerned with getting the AI right before he goes into production."

"What does he do?" I asked.

"Oh, he can do a lot of things. Since he's meant to be a joint resource, we're teaching him how to follow directions depending on which service is using him. Here, I'll show you."

He pushed a button on the control console, leaned over a microphone, and said, "Charlie, Army, secure building number one."

A speaker on the console replied: "Order acknowledged." The machine spun to one of the buildings, and deployed six smaller vehicles that surrounded the building and took up defensive positions.

"Guards posted. Building secure. Charlie out," the electronic voice reported.

"Now for the next one," Zippy said with a grin. "Charlie, Marine Corps, secure building two."

"Order acknowledged." The robot spun toward another building. Several panels opened on the sides and top of the machine and out popped a variety of weapons. Ten seconds later, the building had been reduced to rubble.

"Potential threat neutralized. Building secure. Charlie out."

"That's quite a different interpretation," I remarked.

"Yes," Zippy replied, "that's an issue with developing one system for different groups. You have to take into account that words can mean different things depending on who you're dealing with, like doors versus bulkheads, decks versus floors."

He turned back to the microphone and said, "Charlie, Navy, secure building number three."

"Order acknowledged." Charlie rolled over to another building. This time, a long, thin probe extended out and plugged into the side of the building. All the lights in the windows went out, and there was a succession of audible clicks.

"Lights out and doors locked. Building secure. Charlie out." Charlie rolled back to the middle of the intersection.

"May I try?" I asked.

Zippy nodded and stepped away from the microphone.

"Charlie," I said, "Air Force, secure building number four."

"Order acknowledged."

But other than what looked like a satellite dish swiveling about 30 degrees, Charlie didn't move an inch.

"It's not doing anything," I said.

"Sure it is," Zippy replied. "This was actually the hardest one to code. It's calling the landlord and negotiating a three-year lease with an option to buy."

As it turns out, Charlie's AI also includes routines that would allow it to run network defenses and counter-operations against cyber-

warfare attacks, so even if we never produce the physical version, maybe we can use something like Charlie, with a good semantic understanding and much better cyber-reflexes than humans, for C2 in our network defense systems.

But before we use any tool, we should understand what we're up against so we can give it the correct commands. And the biggest warmongers in the frontier that is cyberspace are: Botnets.

Botnet 101

We have looked at distributed computing in CHIPS in the Fall 2004 issue (www.chips.navy.mil/archives/04_fall/web_pages/grid_computing.htm) in terms of projects like SETI@home which can distribute pieces of a puzzle and have many computers working in parallel for a shared objective.

A botnet, like most distributed systems, is a collection of otherwise independent computers working "cooperatively" to accomplish a distributed task. However, the term "botnet" is reserved specifically for describing distributed computing systems designed and used for illegal and malicious purposes.

One feature that particularly distinguishes botnets from other distributed computing systems is that botnets are typically composed of machines that have been compromised and assimilated into the botnet without their owners' knowledge or consent. The compromised computers are referred to as drones or zombies. The software application inserted and hidden on a computer that executes botnet commands is called a "bot." The people who manage botnets are referred to as "herders."

Building a botnet involves assimilating drones into the collective. Bot software can be spread by a number of means, including: spam e-mails, infected files, scripts inserted by malicious Web sites, or drones actively seeking and infecting other computers with security holes.

The most successful botnet is known as Storm, which some say infected more than 1 million computers worldwide. Storm uses a worm (*malicious software hidden inside an attractive shell*) combined with social engineering techniques to lure people to Web sites that infect their PCs through a Web browser. The bot code then hides itself on the user's PC and, while waiting for commands from the botnet, spends its time *quietly* looking for other computers to infect.

For an explanation of how Storm functions, I recommend, "Storm and the future of social engineering" (www.net-security.org/malware_news.php?id=946) on the Help Net Security Web site.

More drones equal more power. Consider a botnet with 1,000 ordinary PCs in homes across the world, each with a 56-kilobit dial-up connection to the Internet. That collectively translates into more than 50 megabits of total bandwidth for the botnet, which is enough to launch a distributed denial of service (DDoS) attack on a 45-megabit (T3) connection.

Then consider what kind of bandwidth, 100,000 or 1,000,000, zombies represent and that most of the zombies in the botnet have a much faster connection than 56 kilobits if they are connected via a digital subscriber line (DSL), cable modem or T1.

That is serious bandwidth!

Botnet C2

What distinguishes a botnet from a worm is that while many worms are designed to just self-replicate, botnets have a unifying C2 (to borrow a military term) mechanism designed to organize and focus their activities.



Bot herders do not communicate directly with their drones. They communicate with botnets through what we would think of as C2 servers. If the C2 server is privately owned and operated, this offers the herder some protection. Herders can also use a network anonymous proxy — a service that masks who they are — as an additional layer of protection. Even if law enforcement officials find, seize and search a botnet C2 server, the anonymous herder is still out there, likely salvaging and rebuilding the botnet through a backup server.

One of the traditional mechanisms for controlling botnets is Internet Relay Chat. IRC has been a common Internet communications standard for a long time. It is simple to use, flexible and easy to adapt to a variety of functions. Bot applications are programmed to connect the infected PC to an IRC server and accept commands as they are posted to the chat server, so this is a real-time C2 protocol.

Bot herders can either use existing chat services and networks or set up their own control servers by installing an IRC program that runs in the background on one of the infected PCs in the botnet.

The main disadvantage of IRC for a bot herder is that traffic is generally transmitted as clear text. This makes finding and analyzing botnet messages relatively easy if you know what to look for and have the right tools. Herders have adapted by using encryption to mask their bot commands, but any encrypted traffic will stand out among all the clear text.

Botnets may also use hypertext transfer protocol for C2. With this method, the drone browses a Web page looking for instructions. However, unlike IRC, using HTTP requires the drone to periodically refresh the command page, so herders cannot send commands in real time. HTTP has an advantage over IRC in that it is not usually blocked by firewalls and monitoring the communication will not reveal any information about other drones on the network.

Lions and Tigers and Botnets, Oh My!

Botnets give their herders a lot of power on the Internet, and it is very unlikely that most bot herders built their botnets to help analyze signals from outer space or figure out protein folding within human DNA. Botnets are weapons — and they have many uses.

Let us start with the most "weaponized" use: DDoS attacks. Botnets can attack other systems on the Internet by completely saturating their bandwidth or computing resources. While a DDoS is merely a brute force assault on a system that does not steal information or add new drones to the collective, it can take down the target site and render it essentially inoperative for very long periods of time.

The problem of defending against a DDoS is that the attack comes from thousands of different places simultaneously. There is no single source that you can identify, block or retaliate against. The easiest way to stop the attack from hitting your system is to disconnect from the Internet. Ironically, this achieves the same result as the DDoS attack: denial of service.

Bot herders have extorted money from businesses with an online presence by "DDoSing" their site and then demanding payment to stop the attack.

Another common botnet function is "click fraud." This is where

drones are commanded to visit Web pages and “click” on advertising banners. Herders use this method to steal money from online advertisers that pay a small amount of money for each click on its banner ad.

Thousands of bots, each clicking a few times on various ads, can generate a lot of revenue, and since the clicks can come from thousands of drones scattered all over the world it may look like legitimate traffic to the advertisers. DDoS does not pay a bot herder’s rent, but click fraud might.

Botnets can be used to steal, store or distribute software. They can search the hard drives of their victims’ computers for software and licenses and transfer them elsewhere for duplication and distribution. Drones may also be used to store copies of pirated software. Drones can function as a distributed storage network with an aggregate storage capacity on the same scale as its aggregate bandwidth.

Bots can grant the herder complete access to a drone’s file system and allow the herder to transfer any files, read any documents, or upload more malicious applications.

More frighteningly, botnets can “keylog” on infected drones. Keylogging captures keyboard activity and reports keystrokes back to the bot herder. Bots can be programmed to log keystrokes when its drone visits banking or other Web sites involving financial transactions and steal passwords and other account information.

Finally, botnets are a major mechanism for spreading e-mail spam, which some say accounts for a majority of all e-mail traffic on the Internet. In March, *USA Today* reported two alarming statistics in “Botnet scams are exploding,” an article by Byron Acohido and Jon Swartz.

Security firm Damballa pinpointed 7.3 million unique instances of bots carrying out nefarious activities on an average day in January — an astronomical leap from a daily average of 333,000 in August 2006. That included botnet-delivered spam, which accounted for 91% of all e-mails in early March, up from 64% last June, says e-mail management firm Cloudmark.

– www.usatoday.com/money/industries/technology/2008-03-16-computer-botnets_N.htm

If Damballa’s and Cloudmark’s data are correct, botnet activity increased by nearly 22 times in five months and nine out of every 10 e-mails sent on the Internet in March 2008 were botnet-generated spam. That would suggest that botnet growth in the last year dwarfs the most aggressive organic cancers currently known to medical science.

Four-Dimensional Warfare

I mentioned earlier that cyber warfare will require thinking in more than three dimensions. This is because, unlike physical attacks that require movement of troops or weapons through space over time, botnet attacks are not bound by normal space and time limitations. They come instantaneously and from thousands of directions simultaneously.

Even if you own a botnet of similar or larger size, you can only return *fire* to a limited number of drones in real time. For example, if you have 500,000 bots of your own, know the location and address



of every zombie attacking you, and could neutralize one attacking drone with a DDoS attack by just 100 of your own drones, you can still only take down 5,000 of the machines attacking you. If the attacker has 6,000 zombies that leaves 1,000 zombies still active — and you have no remaining capacity to deal with a second attack.

Botnet war in cyberspace is likely to be asymmetric, with botnets as offensive weapons, and some other more subtle or indirect methods used for defense.

Botnets are only really dangerous when the herders own large numbers of zombies. A botnet with 50,000 zombies is a serious threat, a botnet with 500 — not so much. But the best way to neutralize botnets is to keep them from forming in the first place.

Unfortunately, botnets form because malicious software infects vast numbers of unsecured systems. While we can hope everyone else patches and upgrades their systems, we cannot depend on it. All we can do is ensure that our own systems and software are defended so we don’t contribute to the problem.

Next in our arsenal is something every submariner knows: listen carefully to every sound, no matter how small. The key to dealing with botnets is finding them, and careful listening is the key. This includes:

- Using “honeypots” – baited and trapped systems to attract and collect malicious software from bots and other attacking computers.
- Monitoring instant message spam and identifying links sent to IM users that point to malicious files.
- Browsing forums and search engines for keywords related to known malicious applications and their variants.

At some point you may collect enough information to identify a botnet’s C2 methodology and control channels. If you can identify the herders, and they live in a cooperative country, send local law enforcement after them.

Final Words

Keeping your personal computing devices secure is just as important as safeguarding the network environment in the office. While we have security experts and policies to help us at work, the stakes are just as high at home, and we must be ever vigilant.

We have really just scratched the surface of botnets here, so if you want to keep current with what is going on in the world of botnets, my recommendation is to start with the Shadowserver Foundation, a volunteer watchdog group of security professionals that gather, track and report on malware, botnet activity and electronic fraud. Their mission is, “to improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers, and the spread of malware.”

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 resources management from the Air Force Institute of Technology. He is currently serving as a telecommunications manager in the Department of Homeland Security. 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:

Asset Discovery Tools

Belarc

Belmanage Asset Management - Provides software, maintenance and services.

Contractor: *Belarc Inc.* (W91QUZ-07-A-0005)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 30 Sep 11

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0005>

BMC

Remedy Asset Management - Provides software, maintenance and services.

Contractor: *BMC Software Inc.* (W91QUZ-07-A-0006)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 29 Sep 08 (Call for extension information.)

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0006>

Carahsoft

Opware Asset Management - Provides software, maintenance and services.

Contractor: *Carahsoft Inc.* (W91QUZ-07-A-0004)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 19 Nov 09

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0004>

DLT

BDNA Asset Management - Provides asset management software, maintenance and services.

Contractor: *DLT Solutions Inc.* (W91QUZ-07-A-0002)

Authorized Users: This BPA has been designated as a GSA Smart-BUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all federal agencies.

Ordering Expires: 01 Apr 13

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0002>

Patriot

BigFix Asset Management - Provides software, maintenance and services.

Contractor: *Patriot Technologies Inc.* (W91QUZ-07-A-0003)

Authorized Users: This BPA has been designated as a GSA Smart-BUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all Federal agencies.

Ordering Expires: 08 Sep 12

Web Link: <https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0003>

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/compact-view.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/>

www.it-umbrella.navy.mil

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-hp.htm>

COTS Systems Integration Services

COTS Systems

COTS Systems Integration Services - Provides the 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) 747-5669

Computer Sciences Corp. (N00104-04-A-ZF16); (856) 988-4505

Deloitte Consulting LLP (N00104-04-A-ZF17); (703) 885-6449

IBM Corp. (N00104-04-A-ZF18); (703) 424-7581

Ordering Expires: 03 May 09

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

Database Management Tools

Microsoft Products

Microsoft Database Products - See information under Office Systems on page 73.

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 manager below.

Contractors:

Oracle Corp. (W91QUZ-07-A-0001)

DLT Solutions (W91QUZ-06-A-0002)

Mythics, Inc. (W91QUZ-06-A-0003)

Ordering Expires:

Oracle: 30 Sep 11

DLT: 1 Apr 13

Mythics: 18 Dec 11

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 sys-

tems, 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 Bill Huber, NAVICP Mechanicsburg contracting officer at (717) 605-3210 or e-mail William.Huber@navy.mil, for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWAR-SYSCEN) 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:

- as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
- under a service contract;
- under a contract or agreement administered by another agency, such as an inter-agency agreement;
- under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
- 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: 30 Sep 08 (Call for extension information.)

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 Application Integration

BEA

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) 752-0657

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

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 Aug 08 (Call for extension information.)

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 Sep 08 (Please call for information about follow-on contract.)

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: 19 Sep 11

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. ONLY Active Directory Products 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: 01 Apr 13

Web Links:

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. (N00104-07-A-ZF48); Small Business Disadvantaged; (301) 352-7878, ext. 116

Red River Computer Company (N00104-07-A-ZF47); Small Business; (603) 448-8880

Spectrum Systems, Inc. (N00104-07-A-ZF46); Small Business; (703) 591-7400

Ordering Expires:

Bay State Computer, Inc.: 14 Aug 10

Red River Computer Company: 31 Jul 10

Spectrum Systems, Inc.: 31 Jul 10

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: 31 Aug 10

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 70.

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); (609) 937-7628

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>

Information Assurance Tools

Data at Rest Solutions BPAs offered through ESI/SmartBUY

The Office of Management and Budget, Defense Department and General Services Administration awarded multiple contracts for blanket purchase agreements (BPA) to protect sensitive, unclassified data residing on government laptops, other mobile computing devices and removable storage media devices.

These competitively awarded BPAs provide three categories of software and hardware encryption products — full disk encryption (FDE), file encryption (FES) and integrated FDE/FES products. All products use cryptographic modules validated under FIPS 140-2 security requirements and have met stringent technical and interoperability requirements.

Licenses are transferable within a federal agency and include secondary use rights. All awarded BPA prices are as low as or lower than the prices each vendor has available on GSA Schedules. The federal government anticipates significant savings through these BPAs. The BPAs were awarded under both the DoD's Enterprise Software Initiative (ESI) and GSA's governmentwide SmartBUY programs, making them available to all U.S. executive agencies, independent establishments, DoD components, NATO, state and local agencies, foreign military sales (FMS) with written authorization and contractors authorized to order in accordance with the FAR Part 51.

Service component chief information officers (CIO) are currently developing component service-specific enterprise strategies. Accordingly, customers should check with their CIO for component-specific policies and strategies before procuring a DAR solution. The Department of the Navy, Army and Air Force will be releasing service-specific DAR guidance for their personnel to follow. Go to the ESI Web site at www.esi.mil for more information.

As of press time, DoD users are not authorized to purchase DAR software because service-specific guidance has not been issued. DON users are not authorized to purchase a DAR solution until the DON CIO has issued an enterprise solution for purchasing DAR software in the third quarter of FY 2008.

Mobile Armor – MTM Technologies, Inc. (FA8771-07-A-0301)

Safeboot/McAfee – Rocky Mountain Ram (FA8771-07-A-0302)

Information Security Corp – Carahsoft Technology Corp. (FA8771-07-A-0303)

Safeboot/McAfee – Spectrum Systems (FA8771-07-A-0304)

SafeNet, Inc. – SafeNet, Inc. (FA8771-07-A-0305)

Encryption Solutions, Inc. – Hi Tech Services, Inc. (FA8771-07-A-0306)

Pointsec/Checkpoint – immix Technologies (FA8771-07-A-0307)

SPYRUS, Inc. – Autonomic Resources, LLC (FA8771-07-A-0308)

WinMagic, Inc. – Govbuys, Inc. (FA8771-07-A-0310)

CREDANT Technologies – Intelligent Decisions (FA8771-07-A-0311)

GuardianEdge Technologies – Merlin International (FA8771-07-A-0312)

Ordering Expires: 14 Jun 12 (If extended by option exercise.)

Web Link: <http://www.esi.mil>

McAfee

McAfee - Provides software and services in the following areas: Anti-Virus; E-Business Server; ePolicy Orchestrator; GroupShield Services; IntruShield; Secure Messaging Gateway and Web Gateway.

Contractor: En Pointe (GS-35F-0372N)

Ordering Expires: Call for expiration information.

Web Link: <http://www.esi.mil>

Antivirus Web Links: Antivirus software available at 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: https://www.jtfgno.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.* (FA8771-06-A-0303)

Ordering Expires: 04 Jan 11 (if extended by option exercise)

Web Link: <http://www.esi.mil>

Symantec

Symantec - Symantec products can be divided into 10 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. This BPA provides the full line of Symantec Corp. products and services consisting of over 6,000 line items including Ghost and Brightmail. It also includes Symantec Antivirus products such as 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; and support.

Contractor: *immixGroup* (FA8771-05-0301)

Ordering Expires: 12 Sep 10

Web Link: <http://var.immixgroup.com/contracts/overview.cfm> or www.esi.mil

Notice to DoD customers regarding Symantec Antivirus Products:

A fully funded and centrally purchased DoD enterprise-wide antivirus and spyware software license is available for download to all Department of Defense (DoD) users who have a .mil Internet Protocol (IP) address.

Contractor: *TVAR Solutions, Inc.*

Antivirus Web Links: Antivirus software can be downloaded at no cost by linking to either of the following Web sites:

NIPRNET site: https://www.jtfgno.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 (Call for extension information.)

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 (N00104-08-A-ZF33); Small Business; (800) 248-2727, ext. 5303

CDW-G (N00104-08-A-ZF34); (703) 621-8211

GovConnection, Inc. (N00104-08-A-ZF35); (301) 340-3861

Insight Public Sector, Inc. (N00104-08-A-ZF36); (301) 261-6970

Ordering Expires: 30 Jun 10

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

iGrafX - Provides software licenses, maintenance and media for iGrafX Process 2005 and 2006 for Six Sigma; iGrafX Flowcharter 2005 and 2006; iGrafX Process for Six Sigma 2007; iGrafX Flowcharter 2007; Enterprise Central; and Enterprise Modeler.

Contractors:

Softchoice (N00104-06-A-ZF40); (416) 588-9002 ext. 2072

Softmart (N00104-06-A-ZF39); (610) 518-4292

Software House International (N00104-06-A-ZF38); (732) 564-8333

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: 30 Nov 08 (Please contact Project Management for extension Information.)

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); (877) 890-1330

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

GTSI (N00104-02-A-ZE79); Small Business; (800) 999-GTSI or (703) 502-2959

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

Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638

Softmart (N00104-02-A-ZE84); (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

Ordering Expires: 31 Mar 10

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



Minitab - NEW!

Minitab - A DoD-wide Blanket Purchase Agreement was established non-competitively with Minitab, Inc. to provide software licenses, media, training, technical services and maintenance for products including Minitab Statistical Software, Quality Companion, and Quality Trainer. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: Minitab, Inc. (N00104-08-A-ZF30); (800) 448-3555 ext. 311

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) Components, U.S. Coast Guard, NATO, Intelligence Community and authorized DoD Contractors.

Ordering Expires: 07 May 13

Web Link: <http://www.it-umbrella.navy.mil/contract/minitab/minitab.shtml>

Red Hat/Netscape/Firefox

Through negotiations with August Schell Enterprises, DISA has established a DoD-wide enterprise site license whereby DISA can provide ongoing support and maintenance for the Red Hat Security Solution server products that are at the core of the Department of Defense's Public Key Infrastructure (PKI).

The Red Hat Security Solution includes the following products: Red Hat Certificate System and dependencies; Red Hat Directory Server; Enterprise Web Server (previously Netscape Enterprise Server); and Red Hat Fortitude Server (replacing Enterprise Server).

August Schell also provides a download site that, in addition to the Red Hat products, also allows for downloading DISA approved versions of the following browser products: Firefox Browser; Netscape Browser; Netscape Communicator; and Personal Security Manager.

The Red Hat products and services provided through the download site are for exclusive use in the following Licensed Community: 1) All components of the U.S. Department of Defense and supported organizations that utilize the Joint Worldwide Intelligence Communications System, and 2) All non-DOD employees (e.g. contractors, volunteers, allies) on-site at the U.S. Department of Defense and those not on-site but using equipment furnished by the U.S. Department of Defense (GFE) in support of initiatives which are funded by the U.S. Department of Defense.

Licensed software products available through the August Schell contract are for the commercial versions of the Red Hat software, not the segmented versions of the previous Netscape products 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 Red Hat product 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 August Schell Red Hat 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 August Schell Red Hat download site (or contact the project manager listed below).

GIG or GCCS users: Common Operating Environment Home Page

<http://www.disa.mil/gccs-j/index.html>

GCSS users: Global Combat Support System

<http://www.disa.mil/main/prodsol/gccs.html>

Contractor: August Schell Enterprises (www.augustschell.com)

Download Site: <http://redhat.augustschell.com>

Ordering Expires: 14 Mar 09 (Contract options expire 15 Mar 11)

Web Link: <http://iase.disa.mil/netlic.html> - All downloads provided at no cost.

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/>

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 Standard, 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

Please go to the DON IT Umbrella Web site for more information:
www.it-umbrella.navy.mil.

Sun (SSTEWS)

SUN Support - Sun Support Total Enterprise Warranty (SSTEWS) 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 BPA

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: Effective for term of GSA contract

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: 5 Dec 10

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, AccVerify for Microsoft FrontPage and AccVerify Server. Also includes consulting and training support services.

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

Ordering Expires: 31 Aug 10

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.



The new DON IT Umbrella program manager Sandy Sirbu.

www.it-umbrella.navy.mil

www.itec-direct.navy.mil

www.esi.mil



YOU ARE INVITED TO THE West Coast DON IM/IT Conference

Department of the Navy Information Management/Information Technology Conference

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

February 9 - 12, 2009

SAN DIEGO CONVENTION CENTER, SAN DIEGO, CA

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

Computer Network Defense
Data Strategy
DON IT Workforce
DON IT Umbrella Program
Electromagnetic Spectrum
Enterprise Architecture

Enterprise Software
Information Assurance
Knowledge Management
Privacy
Service Oriented Architecture
Wireless

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

In the coming months, check the DON CIO website at www.doncio.navy.mil to register for the conference and to see tentative and final agendas.

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