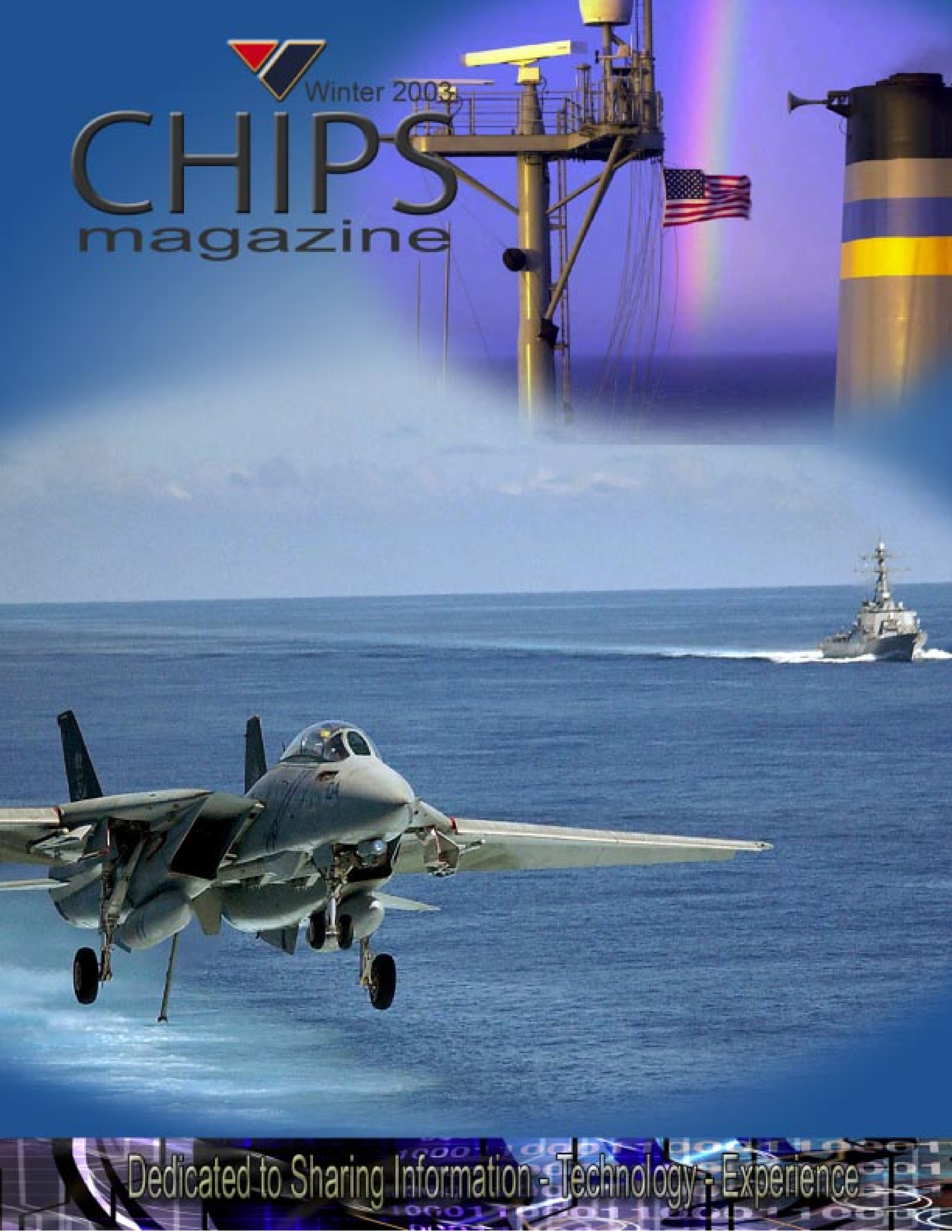
Winter 2003

CHIPS magazine



Dedicated to Sharing Information - Technology - Experience

Department of the Navy Chief Information Officer
Mr. Dave Wennergren

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

Space & Naval Warfare Systems Center, Charleston
Commanding Officer
Captain Nancy L. Deitch

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

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

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

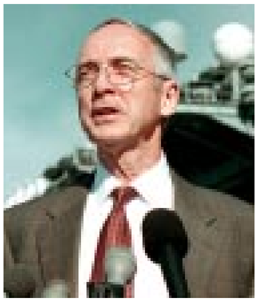
CHIPS is published quarterly by the Space & Naval Warfare Systems Center, Charleston. USPS 757-910 Periodical postage paid at Norfolk, VA and at additional mailing office. POSTMASTER: Send changes to CHIPS, SSC Charleston, Norfolk Office, 9456 Fourth Ave., Norfolk, VA 23511-2130.

Submit article ideas to CHIPS editors at chips@spawar.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@spawar.navy.mil; FAX (757) 445-2103; DSN 565. Web address: http://www.chips.navy.mil/.

Disclaimer. The views and opinions contained in CHIPS are not necessarily those of the Department of Defense nor do they constitute endorsement or approval by the DON CIO, DON IT Umbrella Program Office 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.

Features



Page 6

"...the war on terrorism is just beginning ..."
The Honorable Gordon R. England
Secretary of the Navy

Page 8

"... Our goal is to make the Navy the employer of choice for our young men and women ..."
Adm. Vern Clark
Chief of Naval Operations

Page 12

"... President Bush said that the success of the Pacific is essential to the entire world ..."
Adm. Walter F. Doran
Commander, U.S. Pacific Fleet

Page 14

"When President Theodore Roosevelt announced that the nation would 'Speak softly and carry a big stick,' the big stick he was referring to was the United States Navy ..."
Vice Adm. Albert H. Konetzni, Jr.
Deputy and Chief of Staff
U.S. Atlantic Fleet

Page 21

"I think one of the cornerstone joint applications is the Global Command and Control System."
Diann L. McCoy
DISA Principal Director for Applications Engineering

Page 25

"JITC's relationship with the Navy spans nearly three decades."

CHIPS WINTER 2003

Volume XXI Issue I

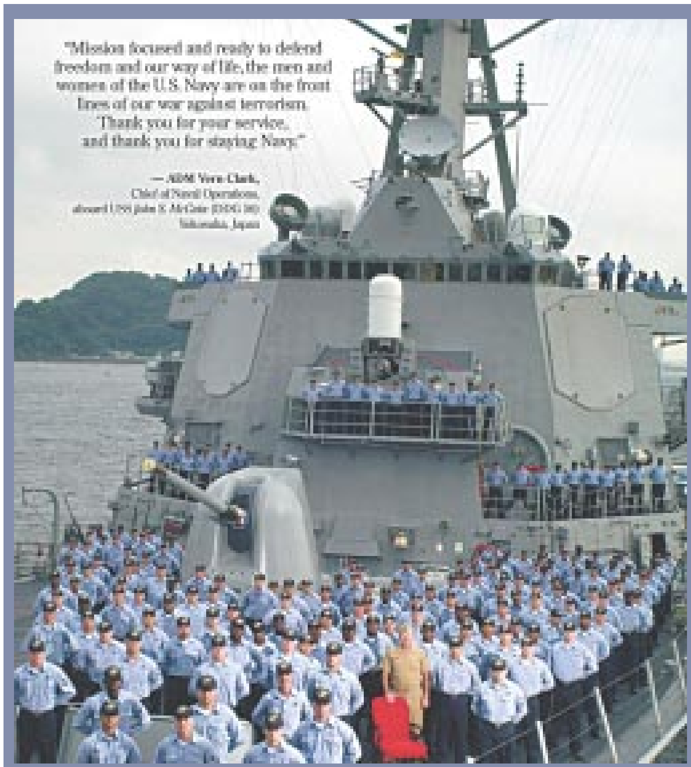
Editor's Notebook

The photo top left is one of my favorites. I can't think of a prettier site than a U.S. Navy ship with her proud crew standing topside — unless, of course, it is a Navy or Air Force F/A-18 Super Hornet with the sun glinting on her wings, or a speeding Coast Guard cutter, or a Marine standing watch, or an advancing Army battalion ... I think you get my point. In the months since 9-11, 80,000 Americans have deployed in the fight against terrorism. Through these difficult months Combatant Commanders have repeatedly praised the bravery of military members across the Services. When questioned about the "toughness" of the younger generation of warfighters top military leadership and Combatant Commanders alike express pride and awe at the dedication and self-sacrifice of today's servicemembers. They are eager to defend freedom — and embrace the latest in C2 and C4ISR innovations. In this issue we explore some of the new technologies that will arm our warfighters in the battle for freedom.

At the USNI Warfare Exposition and Symposium, Oct. 2002, I had the privilege of briefly meeting retired Navy Lt. Kevin Schaeffer who sustained serious life threatening injuries and burns on 40 percent of his body when the Navy Command Center where he worked exploded in a ball of fire after terrorists flew a hijacked airliner into the southwestern wedge of the Pentagon Sept. 11, 2001. Meeting Lt. Schaeffer was a revelation for me. He said he doesn't consider himself to be a hero, rather he says he is a survivor. Lt. Schaeffer said the real heroes today are U.S. servicemembers fighting the war on terrorism.

Our heroes risk their lives 24x7, they aren't faceless or nameless — they are our husbands, wives, brothers, sisters, children, neighbors, friends and fellow Americans. We must arm America's best and bravest with the very latest in technology and warfare capability — they deserve nothing less.

Sharon Anderson



"Mission focused and ready to defend freedom and our way of life, the men and women of the U.S. Navy are on the front lines of our war against terrorism. Thank you for your service, and thank you for staying Navy."

— ADM Vern Clark,
Chief of Naval Operations,
aboard USS John S. McCain (DDG 56)
Yokosuka, Japan

Apr. 26, 2002, at a ceremony at the Pentagon's Hall of Heroes, CNO Adm. Vern Clark presented the Purple Heart to Lt. Schaeffer for the injuries he sustained during the 9-11 attack. Director of the Army Staff Lt. Gen. Kevin Byrnes presented the Soldier's Medal to Army Sgt. 1st Class Steve Workman for rescuing Schaeffer. Photo by PH1 Roseborough.

U.S. Marines assigned to 2nd Battalion, 2nd Marines, Echo Company, 24th Marine Expeditionary Unit (MEU) Special Operations Capable (SOC) disembark from an Amphibious Assault Vehicle (AAV) to conduct a live fire training exercise. Marines from the 24th MEU (SOC) are on a regularly scheduled deployment conducting exercises in the U.S. Central Command Area of Responsibility (AOR) in support of Operation Enduring Freedom. U.S. Navy photo by PH2 Michael Sandberg.

U.S. Central Command Commander Army Gen. Tommy R. Franks speaks to Airmen, Soldiers, Sailors and Marines during a recent troop call. The general visited the base, which is supporting Operation Southern Watch, to thank the troops for their efforts in conducting the global war on terrorism and enforcing the Southern No-Fly Zone over Iraq. Photo by Senior Airman Nicole Bickford.

Department of the Navy, Chief Information Officer, Dave Wennergren

DON CIO

Embracing Change: Continuing Transformation

Change is inevitable. The work of a Chief Information Officer revolves around change, and those that lead change must be prepared to live it too. And so it is with great respect and admiration that we wish “fair winds and following seas” to Mr. Dan Porter who retired from Federal Service and stepped down as the Department of the Navy CIO on December 1. Over a four year period, Mr. Porter successfully led the most aggressive and transformational Information Management/Information Technology (IM/IT) agenda in the Federal Government. His tenure included the launching of numerous groundbreaking and innovative efforts, including the Navy Marine Corps Intranet, DON eBusiness Operations Office, the first online reverse auction in Federal Government history, DoD Common Access Card, Critical Infrastructure Protection, Knowledge Management and Legacy Applications rationalization. It’s not often that you find an individual that embodies the traits of a great leader, great teacher, great innovator, great mentor and great friend, but those of you who worked with Dan know that he has been all these things, and more, during his almost 30 years of service to the U. S. Navy and nation.

But change in the IM/IT world is as inevitable as the change in seasons, and so it with a great deal of enthusiasm and excitement that I am proud to continue championing the Department’s outstanding IM/IT work to ensure a knowledge- and network-centric Navy and Marine Corps team. Our vision remains clear — to create and maintain: (1) an integrated, results-oriented Navy and Marine Corps team characterized by strategic leadership, shared goals, ubiquitous communication, and invisible technology, (2) an effective, flexible and sustainable DON enterprise-wide information and technology environment that delivers decisive capability to the Naval Warfighting Team, and (3) a knowledge-centric culture that fosters innovation and organizational learning, enabling the rapid and effective transition of interoperable solutions in support of our expeditionary warfighting and homeland security missions.

Having served as one of the Department’s Deputy CIOs for the last four years, I’ve had the tremendous opportunity and great pleasure of working with — and continuing to work with — the most phenomenal group of information professionals: on the CIO staff, at the Navy and Marine Corps headquarters and throughout the entire Navy and Marine Corps team. I believe that the Department’s current IM/IT agenda and strategic plan is right on target: creating a seamless enterprise network; embracing knowledge management and eGovernment; rationalizing our legacy applications; moving our applications to the Web — accessed through an enterprise portal structure; establishing authoritative data sources and consolidating databases; providing career paths and growth opportunities for the IM/IT workforce; embracing new technologies, like wireless, to address the needs of our mobile workforce; providing tools to our people to help them implement these new strategies; championing Smart Cards and Public Key Infrastructure to increase security; and, aggressively focusing on Critical Infrastructure Protection as a part of our full dimensional protection strategy.

The IM/IT world will continue to evolve. As we evolve with it, we must each keep an eye to the future and continue to ensure that the Navy-Marine Corps team remains agile and ready to embrace these new ideas and new technologies. Part of this evolution is the ongoing restructuring of IM/IT management in the Department, which will strengthen and align our efforts in several ways. First, it will establish a Navy Flag Officer and Marine Corps General Officer as Deputy Chief Information Officers for the Navy and Marine Corps. Formal reporting relationships will also be established between these Deputies and the Information Officers at our major commands to align the DON’s IM/IT vision and execution. “Centers of Excellence” across the Department will become management partners, working on specific tasks on behalf of the CIO. Finally, a DON IM/IT Implementation Plan will be developed. This detailed document will link the Department’s vision and strategy to actual implementation guidance that will serve as the basis for funding and approving IM/IT initiatives.

It is a very exciting time, and the opportunities to improve the ways our Sailors, Marines and Civilians fight and work are tremendous. But it is a time of change, and we must all do our part to be change leaders. Choosing to change almost inevitably means choosing to accept some risks; but choosing not to change, in the midst of the digital revolution, almost certainly risks irrelevancy. I look forward to working with each of you as we continue our transformational efforts to ensure that we continue to have the greatest Navy and Marine Corps in the world.

“Putting Information to Work for Our People.”

... the war on terrorism is just beginning ...

The Honorable Gordon R. England
Secretary of the Navy

"Never forget that our great nation is still threatened and eternal vigilance is still essential to preserve freedom. Never forget the sacrifices of heroes past and present."

Edited from Secretary England's address to the USNI Warfare Exposition and Symposium, Virginia Beach, Va., Oct. 3, 2002.

... As our nation approaches the first anniversary ... of our first blows for freedom in the War on Terror ... and I'm not speaking of 9-11, but rather, Oct. 7 [2001] — it will be exactly a year since Capt. Dave Mercer, CAG, Carrier Air Wing Eight, launched off the deck of USS Enterprise to deliver the first strike against Taliban and al Qaeda positions in Afghanistan. Now, a year later, the terrorist camps have been destroyed, the terrorist networks disrupted, and the people of Afghanistan liberated ... but there are still many more battles to fight ...

All manners of journalism will be a part of this fight. The military and journalists are partners in freedom. The military defends our freedom. Journalists maintain our freedom ... by defending the truth ...

September 11 is indelibly etched in the collective memory of America. Even as we wrestled with the internal feelings of shock, disbelief, fear, anger and overwhelming grief ... America was already responding to the attacks. In New York and at the Pentagon ... police, firefighters, emergency service providers and ordinary citizens worked feverishly to rescue survivors and treat the wounded ... and, of course, as we all know very well, heroic actions aboard United Flight 93 foiled the terrorists' last planned attack on our nation's capital.

While it would be comforting to believe that this war is drawing to an end, it's unfortunately closer to the beginning than to the end. This is still a time of testing for America ... and for freedom and liberty.

In my lifetime, there have been three "isms" that threatened America. It took a World War to defeat the first ism, which America entered when I was four years old. That was the war to defeat fascism. We prevailed militarily and were ultimately victorious by establishing a new government in Germany and in Japan.

In 1950, a few short years after defeating fascism, the nation found itself in war again in Korea. At that time, we did not know that the Korean War was merely the first bloody battle of a long war that would last until the wall came down — almost 40 years later — in Berlin in 1989. Korea was the beginning of the Cold War when the free nations of the world stood shoulder-to-shoulder to stop communism, the second ism of my lifetime. It took a World War to defeat fascism and a Cold War to defeat communism.

Now we are embarked on the war against terrorism, the third ism, and history has not yet recorded how this war will be characterized. We do know, however, that it will be a long war. It is also a war in which the United States and its allies must prevail because the consequences are so profound. For the first time in the history of mankind, a small number of people with weapons of mass destruction can wreak untold havoc in our cities and against our citizens ... against our allies ... and against freedom loving people around the world.

Several months ago, I was at Pearl Harbor in Hawaii and visited the USS Arizona. I was also on board the USS Missouri. These ships rest side by side. The Arizona is symbolic of the beginning of World War II for America ... and the Missouri symbolic of the ending of that war. The peace treaty with Japan was signed on the deck of the Missouri. These two memorials provide a visual perspective of the beginning and end of a terrible war. Now visualize the tragedy in New York when the airliners crashed into the World Trade Centers ... the beginning of the war on terrorism. Now, try to visualize how this war will end. It certainly will not end with a peace treaty as it did on the USS Missouri at the end of World War II. Rather, it will require the military defeat of terrorism followed by a change of governments in countries that support terrorism. Ultimately that was what was required to defeat fascism and communism.

... Who could have imagined how fascism and communism would have ultimately ended by December 1942 or July 1951? The weapon that ended World War II was still embryonic in December of 1942, and certainly no one could have imagined in July 1951 that the Cold War was going to last another 38 years or that it would ultimately be won economically rather than militarily.

I can tell you one year into this war that our Naval services, our Navy and Marines, have never been better prepared than they are today. All of our readiness accounts are fully funded, our equipment is ready, our morale is high, and we are ready to prosecute the President's orders. This does not mean that these are comfortable times. Rather, as we continue our war against terrorism, we are also in the process of transforming our military ... and transforming the very way that the DoD manages its enterprise to be better prepared to protect and defend our nation as we face new future threats. This is not, however, a new role — our Naval forces have continuously changed to protect and defend our nation for the past 227 years.

One year into this war, I do know that victory in the war against terrorism will be much broader than just military. It will take our military, economic and diplomatic strength to win, and it will also take the strength of our journalists ... I also find it of great personal interest that none of the countries associated with any of the three isms ... had or have a free press. Jefferson was certainly right when he uttered his now famous dictum, "Were it left to me to decide ... whether we should have a gov-

Unveiled during a dedication ceremony held on the first anniversary of the Sept. 11, 2001, terrorist attacks, a memorial wall located near the Navy's newly-reconstructed Navy Operations Center in the Pentagon honors those DON personnel who perished when the hijacked American Airlines Flight 77 crashed into the building. The Navy lost 42 of its personnel, active duty, retired, and employees in the Pentagon and four retired officers and a Navy employee aboard Flight 77. U.S. Navy photo by PHC Philomena Gorenflo.

ernment without newspapers ... or newspapers without a government ... I should not hesitate a moment ... to prefer the latter." ... To professionally challenge assumptions and conclusions and cause a measured and factual debate is beneficial and therefore encouraged. Dissent in the name of freedom is a virtue.

I said this would likely be a long war and that means we will ask our sons and daughters, mothers and fathers, — members of our American families to shed blood and, when necessary, to make the ultimate sacrifice for freedom. That includes the press. Last year 51 journalists were killed around the globe. All of you ... play a critical role in maintaining public awareness ... and enhancing public understanding of our Navy's daily action ... and the Navy's role in protecting America.

... I am reminded of the words President Bush spoke on his first visit to the Pentagon ... hours after the attack ... at 6:20 p.m. on September 12. The fires still burned in the Pentagon roofline ... the smell of smoke permeated the building ... and the sound of emergency sirens still pierced the air. Our military was on the highest alert. The Nation's senior uniformed and civilian military leaders were in the room ... the Joint Chiefs of Staff ... my fellow Service Secretaries ... the Secretary of Defense and his Deputy.

The President looked hard at each of us in turn and said ..."NEVER FORGET ... what happened yesterday ... never forget how you felt. I will never forget. The nation will go on because the nation has to go on ... people will need to get on with their lives ... but you and I can never forget, because we are charged by the American people to protect and defend our nation." We owe it to our children and our grandchildren to create a world that is free of the scourge of terrorism ... we owe it to the memory of those who have fallen in the line of duty ... We must remember the fallen as they would have wanted to be remembered — living in freedom as Americans. And it is the challenge to all of us ... to ensure that Americans ... across time and across this great land ... never forget: Never forget that our great nation is still threatened and eternal vigilance is still essential to preserve freedom. Never forget the sacrifices of heroes past and present. Never forget what happened in New York City ... at the Pentagon ... and in the skies over Somerset County, Pennsylvania. Never forget that as comrades-in-arms, our military and the press have a solemn duty to preserve liberty and freedom.

God bless each and every one of you ... God bless our fallen heroes and their families ... and God bless the United States of America.

Editor's Note: When President Bush signed the Homeland Security Bill into law Nov. 25, he established a new cabinet-level department to ensure the safety of the American people. Before Bush signed the bill in a White House ceremony, he announced he will nominate former Pennsylvania Governor Tom Ridge to be the first Secretary of Homeland Security. He also said he will nominate Navy Secretary Gordon England to be deputy at the 170,000-worker agency.

"The trust and confidence that President Bush has shown in selecting me to join Governor Tom Ridge in this important work for our nation is deeply appreciated," said England, who has served as Secretary of the Navy since May 2001. "My only regret is that my time as Secretary has been too short; however, the naval services continue in the good hands of the Secretariat, Adm. Vern Clark, Gen. Jim Jones and all the other leaders of the Navy-Marine Corps Team. Our naval services are well positioned to carry on their long and great tradition of defending liberty and freedom around the world."

The new department will analyze threats, guard borders, coordinate national responses and focus the "full resources of the American government on the safety of its people," Bush said. The bill is a response to the Sept. 11 attacks in New York and Washington D.C. The idea is to place all federal agencies involved with homeland security under one umbrella. The few exceptions are the military, the Federal Bureau of Investigation and the Central Intelligence Agency. He said the Homeland Security Act is the "next logical step" in defending America. The act amalgamates 22 agencies into one department. "To succeed in their mission, leaders of the new department must change the culture of many diverse agencies, directing all of them toward the principal objective of protecting the American people," Bush said. "The effort will take time and focus and steady resolve." He said adjustments in the department will be needed, as this is the largest reorganization of the U.S. Government since the 1947 act that established the Defense Department. He said the new department would analyze information collected by U.S. intelligence agencies and match that against American vulnerabilities. The new agency will work with other agencies, the private sector, and state and local governments to harden America's defenses against terror, Bush stated.

The agency will focus on safeguarding the U.S. computer network, and defend against the growing threat of chemical, biological or nuclear assaults. The Department of Homeland Security will be one point of contact for state and local officials, and place security for all U.S. transportation systems under one roof. Bush noted the Department of Homeland Security will end duplication and overlapping responsibilities.

As we go to press Secretary England is expected to continue as Secretary of the Navy until January 2003.

SEA POWER 21

By Adm. Vern Clark, Chief of Naval Operations

Adm. Clark has written numerous articles and continues to speak about his vision for a fully-networked joint warfighter embodied in the vision for Sea Power 21. CHIPS' editors had the opportunity to talk with Adm. Clark and hear him speak about how Sea Power 21 will tie together the Naval, Joint and national information grid, at the USNI Warfare Exposition and Symposium, Virginia Beach, Va., Oct. 2, 2002. At a lively question and answer session, one young Sailor challenged the CNO doubting that the Navy's transformation could be done — the CNO countered, "You just watch us, but we would rather have you join us." Excerpts are taken from the CNO's article for Proceedings Magazine (October 2002 Volume 128/10/1,196), "Sea Power 21— Projecting Decisive Joint Capabilities" and the admiral's remarks at the symposium. At left: U. S. Navy photo by PH3 Yesenia Rosas.

...The 21st century sets the stage for tremendous increases in Naval precision, reach, and connectivity, ushering in a new era of joint operational effectiveness. Innovative concepts and technologies will integrate sea, land, air, space and cyberspace to a greater extent than ever before. In this unified battlespace, the sea will provide a vast maneuver area from which to project direct and decisive power around the globe. Future Naval operations will use revolutionary information superiority and dispersed, networked force capabilities to deliver unprecedented offensive power, defensive assurance, and operational independence to Joint Force Commanders. Our Navy and its partners will dominate the continuum of warfare from the maritime domain — deterring forward in peacetime, responding to crises, and fighting and winning wars. By doing so, we will continue the evolution of U.S. Naval power from the blue-water, war-at-sea focus of the "Maritime Strategy" (1986), through the littoral emphasis of ". . . From the Sea" (1992) and "Forward . . . from the Sea" (1994), to a broadened strategy in which Naval forces are fully integrated into global joint operations against regional and transnational dangers.

The events of 9-11, tragically illustrated that the promise of peace and security in the new century is fraught with profound dangers: nations poised for conflict in key regions, widely dispersed and well-funded terrorist and criminal organizations, and failed states that deliver only despair to their people. These dangers will produce frequent crises, often with little warning of timing, size, location or intensity. Associated threats will be varied and deadly, including weapons of mass destruction, conventional warfare, and widespread terrorism. Future enemies will attempt to deny us access to critical areas of the world, threaten vital friends and interests overseas, and even try to conduct further attacks against the American homeland. These threats will pose increasingly complex challenges to national security and future warfighting.

Previous strategies addressed regional challenges. Today, we must think more broadly. Enhancing security in this dynamic environment requires us to expand our strategic focus to include both evolving regional challenges and transnational threats. This combination of traditional and emerging dangers means increased risk to our nation. To counter that risk, our Navy must expand its striking power, achieve information dominance, and develop transformational ways of fulfilling our enduring missions of sea control, power projection, strategic deterrence, strategic sealift, and forward presence.

Three fundamental concepts lie at the heart of the Navy's continued operational effectiveness: Sea Strike, Sea Shield and Sea Basing, illustrated in Figure 1. Sea Strike is the ability to project precise and persistent offensive power from the sea; Sea Shield extends defensive assurance throughout the world; and Sea Basing enhances operational independence and support for the joint force. These concepts build upon the solid foundation of the Navy-Marine Corps team, leverage U.S. asymmetric advantages, and strengthen joint combat effectiveness.

We often cite asymmetric challenges when referring to enemy threats, virtually assuming such advantages belong only to our adversaries. Sea Power 21 is built on a foundation of American asymmetric strengths that are powerful and uniquely ours. Among others, these include the expanding power of computing, systems integration, a thriving industrial base, and the extraordinary capabilities of our people, whose innovative nature and desire to excel give us our greatest competitive advantage.

Sea Strike, Sea Shield and Sea Basing will be enabled by ForceNet, an overarching effort to integrate warriors, sensors, networks, command and control, platforms, and weapons into a fully netted, combat force. We have been talking about network-centric warfare for a decade, and ForceNet will be the Navy's plan to make it an operational reality. Supported by ForceNet, Sea Strike, Sea Shield and Sea Basing capabilities will be deployed by way of a Global Concept of Operations that widely distributes the firepower of the fleet, strengthens deterrence, improves crisis response, and positions us to win decisively in war.

Projecting Decisive Combat Power

Projecting decisive combat power has been critical to every commander who ever went into battle, and this will remain true in decades ahead. Sea Strike operations are how the 21st century Navy will exert direct, decisive, and sustained influence in joint campaigns. They will involve the dynamic application of persistent intelligence, surveillance, and reconnaissance; time-sensitive strike; ship-to-objective maneuver; information operations; and covert strike to deliver devastating power and accuracy in future campaigns. Information gathering and management are at the heart of this revolution in striking power. Networked, long-dwell Naval sensors will be integrated with national and joint systems to penetrate all types of cover and weather, assembling vast amounts of information. Data provided by Navy assets — manned and unmanned — will be vital to establishing a comprehensive understanding of enemy military, economic, and political vulnerabilities. Rapid planning processes will then use this knowledge to tailor joint strike packages that deliver calibrated effects at precise times and places.

... Information superiority and flexible strike options will result in time-sensitive targeting with far greater speed and accuracy. Military operations will become more complicated as advanced intelligence, surveillance, and reconnaissance products proliferate. Expanded situational awareness will put massed forces at risk, for both friends and adversaries. This will compress timelines and prompt greater use of dispersed, low-visibility forces. Countering such forces will demand speed, agility and streamlined information processing tied to precision attack. Sea Strike will meet that challenge.

The importance of information operations will grow in the years ahead as high-technology weapons and systems become more widely available. Information operations will mature into a major warfare area, to include electronic warfare, psychological operations, computer network attack, computer network defense, operations security and military deception. Information operations will play a key role in controlling crisis escalation and preparing the battlefield for subsequent attack. This U.S. asymmetric [advantage] will be a critical part of Sea Strike.

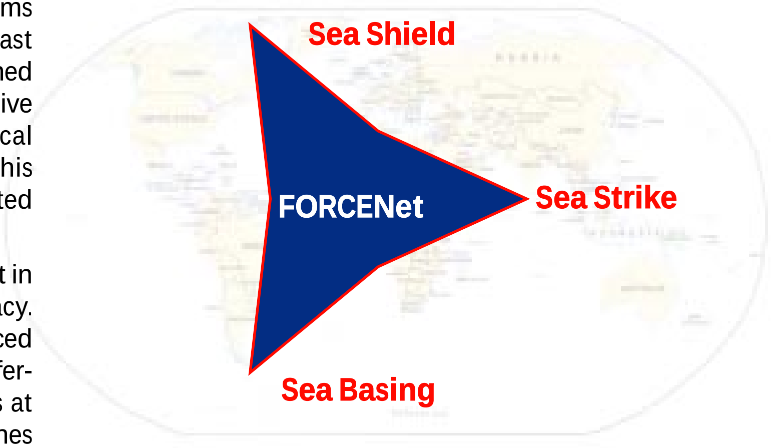
When we cannot achieve operational objectives from over the horizon, our Navy-Marine Corps team moves ashore. Using advanced vertical and horizontal envelopment techniques, fully netted ground forces will maneuver throughout the battlespace, employing speed and precision to generate combat power. Supported by sea bases, we will exploit superior situational awareness and coordinated fires to create shock, confusion and chaos in enemy ranks. Information superiority and networking will act as force multipliers, allowing agile ground units to produce the warfighting impact traditionally provided by far heavier forces, bringing expeditionary warfare to a new level of lethality and combat effectiveness.

... Sea Strike operations will be fully integrated into joint campaigns, adding the unique independence, responsiveness, and on-scene endurance of Naval forces to joint strike efforts. Combined sea-based and land-based striking power will produce devastating effects against enemy strategic, operational and tactical pressure points — resulting in rapid, decisive operations and the early termination of conflict.

Sea Shield to Protect Our National Interests

Traditionally, Naval defense has protected the unit, the fleet and the sea lines of communication. Tomorrow's Navy will do much more. Sea Shield takes us beyond unit and task-force defense to provide the nation with sea-based theater and strategic defense. Sea Shield will protect our national interests with layered global defensive power based on control of the seas, forward presence and networked intelligence. It will use these strengths to enhance homeland defense, assure access to contested littorals and project defensive power deep inland. As with Sea Strike, the foundation of these integrated operations will be information superiority, total force networking, and an agile and flexible sea-based force. Homeland defense will be accomplished by a national effort that integrates forward-deployed Naval forces with the other military services, civil authorities, and intelligence and law-enforcement agencies. Working with the newly established Northern Command, we will identify, track, and intercept dangers long before they threaten our homeland ...

Figure 1. Sea Power 21



Maritime patrol aircraft, ships, submarines and unmanned vehicles will provide comprehensive situational awareness to cue intercepting units. When sent to investigate a suspicious vessel, boarding parties will use advanced equipment to detect the presence of contraband by visual, chemical and radiological methods. Forward-deployed Naval forces will also protect the homeland by engaging inbound ballistic missiles in the boost or mid-course phase, when they are most vulnerable to interception. In addition, our nuclear-armed Trident ballistic missile submarine force will remain on silent patrol around the world, providing the ultimate measure of strategic deterrence. These highly survivable submarines are uniquely powerful assets for deterring aggressors who would contemplate using weapons of mass destruction.

... In times of rising tension, prepositioned Naval units will sustain access for friendly forces and maritime trade by employing evolving expeditionary sensor grids and advanced deployable systems to locate and track enemy threats. Speed will be an ally as linked sensors, high-speed platforms, and improved kill vehicles consolidate area control, including the location and neutralization of mines via state-of-the-art technology on dedicated mine warfare platforms and battle group combatants. Mission-reconfigurable Littoral Combat Ships, manned and unmanned aviation assets, and submarines with unmanned underwater vehicles will gain and maintain the operational advantage, while sea-based aircraft and missiles deliver air dominance. The result will be combat-ready forces that are prepared to "climb into the ring" to achieve and sustain access before and during crises.

A next-generation long-range surface-to-air Standard Missile, modernized E-2 Hawkeye radar and Cooperative Engagement Capability will combine to extend sea-based cruise missile defense far inland. This will reinforce the impact of sea-based ballistic missile defense and greatly expand the coverage of Naval area defense. These capabilities represent a broadened mission for our Navy that will lessen the defensive burden on land forces and increase sea-based influence over operations ashore.

"... In the role of ForceNet chief engineer, we must think outside the boundaries of SPAWAR's traditional product lines to build a truly robust architecture encompassing the integration of weapon, sensor and information grids ... It is an exciting time to be a part of the SPAWAR team. Our mission is critical, now more than ever, to the Navy and Nation during the war against terrorism. In the weeks and months to come, we must continue to focus on providing the blue prints for ForceNet ..."

Rear Adm. Kenneth D. Slaght, COMSPAWAR, addressing SPAWAR employees, June 21, 2002

Offensive and Defensive Independence

... Sea Basing serves as the foundation from which offensive and defensive fires are projected — making Sea Strike and Sea Shield realities. As enemy access to weapons of mass destruction grows, and the availability of overseas bases declines, it is compelling both militarily and politically to reduce the vulnerability of U.S. forces through expanded use of secure, mobile, networked sea bases. Sea Basing capabilities will include providing Joint Force Commanders with global command and control extending integrated logistical support to other Services. Afloat positioning of these capabilities strengthens force protection and frees airlift-sealift to support missions ashore.

Netted and dispersed sea bases will consist of numerous platforms, including nuclear-powered aircraft carriers, multi-mission destroyers, submarines with Special Forces and maritime prepositioned ships, providing greatly expanded power to joint operations. Sea-based platforms will also enhance coalition-building efforts, sharing their information and combat effectiveness with other nations in times of crisis.

Sea Basing accelerates expeditionary deployment and employment timelines by prepositioning vital equipment and supplies in-theater, preparing the United States to take swift and decisive action during crises. We intend to develop these capabilities to the fullest extent. Strategic sealift will be central to this effort. It remains a primary mission of the U.S. Navy and will be critical during any large conflict fought ashore. Moreover, we will build prepositioned ships with at-sea-accessible cargo, awaiting closure of troops by way of high-speed sealift and airlift. Joint operational flexibility will be greatly enhanced by employing prepositioned shipping that does not have to enter port to off-load. Twenty-first-century operations will require greater efficiencies through the development of joint logistical support ...

ForceNet is the glue ...

ForceNet is the "glue" that binds together Sea Strike, Sea Shield and Sea Basing. It is the operational construct and architectural framework for Naval warfare in the information age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force. ForceNet will provide the architecture to increase substantially combat capabilities through aligned and integrated systems, functions, and missions. It will transform situational awareness, accelerate speed of decision and allow us to greatly distribute combat power. ForceNet will harness information for knowledge-based combat operations and force survivability and provide real-time enhanced collaborative planning among joint and coalition partners.

Using a total system approach, ForceNet will shape the development of integrated capabilities. These include maritime information processing and command and control components that are fully interoperable with joint systems; intelligence, surveillance, and reconnaissance fusion capabilities to support rapid targeting and maneuver; open systems architecture for broad and affordable interoperability; and safeguards to ensure networks are reliable and survivable. ForceNet also emphasizes the human factor in the development of advanced technologies. This philosophy acknowledges that the warrior is a premier element of all operational systems. Today, ForceNet is moving from concept to reality. Initial efforts will focus on integrating existing networks, sensors and command and control systems. In the years ahead, it will enable the Naval service to employ a fully netted force, engage with distributed combat power, and command with increased awareness and speed as an integral part of the joint team.

Global Concept of Operations

Sea Power 21 will be implemented by a Global Concept of Operations that will provide our nation with widely dispersed combat power from platforms possessing unprecedented warfighting capabilities ... The Global Concept of Operations will disperse combat striking power by creating additional independent operational groups capable of responding simultaneously around the world. This increase of combat power is possible because technological advancements are dramatically transforming the capability of our ships, submarines and aircraft to act as power projection forces, netted together for expanded warfighting effect.

... The Global Concept of Operations requires a fleet of approximately 375 ships that will increase our striking power from today's 12 carrier battle groups, to 12 Carrier Strike Groups, 12 Expeditionary Strike Groups, and multiple missile-defense Surface Action Groups and guided-missile submarines. These groups will operate independently around the world to counter transnational threats and they will join together to form Expeditionary Strike Forces — the "gold standard" of Naval power — when engaged in regional conflict.

Sea Trial, Sea Warrior and Sea Enterprise

We are developing Sea Strike, Sea Shield and Sea Basing through a supporting triad of organizational processes: Sea Trial, Sea Warrior and Sea Enterprise — initiatives that will align and accelerate the development of enhanced warfighting capabilities for the fleet .... The Navy starts with the fleet, and Sea Trial will be fleet-led. The Commander, U.S. Fleet Forces Command, will serve as Executive Agent for Sea Trial, with Second and Third Fleet commanders sponsoring the development of Sea Strike, Sea Shield and Sea Basing capabilities. These commanders will reach throughout the military and beyond to coordinate concept and technology development in support of future warfighting effectiveness. The Systems Commands and Program Executive Offices will be integral partners in this effort, bringing concepts to reality through technology innovation and the application of sound business principles.

The Navy Warfare Development Command, reporting directly to the Commander, U.S. Fleet Forces Command, will coordinate Sea Trial. Working closely with the fleets, technology development centers and academic resources, the Navy Warfare Development Command will integrate wargaming, experimentation, and exercises to speed development of new concepts and technologies. They will do this by identifying candidates with the greatest potential to provide dramatic increases in warfighting capability. Embracing spiral development, these technologies and concepts will then be matured through targeted investment and guided through a process of rapid prototyping and fleet experimentation.

" ... I don't need anymore R&D bills for the old Navy stovepipe — everything we build or buy — will be for a joint environment ..."

... The Sea Warrior program implements our Navy's commitment to the growth and development of our people. It will serve as the foundation of warfighting effectiveness by ensuring the right skills are in the right place at the right time. Led by the Chief of Naval Personnel and Commander, Naval Education and Training Command, Sea Warrior will develop naval professionals who are highly skilled, powerfully motivated, and optimally employed for mission success.

Traditionally, our ships have relied on large crews to accomplish their missions. Today, our all-volunteer service is developing new combat capabilities and platforms that feature dramatic advancements in technology and reductions in crew size. The crews of modern warships are streamlined teams of operational, engineering and information technology experts who collectively operate some of the most complex systems in the world. As optimal manning policies and new platforms reduce crew size further, we will increasingly need Sailors who are highly educated and expertly trained.

In July 2001, we established Task Force EXCEL (Excellence through our Commitment to Education and Learning) to begin a revolution in training that complements the revolution in technologies, systems, and platforms for tomorrow's fleet. We are dedicated to improving our Sailors' professional and personal development, leadership, military education, and performance. Task Force EXCEL will apply information-age methods to accelerate learning and improve proficiency, including advanced trainers and simulators, tailored skills training programs, improved mentoring techniques, and more effective performance measurement and counseling tools.

... Central to Sea Warrior is Project SAIL (Sailor Advocacy through Interactive Leadership). Project SAIL is moving the Navy toward an interactive and incentivized distribution system that includes guaranteed schools for high-performing non-rated personnel, team detailing, Internet job listings, an information call center and expanded detailer outreach. These actions will put choice in the process for both gaining commands and Sailors, and it will empower our people to make more informed career decisions. Our goal is to create a Navy in which all Sailors — active and reserve, afloat and ashore — are optimally assessed, trained and assigned so that they can contribute their fullest to mission accomplishment.

Among the critical challenges that we face today are finding and allocating resources to recapitalize the Navy. We must replace Cold War-era systems with significantly more capable sensors, networks, weapons, and platforms if we are to increase our ability to deter and defeat enemies.

Sea Enterprise, led by the Vice Chief of Naval Operations, is key to this effort. Involving the Navy Headquarters, the Systems Commands and the Fleet, it seeks to improve organizational alignment, refine requirements, and reinvest savings to buy the platforms and systems needed to transform our Navy. Drawing on lessons from the business revolution, Sea Enterprise will reduce overhead, streamline processes, substitute technology for manpower and create incentives for positive change. Legacy systems and platforms no longer integral to mission accomplishment will be retired, and we will make our Navy's business processes more efficient to achieve enhanced warfighting effectiveness in the most cost-effective manner.

... It is also important that our leaders understand sound business practices so that we can provide the greatest return on the taxpayer's investment. To meet this need, we are creating educational opportunities to teach our leaders about executive business management, finance and information technology. For example, the Center for Executive Education at the Naval Postgraduate School brings together rising flag officers and private industry decision-makers to discuss emerging business practices. We must also extend this understanding to the deckplates, so that our future leaders gain experience in a culture of strengthened productivity and continually measured effectiveness.

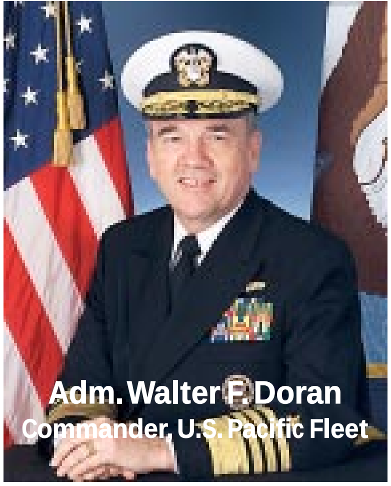
Increased inter-service integration also holds great promise for achieving efficiencies. For example, the Navy and Marine Corps tactical aviation integration plan will save billions of dollars for both services, enhance our interoperability, and more fully integrate our people. Whether it is the U.S. Coast Guard's Deepwater Integrated Systems Program, new munitions being developed with the U.S. Air Force, joint experiments with the U.S. Army on high-speed vessels, or a new combined intelligence structure with the U.S. Marine Corps, we will share technologies and systems whenever possible ... Savings captured by Sea Enterprise will play a critical role in the Navy's transformation into a 21st-century force that delivers what truly matters: increased combat capability.

"... Generation X, what is that? ... All I can say is that the young people in the Navy today fighting in defense of freedom are the best. I am very proud of the job they are doing ..."

Global Naval Power

The 21st century is clearly characterized by dangerous uncertainty and conflict. In this unpredictable environment, military forces will be required to defeat a growing range of conventional and asymmetric threats. Sea Power 21 is our vision to align, organize, integrate, and transform our Navy to meet the challenges that lie ahead ... It is global in scope, fully joint in execution, and dedicated to transformation. It reinforces and expands concepts being pursued by the other Services — long-range strike; global intelligence, surveillance, and reconnaissance; expeditionary maneuver warfare; and light, agile ground forces — to generate maximum combat power from the joint team ... □

Uniting and Securing the Pacific Through Technology



Adm. Walter F. Doran
Commander, U.S. Pacific Fleet

Edited from a brief given by Adm. Doran at TechNet Asia-Pacific 2002, November 2002.

"Uniting and Securing the Pacific through Technology" is an appropriate theme, considering the vastness, diversity, and importance of the region. Earlier this year, while addressing the Diet in Tokyo, President Bush said that the success of the Pacific is essential to the entire world, and that he's convinced *"the 21st century will be the Pacific century."* That's quite an endorsement ... and, it highlights for us that a stable, united, and secure Pacific is in our, and the world's best interest. As the Pacific Fleet Commander, that is one of my primary tasks and I need the help of all of you to accomplish it.

Another important responsibility that I have is to organize, train and equip our Naval Forces for the Pacific Commander, in carrying out that responsibility, I depend on you again ... because we equip our Sailors with the systems and technology that you develop so that they can accomplish the mission. I'll discuss that mission and our current operations and touch upon the technology, developed by many of you, that enables Sailors to succeed ... then I'll describe our vision and goals for the future ... of which you are an increasingly important part.

We are a 310 ship Navy. Today, 161 of these ships are underway or away from their homeport, and of these, 115 are deployed ... more than half from the Pacific. The USS Abraham Lincoln is flying missions over Iraq enforcing the Southern No-Fly zone. The ships of her Battle Group are enforcing U.N. Sanctions against Iraq and hunting for terrorists on the high seas with our allies. The Belleau Wood Amphibious Ready Group is wrapping up her tour in the region supporting Operation Enduring Freedom and contingency operations, and is headed home via some well-deserved port visits. The USS Kitty Hawk, our forward-deployed carrier homeported in Yokosuka, Japan, recently completed Carrier Qualifications with her air wing and is a "full-up round" after a brief respite and a much-needed maintenance period. The Forward Deployed Naval Force truly remains the "Tip of the Spear" in the Western Pacific.

The Essex Amphibious Ready Group, also homeported in Japan, is ready for tasking and training hard. The Constellation Battle Group left San Diego almost three weeks ago en route to the war, and the Tarawa Amphibious Ready Group is in the final stages of their training. The Carl Vinson Battle Group is also training hard and will deploy soon. No surprises here. This is what we do, and we do it better than any Navy in history. None of us know what the future will hold — but the Pacific Fleet will be ready if called.

This past year in support of the Global War on Terror, the Navy has deployed seven Carrier Battle Groups, five Amphibious Ready Groups, and more than 80,000 Sailors and Marines to Southwest Asia. Less than a month after September 11, our pilots were flying combat missions over 1,000 miles inland taking the fight to the Taliban and al Qaeda with a 70 percent bombing effectiveness rate. This is a tribute to our outstanding Airmen and hardworking Sailors, and to you — the technical community — who develop the tools that help us do our jobs better and more efficiently.

Much has been said about our asymmetric scientific and technological advantage, and how we will use this advantage to continue to dominate the battlespace. Your work in the critical areas of communications, electronics, intelligence and information systems, is helping us win the war on terrorism, and will be critical as we continue the fight against a distributed, elusive and dangerous enemy. While we ARE winning, the war is far from over as demonstrated in Yemen, Indonesia, the Philippines and elsewhere.

Thanks to you, our Sailors on the frontline have some extraordinary tools to accomplish their mission. Communications systems are more automated and much more reliable. Radioman have been transformed into Information Technicians. They manage a myriad of communications and Link systems including SHF, EHF SATCOM MDR, Link 16, Satellite Link 16 and multiple forms of old reliable Link 11.

In addition to being the first battle group to deploy the F/A-18 E/F and taking forward our Sea Swap initiative with USS Fletcher — the Abraham Lincoln Battle Group has brought the Joint Fires Network, a network-centric warfare system that enables real-time engagement of time critical targets. This capability will allow ships in a battle group to share real time targeting and intelligence data with each other, as well as with other warfighting assets in a joint or coalition task force.

Area Air Defense Commander capabilities also accompanied Lincoln to the fight, and next year's deployment of Nimitz Battle Group will introduce Cooperative Engagement Capability to the Pacific Fleet. Today, Collaboration at Sea and K-WEB are addressing the challenge that Naval Forces face in connecting a large group of worldwide users to a significant amount of information, in an environment of low bandwidth and intermittent connectivity. Collaboration at Sea and K-WEB are addressing these issues through the use of three important tools: a standardized operational Web site for non-real time collaboration, chat capability for real time collaboration, and customized Web site replication to mitigate bandwidth limitations. In the past, Battle Group Commanders' fireside chats were conducted via a satellite command circuit — a Communications Officer's nightmare! Today, in many cases, they are conducted via chat room. Warfare Commanders have separate chat rooms to help manage the war, as do operators to share expertise and experience.

A Joint Task Force can now train via the Web ... In the Pacific Fleet, we have just demonstrated the value and efficiency of this innovative training tool. Sailors, Soldiers, Airmen and Marines, making up a standing Joint Task Force, can train through Web-based technology at their individual duty stations. Then, when called upon, can assemble as a JTF and carry out missions directed by the Pacific Commander. This is truly transformational and has great potential for use, not only here, but in every theater. We are also pushing the bandwidth envelope. Photos of suspected oil smugglers or terrorists are relayed back from the front where their profiles can be compared in worldwide databases. Through Distance Support, ship technicians are reaching back to CONUS for help in troubleshooting and repairing casualties allowing ships to stay on station and minimize the expense of flying technicians to the theatre. There are many other examples. Advances in IT have taken the Navy into the 21st Century. We are breaking new ground with unmanned vehicles, shortening the timeline from sensor to shooter, and adding precision and lethality to our weapons.

USS Abraham Lincoln (CVN 72) Nov. 24, 2002 — EWS2 Sarah Lanoo operates a Naval Tactical Data System (NTDS) console in the Combat Direction Center (CDC) aboard USS Abraham Lincoln. The Abraham Lincoln is on a regularly scheduled deployment conducting combat operations in support of Operation Southern Watch. U.S. Navy photo by PH3 Patricia Totemeier.

But, as we all know, advancement and innovation does not come without challenges. One such challenge is bandwidth. Our new Arleigh Burke Aegis Destroyers, even with a Dual Inmarsat capability, are limited to 64 kilo bits per second, and [they] have multiple antenna blind zones to manage. Bandwidth allocation and management — Fleet and Battle Group-wide — is still a challenge, as is interoperability with our coalition, and in some cases, joint partners. The Coalition Wide Area Network is a success and being used extensively during Operation Enduring Freedom as a critical communications link with our coalition partners. However, COWAN has many restrictions making information sharing across the coalition often very, very difficult. We must get this right.

These are some of the nagging problems that Sailors work through daily. The future holds the solutions to these problems, because you will deliver them along with other advances and innovations not yet imagined. To achieve this goal — with your help and capability — we in uniform must share our vision of the future. I'm convinced the future is exciting for the U.S. Navy ... and while our focus remains unquestionably the Global War On Terrorism, we must plan and prepare for a dynamic and indeed an uncertain future. Today's strategic environment is far less stable than the era of the Cold War where we had predominantly one competitor and adversary — the former Soviet Union.

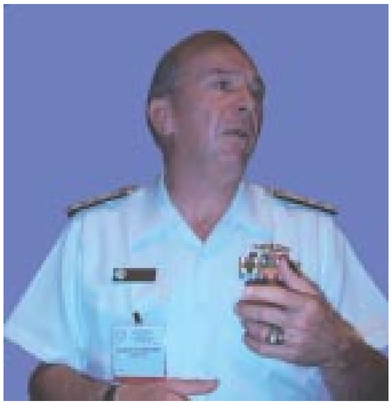
Today in the Pacific we face a multitude of threats from state and non-state actors magnified by the proliferation of weapons of mass destruction. To effectively deal with this destabilizing and dangerous threat, we must recapitalize our force, transform, and distribute our combat power. As defined by Adm. Clark, our CNO, Sea Power 21 is the blueprint for this change organized around three core operational concepts: Sea Strike (projecting precise, persistent, and decisive firepower globally from the sea), Sea Shield (projecting defensive power deep overland to protect our joint forces and ensure our access to the littoral), and Sea Basing (projecting operational independence for our joint forces from the sea).

The glue that binds these concepts together is ForceNet ... a concept that is being developed by Vice Adm. Dick Mayo and his crew at the new Naval Network Warfare Command. ForceNet, when fully developed, will integrate our ships, sensors and weapons into a networked combat force. The first step toward ForceNet is, in the near term, to network legacy systems and remove systems that can't be networked. Sea Power 21 will be implemented by a Naval Global Concept of Operations that restructures our force and distributes our striking power. Tomorrow's force will be made up of Carrier and Expeditionary Strike Groups, Missile Defense Surface Action Groups, the Cruise Missile Nuclear Submarine and a faster, more capable, and more versatile combat logistics force — all networked together.

In fact, in the coming year, both the Pacific and Atlantic Fleets will use deployers to experiment with the Expeditionary Strike Group [ESG - an amphibious ship with embarked Marine Expeditionary Units, a cruiser, a destroyer, a frigate, an attack submarine and dedicated P-3 Orion surveillance aircraft] concept, it combines surface combatants and submarines with our Amphibious Ready Groups and gives us greater operational agility and offensive capability. The experiments look different on each coast ... In the Pacific we will add a Flag Officer in command with an operational staff ... this will give us an opportunity to compare and learn from two different approaches. We will also experiment with this concept early next year during Exercise Tandum Thrust.

Sea Power 21 supporting initiatives already in development are: Sea Trial (a fleet-led effort to identify and transition promising capabilities to our ships through aggressive experimentation), Sea Warrior (an innovative training and detailing approach to ensure our Sailors are given the right skills, and are detailed commensurate with these skills at the right time), and Sea Enterprise (a badly needed streamlining of our resource and acquisition process). In the development of ForceNet, clearly there is a role for the technology community — your intellect, and experience, at every step of the transformation process to make Sea Power 21 a reality. It's going to be a fast and exciting ride and we will take it together. I will go further to say that your role in this process is absolutely vital. You are the source of our asymmetric advantage and the ones who, year after year, deliver our Sailors the tools to keep our nation safe.

Earlier this year, at the Argonne National Laboratory in Illinois, the President said, *"In this new war, we will rely upon the genius and creativity of the American people. Our scientific community is serving on the front lines of this war, by developing new technologies that will make America safer."* He couldn't be more right and this is the charge for each and every one of you. I hope that I have given you an adequate picture of where the Navy is, where we are going, and how much we appreciate and depend on your service. We all have a great challenge ahead of us, and I am confident that together we will meet those challenges.



Talking with Vice Adm. Albert H. Konetzni, Jr., USN Deputy and Chief of Staff U.S. Atlantic Fleet

"When President Theodore Roosevelt announced that the nation would 'Speak softly and carry a big stick,' the big stick he was referring to was the United States Navy ..."

Edited from remarks given by Vice Adm. Konetzni at the USNI Warfare Exposition and Symposium, Oct. 2, 2002.

It is a great pleasure to be with you to discuss the state of the U.S. Navy ... I had the great pleasure of welcoming the USS Monitor's turret home to Hampton Roads a few weeks ago. It was an impressive occasion. I think Monitor's story has great lessons for Americans.

In many ways USS Monitor symbolizes both the best and worst about America. In my view, America's greatest quality is our innovative spirit. Our freedom, ideas and actions have produced the world's greatest inventions and subsequently the greatest economy. At the same time, Americans have short memories. We, too quickly forget the sacrifices that have been made by so many to make this nation what it is today.

USS Monitor was clearly the most innovative ship of her day — an iron ship,172-feet long with a 41-feet, 6-inch beam and two 12-inch guns housed in a revolving turret. There are many first's associated with the USS Monitor, she was the first ship to have a revolving turret, she was the first ship where the officers and crew had to live entirely below the waterline, she was the first ship credited with having below waterline flushing toilets. [But] most important was the crew. The crew — like all of our Sailors today — were strictly volunteers.

Those young people valiantly fought the USS Virginia to a draw and ended Virginia's unchallenged assault on the U.S. Fleet. But what too many people forget is that those men went down in a storm because Monitor wasn't really ready for action. Our greatest weakness is that [our] memories are too short. USS Monitor was an innovative ship, but we could have done better.

The fact is that the Monitor's pumps were inadequate to keep her from sinking during stormy weather in December 1862. The USS Monitor's construction had been rushed because the U.S. Navy was too slow to embrace ironclads. In the end, Monitor sunk not from enemy fire, but from faulty systems and design. That is the message I want to bring to you today. We have a great country, capable of awesome Naval innovation. We have great young men and women, who will carry the day when the nation calls. If we ignore history we will allow our readiness to slip and our force structure to dwindle. Our young people are the ones who will suffer the consequences.

Innovation, especially in America, is truly accelerating. Think of how the cellular telephone and personal computer have changed our lives. Technologies like the Global Positioning System and unmanned systems are changing the way we live and fight. I am convinced that these are just the tips of the technological iceberg of change. The question is: How do we capture these innovations and use them correctly to ensure that we are ready for the challenges ahead? In my view, great innovations will only be successful if they are formed by knowledge of history. We have not always applied American ingenuity soon enough to make a difference.

History is full of examples of [America] not being ready for the worst: World War II — after a devastating blow at Pearl Harbor, we sent our submarines to the fight with torpedoes that didn't work; in Korea — our soldiers froze because they didn't have warm clothing and we didn't have the bridge forging machines that we needed. In Vietnam — we didn't build the national and military resolve necessary to win.

Unfortunately, the war on terrorism in some ways is no different. I could go on all day about the [problems] of the nineties ... as a result, our Navy had some real problems at the start of the war [on terrorism]. We didn't have enough bombs to get the job done and were forced to borrow thousands from the U.S. Air Force. Years of neglect on maintaining the Fleet showed, as we had to pump millions of dollars into the USS John F. Kennedy to get her underway. The size of our Fleet is dwindling toward 300 ships or lower — yet we don't have the resources to build ships while at the same time maintain the ones we have.

Our nation's foreign policy with regard to terrorism was also rather naive. In hindsight, it is clear that our response to terrorism pre-9-11 was inadequate. If we had taken the time to understand history and our cultural differences with other people, we may have seen the signs of 9-11 on the horizon. Whether it was Lebanon, Khobar Towers, our embassies in Africa, or the USS Cole, our responses were piecemeal and ineffective ...

History has told us that wars always result from miscalculation. We left the impression in the minds of the terrorists that we were weak and unwilling to risk going after them. We left the widespread idea that America would only lob a few rockets and then go home. How wrong they were ...

...I don't want you to get the impression that I am negative — quite the opposite. We are making real progress in this war. The Taliban that supported al Qaeda is no longer in power in Afghanistan. Almost 2,000 terrorists and their supporters have been captured. President Bush is serious when he says that "We will not stop until we get them all." Naval Forces are the

difference-makers in this new war: ♦In the last year, six CVBGs (Carrier Battle Groups) and seven ARGs (Amphibious Ready Groups) have sustained our Seals and Marines over 600 miles inland. ♦The USS Kitty Hawk (CV-63) deployed immediately to serve as a forward operating base for our special forces. ♦Carrier Aircraft have struck over 2,000 targets on missions that have sometimes lasted over 12 hours. ♦Our ships have launched over 100 tomahawk missiles. ♦We have conducted over 200 boardings in support of operations aimed at capturing fleeing terrorists.

We are winning the war on terrorism mainly because of our wonderful people in the military. It comes as no surprise to me that our young people have performed so brilliantly. There has been a lot of talk about this generation or that generation, but let there be no doubt — this current generation is up to the challenge. I have vivid memories of meeting with a young Seal at the Portsmouth Naval Hospital. I can't tell you his name, but his nickname is Turbo. Turbo went to some hellish places to take on al Qaeda. He gave his left leg for his country and some of his buddies gave their lives. You can be proud of your Navy's performance during this war on terrorism. The simple fact is that we could not have executed the campaign in Afghanistan without our nation's aircraft carriers and all the ships — and all the young people that support them. At the same time, however, we all know that the nation is not building enough ships and submarines to accomplish all we are being asked to do today and in the future. We need 8 to 10 [new ships] per year to sustain current force structure; we will build 5 in FY02.

Our efforts in Afghanistan have proven the U.S. Navy is truly the key to success in 21st century warfare where we often will not have forward bases from which to operate. Our dilemma is that given our current resources, we can't maintain a forward fleet, fight the war, maintain our ships at the right level of readiness, and build enough ships to have a future fleet that is adequate. First, we need to be more efficient — then we must argue for an appropriate bottom line. The nation needs to know the consequences for not maintaining and building an adequately sized fleet. So now, the problem that we as a nation face: Which vital missions do we ignore? Which ships do we allow to rust at the pier? Which world crisis do we neglect in order to respond to some other crisis, somewhere else? We need to make the intellectual argument for fully funded depot level maintenance, and building the right number of ships and aircraft. In the end, the Congress and the public need to understand that maintaining the most capable Navy in the world is expensive. But it is still the best security investment for their dollar.

I need your help in keeping the Navy at the forefront of the public's mind. I ask you to read, speak, think and write about our Navy's future. Start a debate. Try and answer some questions like: Do we need more ships, aircraft and submarines? If so, why? For what missions? What should the future Fleet look like? Do we have ship maintenance right or is more needed? Are we on the right course with regard to attrition, retention and leadership? How can we meet the threats of terrorism and weapons of mass destruction? Is Asia going to explode? How can we ensure it doesn't? In the end, it's your Navy and decisions made without a healthy debate are always flawed.

Mine Warfare ...

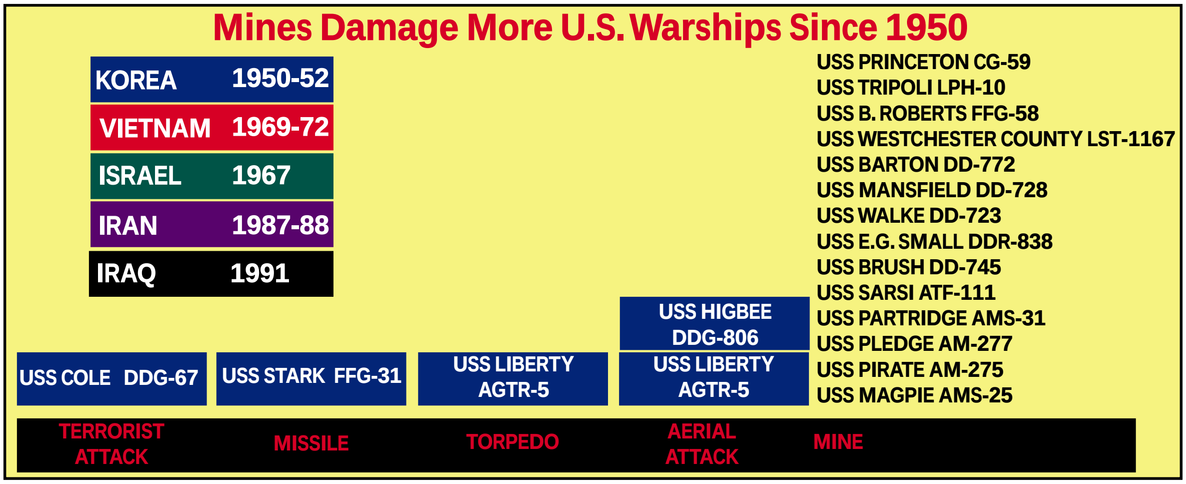
Edited from a brief given by Vice Adm. Konetzni, Jr., Deputy and Chief of Staff, U.S. Atlantic Fleet at the USNI Warfare Exposition and Symposium. Vice Adm. Konetzni invited the press to a dialogue on mine warfare to fully understand the scope of Naval requirements. Thanks to Rear Adm. Paul Ryan, Commander MINEWARCOM and Lt. j.g. Herlina Rojas, MINEWARCOM Public Affairs Officer, for their expert insight and comments regarding this article.

Sea mines have been an historically important factor in naval warfare. Mines have caused major damage to naval ships, slowed or stopped commercial shipping, and forced the alteration of strategic and tactical plans. Fourteen U.S. Navy ships have been sunk or damaged by mines since World War II (see Figure 1), over three times the number damaged by air and missile attack. Today, advancing technology heightens the threat posed by mines, making them more difficult to detect, classify and neutralize. These experiences, plus the ready availability to potential adversaries of inexpensive sea mines (see Figure 2) have increased interest in mine warfare within the U.S. Navy. In 1995, the Chief of Naval Operations directed that mine warfare receive greater emphasis and become an integral capability of battle forces rather than remain the sole province of a dedicated force.

Mine warfare (MIW) is comprised of both mining operations and mine countermeasures, and may be either offensive or defensive in nature. Mine countermeasures (MCM) incorporate much more than actual mine detection and neutralization. Key elements of MCM include: intelligence; reconnaissance and warning; development and exploitation of environmental databases; reduction of ships' magnetic and acoustic signatures; and specialized training in mine warfare tactics.

Successful integration of MIW capability into battle group units requires its promotion as a major warfare area, similar to the traditional air, surface and submarine specialties. Each of these warfare specialties has a "sponsor," specific to the platform type, within the OPNAV requirements division (N7). In contrast, MIW, in which effective execution requires use of platforms from various warfare specialties, has a capabilities-based sponsor, Expeditionary Warfare (N75). Public law [10 USC 505] mandates this sponsorship. Careful consideration should be given to the appropriate sponsorship for Mine Warfare so that the benefits of capabilities-based sponsorship can be maintained while advancing the emphasis on Mine Warfare as a vital warfare competency.

The development of MIW capability within the battle force is known as "mainstreaming." Mainstreaming of MIW can and should be happening today, independent of the introduction of organic mine warfare capabilities into the battle force. Fielding a MCM capability organic to battle force units provides increased impetus to development of MIW expertise. At the same time, mainstreaming provides the professional foundation on which effective utilization of future organic assets will be built. However, mainstreaming, with its emphasis on development of capabilities within the battle force, may lead to the misconception that new organic mine countermeasures systems (OMCM) are replacements for existing dedicated platforms. This is not the case.



Mines Damage More U.S. Warships Since 1950

KOREA	1950-52
VIETNAM	1969-72
ISRAEL	1967
IRAN	1987-88
IRAQ	1991

TERRORIST ATTACK	MISSILE	TORPEDO	AERIAL ATTACK	MINE
USS COLE DDG-67	USS STARK FFG-31	USS LIBERTY AGTR-5	USS HIGBEE DDG-806 USS LIBERTY AGTR-5	USS PRINCETON CG-59 USS TRIPOLI LPH-10 USS B. ROBERTS FFG-58 USS WESTCHESTER COUNTY LST-1167 USS BARTON DD-772 USS MANSFIELD DD-728 USS WALKE DD-723 USS E.G. SMALL DDR-838 USS BRUSH DD-745 USS SARSI ATF-111 USS PARTRIDGE AMS-31 USS PLEDGE AM-277 USS PIRATE AM-275 USS MAGPIE AMS-25

Figure 1.

What is the Threat?

- Cheap
- Lethal
- Asymmetric
- Widely Proliferated

275,000 Mines Worldwide

Figure 2.

A good way to view the distinction between organic and dedicated MIW resources is to classify them either as tactical or strategic assets. Organic MCM systems are tactical in nature. They are resident within the battle group, and are intended to provide the ability to detect mines and a limited minesweeping capability that permits "punching through" a minefield if necessary. Dedicated MCM systems are theater or strategic assets. They are intended to provide large area or long-term MCM capability.

Mine Warfare Command (MINEWARCOM) demonstrated its capability during a ten day at sea training period in the Gulf of Mexico in October 2002 with Norfolk-based USS Kearsarge (LHD 3). USS Kearsarge, acting as a stand-in Mine Warfare Command ship, embarked airborne, surface and undersea MCM personnel and equipment from Naval Station (NS) Ingleside and Naval Air Station (NAS) Corpus Christi during this simulated wartime scenario. According to Rear Adm. Paul Ryan, Commander, Mine Warfare Command, mine warfare forces are expeditionary by design. Packing up and going where needed and when needed is how mine warfare was conducted prior to Desert Storm and prior to having a dedicated mine warfare command and support ship. "This exercise familiarized a new generation of mine warfare personnel with the details of embarking on a ship of opportunity," said Ryan.

During the exercise, MINEWARCOM used USS Kearsarge as a host ship and exercised all three legs of the MCM triad: airborne, surface and underwater MCM. A squadron of MH-53 minehunting helicopters from NAS Corpus Christi provided airborne MCM. Explosive ordnance disposal (EOD) units embarked on USS Kearsarge provided underwater MCM. Three NS Ingleside minehunter and minesweeper ships, USS Sentry (MCM 3), USS Scout (MCM 8) and USS Devastator (MCM 6), provided surface MCM. "We utilized USS Kearsarge the same way we utilized USS Inchon. We hunted for exercise mines, swept the mines once they were located, and used EOD personnel to neutralize designated mines," added Ryan. When the exercise was completed, USS Kearsarge returned to Norfolk.

Since the decommissioning of USS Inchon in June 2002, the Navy has been evaluating options for a permanent replacement. In October, the Navy's Military Sealift Command awarded a $21 million one-year charter contract with renewable one-year options to Bollinger/Incat USA, L.L.C. for the leasing of a High Speed Vessel (HSV). The ship will support U.S. Navy Mine Warfare Command and serve as a test platform for experiments with advanced hull and propulsion technology integrated with advanced communications technology. Currently, the HSV is slated to participate in three exercises from September to December 2003. These exercises include Atlantic Fleet Joint Task Force Exercise, Gulf of Mexico (GOMEX 04-1) Exercise and Pacific Fleet Joint Task Force Exercise.

Top: EOD units embarked aboard USS Kearsarge (LHD 3) launch their RHIBs (Rigid Hull Inflatable Boats) from the ship's well deck while three minesweepers from Naval Station Ingleside look on. Bottom: The Navy's HSV-1X. (U.S. Navy photos.)

Mine Countermeasures Ship (MCM/MHC) Reliability

The need for U.S. Naval forces to maneuver and project power in the world's littorals is increasing. Littorals are highly susceptible to extensive enemy mining. Current MCM force consists of 14 MCMs with minesweeping (mechanical, magnetic and acoustic) and minehunting (detect, classify, identify, neutralize) capabilities, and 12 MHCs with mine hunting capabilities only. Dedicated MCM capability is required for deliberate, large-area mine clearance. Planned organic capabilities provide "See & Avoid" hunting and

Near-Term Recommendations

- With the decommissioning of Inchon, make MCS functions portable.
- Plan to use "Large Deck of Opportunity."
- Exercise portable functions regularly.
- Plan for a replacement MCS.
- Re-engine MCM/MHCs with priority on MCMs (~ $100 million).
  - Consider intermediate maintenance contract for diesels.
- Support long-range class modernization program.
- Require frequent deployments to improve fleet engagement.

Mid-Term Recommendations

- Retain MH-53E until an adequate replacement is developed.
- Upgrade MH-53E with "Organic" technologies.
- Support "Organic" introduction plan.
- Fund current dedicated MCM forces.
- Upgrade dedicated MCM force with proven organic technology.
- Fund phased acquisition of a standoff mining capability.
- Fund development and phased acquisition of modern mine inventory.

Long-Term Recommendations

- Make unmanned sweeping systems a fleet requirement.
- Demonstrate concept with current systems.
  - Ex: Unmanned Surface Vessel (USV) tows MK-106 Sled/SQS-20.
- Consider MCS(X) options with emphasis on unmanned systems.

Figure 3. Mine Warfare Study Outline

"Punch Through Clearance" but are insufficient for sustained, large-scale mine clearance. MCM ships require upgrades to improve equipment reliability through their planned service life (~2022). C4I upgrades are required to maintain MCM/MHC effectiveness.

Mine Warfare

MIW is composed of both Mining and MCM. The proliferation of inexpensive, lethal sea mines makes MIW a critical war fighting capability. Combating mine threat requires an amalgam of surface, air and undersea capabilities. The variety of platforms and equipment involved makes assignment of the optimum OPNAV program sponsorship difficult. OPNAV program sponsorship must be properly aligned to ensure that maximum benefit is obtained from scarce resources. Capabilities-based rather than platform-based sponsorship may provide MIW with better representation.

The future of MIW lies with emerging technologies, and will most likely include the use of unmanned, undersea vehicles (UUVs), remotely controlled sensor arrays and various other undersea platforms/weapons. The future vision of distributed sensor fields with embedded autonomous mines plus remotely controlled minefields will require extensive water space management.

Organic Mine Countermeasures (OMCM) Capabilities

A key requirement of Naval Studies Planning Group objectives is to develop mine detection and clearance capabilities organic to CV [carrier] battle groups (shown in Figure 4) permitting these forces to identify, avoid, or neutralize mines within operationally acceptable timelines and with acceptable levels of operational risk. On-scene MCM capabilities, through introduction of organic capabilities into all CVBGs, will be completed by 2012. Introduction of these capabilities to the first CVBG is planned for 2005. CVBGs are currently deployed with limited active MCM capabilities. MIW capabilities include intelligence collection and surveillance; notification of imminent mining; interdiction; post-interdiction intelligence evaluation and dissemination; and passive MCM (threat awareness and signature control). Embedded MIW capabilities are not being fully realized. Current C2F/C3F mainstreaming initiatives are focused on leveraging these embedded capabilities today. CVBGs today have no capability to detect or avoid mines (except for drifters or detecting minelayers and localizing the potential hazard area to avoid). The Kingfisher system (a funded software upgrade to the SQS-53 Sonar) may provide a mine avoidance capability, but will require a dedicated operator training program that does not exist today.

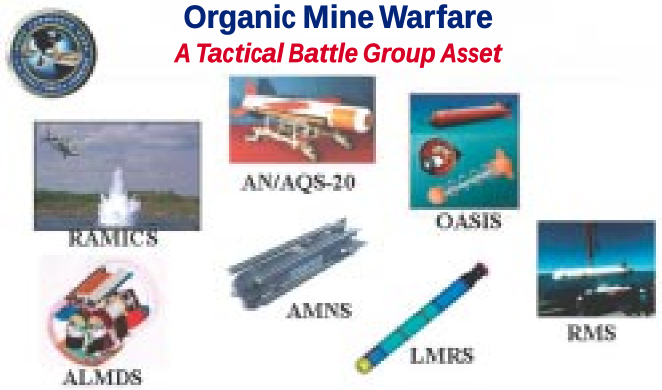
The proliferation of inexpensive, lethal sea mines makes MIW a critical war fighting capability. Combating mine threat requires an amalgam of surface, air and undersea capabilities.

Seven OMCM systems are currently under development and planned for battle group introduction. These systems are intended to instill an MCM capability "organic" to battle group forces. This capability will not be adequate to replace the dedicated MCM forces that currently exist. ♦The Long-term Mine Reconnaissance System (LMRS) is an autonomous UUV, launched and recovered from 688- and 744-class submarines, which provides clandestine mine reconnaissance (detection and limited classification) for advanced battle space preparation. A LMRS system on a host submarine would yield a total system area coverage of up to 400-650 square nautical miles. Engineering challenges include meeting mission reliability goals; achieving reliable launch and recovery; meeting ambitious reduced radiated noise goals; certifying an advanced high-density primary battery for submarine use; and developing effective computer-aided detection/classification algorithms. Nets, cables, nonmilitary shipping and other obstacles, or piracy of the unit can potentially cause premature mission abort. LMRS navigation accuracy remains a potential issue for contact reacquisition, identification and mine neutralization. ♦The Remote Mine-hunting System (RMS) includes a semiautonomous, semi-submersible vehicle that

Figure 4.

Organic Mine Warfare

A Tactical Battle Group Asset



Incorporates a mixture of low, medium and high risk options with a good anticipated rate of return

tows mine reconnaissance sonar and is launched and recovered by surface ships. Engineering challenges include achieving desired high duty cycles and demonstrating reliable launch and recovery techniques even in high sea states. Nets, cables, nonmilitary shipping and other obstacles, or piracy of the unit can potentially cause premature mission abort.

Five remaining MCM systems are airborne (AMCM) being developed primarily for the MH-60s with various launch dates between 2003 and 2007. ♦The AN/AQS-20X, an evolution of current technology, is a towed mine hunting system that includes identification capability. A key engineering challenge includes enhanced CAD/CAC algorithms to achieve reduced false contact rates. ♦The Airborne Mine Neutralization System (AMNS) is an expendable, remotely operated, mine neutralization device compatible with both MH-60s and MH-53E. Deployment from MH-60s including associated munitions certification tests must be demonstrated. ♦The Organic Airborne and Surface Influence Sweep (OASIS) is a combination magnetic/acoustic influence sweep towed system. It provides only OMCM influence sweep capability. Engineering challenges include ensuring the ability to survive shallow water detonations from various mines and achieving appropriate tow depths and speed to effectively sweep certain difficult shallow water bottom influence mines. Its 800 amp system provides roughly half the capability of the MK-105 sled. Significant depth and sweep limitations may prove inadequate for many areas. ♦The Airborne Laser Mine Detection System (ALMDS) is an electro-optical-based mine reconnaissance system capable of rapid detection, localization, and classification of mines on or very near the sea surface (about 40-feet water depth, dependent on turbidity). Engineering challenges include achieving desired or acceptable false contact rates and achieving adequate depth coverage under likely conditions. ♦The Rapid Airborne Mine Clearance System (RAMICS) is a gun system designed to rapidly acquire, target and neutralize floating and near-surface moored mines. It is the least mature of the airborne MCM systems. Engineering challenges include establishing safe helicopter standoff distances from floating or very-near-surface mines, and establishing a gun and turret installation concept that minimizes the impact on the aircraft in terms of loads, recoil and flight dynamics.

The Navy's implementation plan for OMCM includes a mixture of low, medium and high-risk options with good anticipated rates of return.

Mining Issues and Recommendations

For a variety of reasons, the U.S. Navy risks a severely limited ability to conduct mining operations. Without high-level attention and funding now, this critical warfare requirement will be seriously degraded within the next five years. Current mine inventories are adequate to meet requirements for most scenarios, however the small size and advanced age of the stockpile limit operational flexibility. A standoff/high altitude mine delivery capability is necessary for mining to be a viable offensive capability. A conversion kit is needed for the existing MK-62, MK-63 and MK-65 Quickstrike series mines. This is an unfunded requirement. A Tactical Decision Aid is necessary to restore a Fleet Level Minefield Planning capability. Currently all minefields must be planned by reachback. A replacement for the MK-56 intermediate depth moored mine is necessary to retain a mining response in the 150 to 600 feet regime. The Submarine Launched Mobile Mine (SLMM) provides the only clandestine mining capability. This weapon is rapidly reaching end of service life and is not compatible with Virginia Class submarines. I-SLMM development was stopped when Australia backed out of a bilateral development agreement due to funding. I-SLMM would double the payload over SLMM (2 mines vice 1), use the much more capable MK-48 torpedo, and provide a digital fire control capability/compatibility. The Navy's core mining infrastructure has been reduced to 21 engineers and scientists, and we continue to lose this talent to other programs as funding continues to be reduced. Further reductions in infrastructure funding will soon eliminate our ability to develop replacement mines without a significant reinvestment in time and funding.

Vision/Requirements

The U.S. Naval Mine Warfare Plan (developed by Adm. Johnson/ Gen. Jones, 2000) states that sea mines remain a classic, low-cost force multiplier of increased importance during fleet downsizing and increased littoral operations. It states that the Navy is to "develop, procure, maintain, and deploy a modern family of sea mines," with features that permit remote control of sea mines, standoff mining and full-water-depth mining.

Current U.S. Naval mining capability is adequate to execute requirements of some scenarios. However, the inventory is composed of old mines, and mining capabilities are funded at near the minimum levels required to safely maintain the stockpile. Research and development for new mining capabilities is severely restricted. The Navy has no funded plans to acquire any new mines in the next 7 years. A low priority has been placed on mining attributed in part to lack of specific sponsorship within OPNAV. "Mines are weapons that contribute to control of the surface and undersea environment, but their delivery (with the exception of small numbers of SLMMs) is accomplished entirely by air — with U.S. Air Force bombers being the primary platforms for high-volume delivery. Although mines have many of the characteristics of strike warfare weapons, the nominal Navy sponsor for mining is Expeditionary Warfare [N75], which is quite properly more concerned with MCM shortfalls." (NSB report, 2001)

Long-term solutions include use of innovative, emerging technologies for remote control of mines, distributed sensor fields, standoff deliveries, adaptation of new sensors for target influence (magnetic, acoustic, electric, pressure), miniaturization (easing delivery burdens), and the development of nonlethal mines to include devices for fouling propulsion, damaging electronic systems, etc. Recommendations include: The current war on terrorism suggests maintaining weapons stockpiles at levels greater than the minimum requirements; Modernize existing mine stocks with standoff/high altitude delivery capability; Retain the mining core infrastructure and begin development of a replacement for the MK-56 mine to preclude a gap in capability expected to develop by 2010; Add funding to develop a standoff mining capability. This might include production of I-SLMM or research and development on JDAM-ER type bomb conversion packages—or both; and Align functions within MIW community (OPNAV through COMINEWARCOM) to benefit the specific subset of mining operations in accordance with separate point paper on MIW Alignment. Realignment allows focus on operational

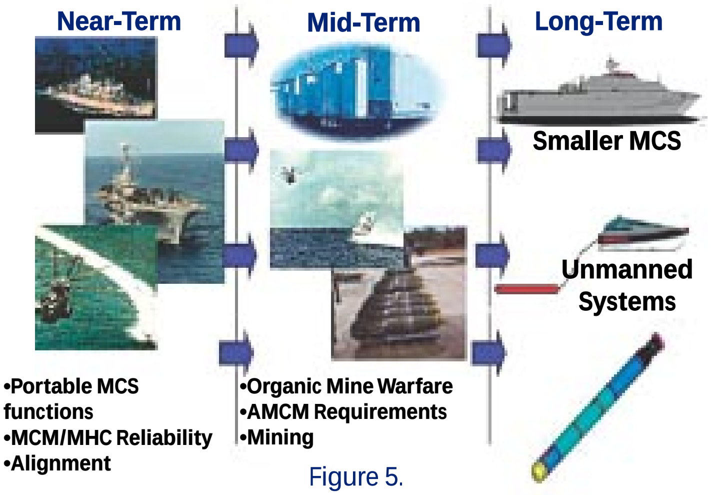
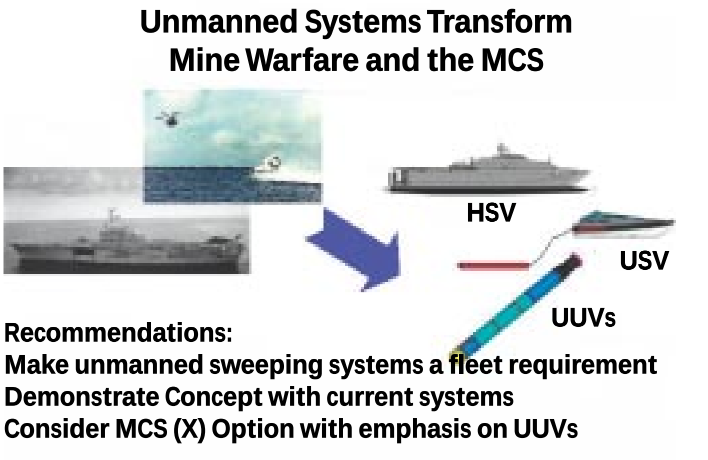


Figure 5.



Recommendations:
Make unmanned sweeping systems a fleet requirement
Demonstrate Concept with current systems
Consider MCS (X) Option with emphasis on UUVs

Figure 6.

mining requirements, which are currently barely met. Realignment also allows a forward-thinking vision of where we want to go —and encourages long-range planning for a phased program that addresses future needs.

Maturing Technologies and Future Mine Clearance Systems

The requirement for a large deck to support MH-53 helicopters for minesweeping is the largest cost driver in acquiring a dedicated MCS. Maturing technologies have the potential to dramatically alter our MIW capabilities in the next decade and transform the nature of future MCS. Programmed organic systems may greatly improve our mine hunting and neutralization capability. Employing AQS-20 sonar on an MH-60 helicopter, for instance, will be three times more effective than the current AQS-14 employed by the MH-53, even considering the substantial difference in range and endurance of the two helicopters. The AQS-20, coupled with the incorporation of the unmanned Remote Minehunting (RMS) and Long-term Mine Reconnaissance (LMRS) systems, offer a significant increase in mine hunting capabilities. These improvements mean that fewer airborne assets will be needed to accomplish the mine hunting mission both in the dedicated (theater) and organic (tactical) MIW forces.

Unfortunately, mine hunting is not effective in sixty-percent of the littoral regions near potential adversaries. Sea access to these areas requires minesweeping. Currently, the MH-53 helicopter wedded to the MK-106 sled, or the MH-60s with the developmental OASIS system, are needed to meet OPLAN minesweeping requirements. AMCM sweeping capabilities require a large-deck design for MCS. Many of the same technologies that are driving the improvements in mine hunting could be leveraged in an effort to develop an unmanned minesweeping system. A desire to keep the man out of the minefield makes unmanned minesweeping systems an attractive option.

Unmanned systems are the minesweepers and hunters of the future. Future MCS must incorporate emerging technologies. A focused technology effort is needed to incorporate unmanned systems into the MCS(X). Adequate study by appropriate technical authorities concluded that USVs have been shown to possess potential as effective low-observable MCM platforms, allowing mine hunting and minesweeping missions to be performed without a man onboard — eliminating the risk to personnel. It is time to press ahead with establishing fleet requirements for unmanned MCM systems that lead to programming decisions. Long-term recommendations include: Establish unmanned minesweeping systems as an emerging fleet requirement; Demonstrate the ability to launch MCM UUV/USV from HSV at the earliest opportunity; Leverage off the Spartan ACTD (Advanced Concept Technology Demonstration) if possible; Request that the MCS(X) working group explore options of using a combination of unmanned systems and a smaller helicopter detachment; and Establish a focused technology effort to incorporate unmanned minesweeping systems into future acquisition plans for a new MCS(X). A summary of near- to long-term strategies is shown in Figures 5 and 6.

Conclusion

The 2001 Quadrennial Defense Review (QDR) reaffirmed that "advanced mines could threaten the ability of U.S. Naval and Amphibious forces to operate in littoral waters" and are a likely method through which "future adversaries may have the means to render ineffective much of our current ability to project U.S. power overseas." The U.S. Navy's long history of difficulty in combating the mine threat culminated in the response to Iraqi mining efforts during the Gulf War. Despite a rudimentary and aged mining capability, Iraq severely damaged two ships and effectively deterred the United States from conducting planned amphibious operations into Kuwait.

Our ability to combat modern sea mines depends upon an amalgam of capabilities including MCS, AMCM squadrons, EOD units and Marine Mammal Systems. A central lesson of the Gulf War is that a dedicated MCS, capable of directing all aspects of the multifaceted MIW campaign plan, is needed to bring the various MCM capabilities together, providing unity of effort in defeating the mine threat. At the same time, it is clear that a heavy lift helicopter is essential to accomplish the airborne minesweeping mission. This will remain the case until maturing unmanned vehicle technologies replace the need for airborne minesweeping.

The future of MIW is clearly with unmanned systems; the Navy needs a focused effort to bring these technologies to maturity as they have the potential to transform the nature of MIW. Given the current state of technology, it is easy to envision a smaller, faster MCS that acts as a mother ship for a variety of unmanned systems that can rapidly move into theater and combat the mine threat without the presence of men in the minefield.

U.S. Navy and Air Force Hit Virtual Bull's Eye

USS Ticonderoga (CG 47)

The Atlantic Fleet cruiser, USS Ticonderoga (CG 47), homeported in Pascagoula, Miss., successfully demonstrated the Navy's newest weapons system trainer while underway Nov. 14, 2002, in the Gulf of Mexico. The ship's test comes on the heels of successful trials the day before by the U.S. Air Force's 46th Test Wing, based at Eglin Air Force Base in Florida, which dropped eighteen, 500-pound, non-exploding bombs from an A-10 aircraft. The Virtual At Sea Training system, or "VAST," allows warfighters to hone their live-fire combat skills while operating at sea.

Ticonderoga's crew successfully engaged a computer-simulated target with explosive and nonexplosive ordnance shot from the ship's MK 45, 5-inch/54-caliber gun. While the rounds hit nothing but water — the demonstration was right on target. Initial indications suggest that the VAST system was able to successfully "score" precisely where the ordnance rounds actually landed — a significant milestone in ensuring effective at sea combat training. VAST is actually comprised of a system by which the ship's crew or "spotter" sees a realistic presentation, for example, a landmass with the topography of a "real world" target, which corresponds to an area actually located over open ocean. During training exercises, the operator fires at the simulation of what they might expect to see in combat, while the ordnance actually lands within an array of buoys in the water. Exercise evaluators, monitoring the target practice on a computer screen, could be either onboard a ship or somewhere ashore.

Developed by the Office of Naval Research and tested by the U.S. Atlantic Fleet, this virtual reality training is one example of the Navy's efforts to keep its Sailors combat ready as weapons systems become increasingly advanced. In addition to programmable targets, VAST has another distinct advantage: It is portable. Ships can take the at-sea trainer — including the firing range — with them wherever they go. The portable "range" is made up of several buoys that form the target area. These buoys are actually placed into the water by the ship conducting the training, in this case by the crew of the Ticonderoga.

Once the ship positions at the proper distance from the buoy field, it engages and shoots at the virtual target. The actual ordnance then falls into this buoy field, which in turn triangulates the point of impact. The IMPASS (Integrated Maritime Acoustic Scoring And Simulator) buoy system is equipped with Global Positioning System (GPS) sensors that enable the accurate triangulation of the rounds. For these initial demonstration trials, one computer provides feedback on accuracy while a second computer is used within the ship to help with the training. In the future, a satellite uplink will potentially allow over-the-horizon operations.

As communications and satellite technology has advanced, the natural evolutionary development of weapons systems has advanced along with it. VAST is a logical next step in leveraging that technology to better train the crews of ships and aircraft that will ultimately deploy these weapons in battle.

The Air Force's 46th Test Wing used other existing systems to measure the effectiveness and accuracy of the VAST buoys during the exercise. The older systems have initially validated the emerging technology. "While the results are preliminary, the data looks promising. We're encouraged by the capability this system brings to our testing efforts and to our pilots. It's exciting to think that we'll be able to use this portable system and convert these wide open spaces to valuable testing areas," said Col. Dennis F. Sager, of Seattle, Wash., who is the commanding officer of the 46th Test Wing.

Another key advantage of VAST is its training versatility. Rather than continuously firing on a static, predictable bombing range, the presentation viewed by the warfighter can be manipulated to more closely resemble the type of terrain or target, which operators face in battle.

As the system develops, planners hope to incorporate models closely resembling geographic areas of interest. While Navy officials are initially encouraged by these preliminary results, more testing is planned. Provided the concept continues to prove successful over the next six-month evaluation period, the Navy plans to invest in as many as 10 additional systems by the end of FY03. There are currently three in the Navy's inventory being tested.

Finally, VAST offers savings in time, logistical considerations and money when compared to live-fire ranges. Navy ships, for example, must typically travel hundreds of miles to practice Naval Gun Fire Support using live-fire ranges. This system shaves days off transiting to and from these ranges. These savings can then allow more time for crews to focus on other critical prerequisites to deploying, including other necessary training, as well as equipment maintenance and repair.

While it offers distinct advantages over other training options, VAST is designed to supplement the available ranges used by the Navy, including ranges still required for coordinated battle group training. These types of innovations will continue to enhance the way Sailors train and prepare for combat.

"This is exciting new technology and we're encouraged with the results of joint Navy and Air Forces testing," said Adm. Robert J. Natter, Commander, U.S. Atlantic Fleet. "VAST also provides tremendous flexibility in that we can train effectively wherever there is sufficient ocean space.

VAST's initial testing results are positive and we see clear potential for joint Navy, Marine Corps and Air Force use of this system. Ultimately, VAST will help us further enhance the combat readiness of our ships and aircraft."

Interview with Diann L. McCoy

DISA Principal Director for Applications Engineering

Diann L. McCoy is the Principal Director for Applications Engineering. She is responsible for engineering information systems to provide command and control, and combat support capabilities to the nation's warfighter. She earned a Bachelor of Science degree in Mathematics from Wright State University in 1974, and a Masters of Science degree in Logistics Management from the Air Force Institute of Technology in 1978. She was selected for her current position in September 2000. Her awards include the Presidential Distinguished Executive Rank Award, the Technology Award for Government Leadership, the DoD Distinguished Civilian Service Award, the Meritorious Civilian Service Award, the Presidential Rank of Meritorious Executive Award, and the Certified Professional Logistician from the Society of Logistics Engineers.

CHIPS: When talking about Defense Transformation in terms of the asymmetric threat spectrum (denial of service, insertion of erroneous information that could cause loss of confidence in official networks/systems, seizure of a network/system for criminal/terrorist purposes, malicious code, etc.) How is DISA responding?

Ms. McCoy: An asymmetrical threat can apply to more than just network attacks; it may apply to more than just the DoD critical infrastructure; the nation as a whole may be impacted, i.e., power plants, critical utilities, etc. While we engage in this type of security, our DISA focus is on the networks for DoD. In a general sense, DISA has the GNOSC, the Global Network Operations and Security Center. It isn't under my direction but their responsibility is to look at the activities that are occurring on the network, assess them and respond appropriately. We do this in conjunction with the JTF-CNO, Joint Task Force-Computer Network Operations, U.S. Strategic Command. The JTF-CNO is led by Maj. Gen. James D. Bryan, U.S. Army, who is dual-hatted as the Vice Director of DISA and Commander of JTF-CNO. In Applications Engineering, we provide many of the capabilities and applications used to analyze the information, to identify trends or activities that could lead to potential denial of service on the network. We are engaged in developing tools and capabilities that will allow us to understand what activity may be occurring and producing methods that will allow us to respond. Everything DISA designs, builds and operates, incorporates required measures to protect against information warfare attacks.

CHIPS: I've read comments from top DoD and DON leadership that there is concern from an information warfare perspective that there is potential for a terrorist/criminal threat that could bring down the whole DoD architecture. With all of DoD and federal agencies on high alert, do you think a threat of that nature is likely to occur — the worst-case scenario?

Ms. McCoy: No, I don't believe so. One of the approaches we use to protect our environment is Defense in Depth, which means you have multiple layers of defense and diverse routing capability so if you lost an application or a communications capability, you still have access to other available capabilities — voice, data, Defense Red Switch Network, VTC, etc. The diversity and robustness in each of these networks or systems comprise the larger Defense Information Systems Network (DISN). You might have an isolated incident, but in terms of vulnerability of the entire system, I think that is highly unlikely. One of the reasons why we have the DISN is for its positive control and accountability — that's why DISA manages the DISN.

CHIPS: Do you mean if everything else fails we can always rely on the DISN?

Ms. McCoy: The DISN has successfully functioned through several major events that degraded Internet performance. More specifically, what I'm saying is because we have diverse routing and multiple paths, and the means to move information, either voice or data, we have redundancy so we don't have to depend on a single way to communicate. Also the physical and electronic security is more robust than a typical network. In Applications Engineering, we provide some applications that allow us to monitor and analyze what is happening over the network. The Network Services organization actually designs and develops these networks with layers of Defense in Depth protection built in.

CHIPS: Secretary Rumsfeld has stated numerous times that information technology is the enabler behind Defense transformation, but isn't this a natural progression for military operations to rely on IT due to the technology advancements of the last 10 years, especially?

Ms. McCoy: The Secretary is looking not just at the technology per se, but the way it is employed in a joint environment to provide a quantum increase in capability to meet the operational goals of the transformation. What we do is leverage that technology to make it work in a warfighting environment. Given the IT capabilities we have today — we can do things differently; and our methods of operations are tied to the type of IT available. For example, we manage the Global Command and Control System, GCCS, which provides the common operational picture of the battlespace. It gives the warfighter a situational awareness of what is happening and through technology we get better information flow and, more timely information, which gives the decision makers a better opportunity to respond to whatever is happening. Technology enables us to get closer in time to what is happening in the battlespace, as well as having a greater awareness of what is in the battlespace, a greater awareness of what capabilities we might have to bring into that particular environment — and what the status is of those assets.

CHIPS: Is there any one technology or system that is key to linking command and control for joint fighting capability?

Ms. McCoy: I think one of the cornerstone joint applications is the Global Command and Control System, and we are incorporating multiple technologies and applications in GCCS. The most important feature of these joint capabilities is they have to be secure and interoperable. On the application side, they have to be able to share data in a certain way so that data has the same meaning, and in a secure way so that it cannot be compromised. This is central to Secretary Rumsfeld's joint command and control initiative — the key being joint and interoperable capability. This is what DISA is in the business of providing every day.

CHIPS: One of the things Dr. Myers (Principal Director, Deputy Chief Information Officer, Department of Defense, CHIPS Summer 2002, "Power to the Edge, the Transformation of the Global Information Grid," www.chips.navy.mil/archives/02_Summer/authors/index2_files/power_to_the_edge.htm) stated that is so important to Combatant Commanders is their confidence in the authenticity and timeliness of data.

Ms. McCoy: What you are really talking about is the issue of latency and that is very important. One of the things we are focusing on with the GCCS is providing near real-time data, so decision-makers have the most current information and don't have to gather and synthesize a lot of information. This lets warfighters shorten their decision-making cycle. Some of the tools and capabilities that we have today allow us to overlay information from various sources and fuse it together so the user has the most currently available information to act upon — that is very important. The other thing you asked about is the issue of data authenticity. We view both authenticity and data integrity as essential. We worry about these in every system we build and are also working on the DoD PKI as a key enabler to improve authentication and integrity in all DoD systems.

CHIPS: Is DISA involved in the Homeland Defense Plan?

Ms. McCoy: DISA as an organization is involved in Homeland Defense from several different aspects. Most importantly we support the communications needs of other DoD organizations with a direct Homeland Defense role to include nation-to-nation leadership communications. We also directly provide and support Presidential communications. We do other things in all the different disciplines to include support of whatever type transport mechanisms are required. In particular, in my area of Applications Engineering we are working on an ACTD or Advanced Concept Technology Demonstration, to work with JFCOM initially and then with NORTHCOM — whomever has the Homeland Defense mission. We would take this Homeland Security ACTD and develop a common operational picture and situational awareness for that Combatant Commander. The point is to take some of the things that we have learned under command and control and, see how they can be used to support DoD's role in Homeland Defense.

CHIPS: I spoke with a Congressional Liaison, who has worked on security matters for the House Armed Forces Committee and she said that she is very impressed with the DoD response to Homeland Defense and the Sept. 11 terrorist attacks. She indicated that federal agencies such as the FBI, FEMA, CIA, etc., could use the DoD model and that the national Homeland Defense strategy could also follow the DoD model. Is this feasible?

Ms. McCoy: In prior jobs that I have had I was involved in the larger federal community. I think where possible DoD is sharing its lessons learned from the kind of quick deployments we have to do. I found that in forums like the National Communications System other folks are willing to listen to our lessons learned. Through the Homeland Defense ACTD we have involvement from several other agencies. As you know there are many political issues in regard to Homeland Defense. In DoD we offer our experience and we found that we may have some things that work, but also we have things that may be different because the whole issue of Homeland Defense is a little bit different. There are different rules of engagement as to who has responsibility. So we can't say these other organizations should just pick up everything we are doing and move with it, but we do offer our experience and capabilities for them to look at — perhaps as a way for them to move forward or begin.

CHIPS: What role is DISA playing in the DoD transformation?

Ms. McCoy: In terms of DISA as an organization, we are playing in multiple forums. One of the biggest efforts we have is the GIG bandwidth expansion (GIG-BE). This will provide a robust network capability throughout the DoD environment. On the applications side, we are looking at the enablers of the "Power to the Edge" vision, the enablers to the transformation. We are involved directly in what we call the "right data strategy," which means that we've changed the way we look at data and the way we provide data. We have begun to employ tools with XML to make it easy to share data across domains and we have designed and built a DoD XML registry to ensure that everyone in DoD who is using XML has access to existing naming standards (metadata tags) and can register new ones. We are also changing or updating our tools and capabilities so they are Web-enabled, making it easier for our customers to access applications and tools that can be used in different environments. A good example is the joint collaboration capability, such as the Defense Collaboration Tool Suite (DCTS) which we are providing to a wide range of users today worldwide, including Combatant Commanders.

We are looking at methodologies and approaches for getting information out and having it available through a process we call content staging. In order to make the vision happen we have to figure out how to manage services in this net-centric environment. We are looking at what types of services are needed and how they should be managed. We call this Net-Centric Enterprise Services (NCES) — critical to the sustainment and technological evolution of the GIG. There are various places where these components are covered in detail as well as how they interact with each other. As an early pilot of these components, DISA will integrate Web-based intelligence services with emerging C3 Enterprise Service to create a baseline C3I "electronic marketplace" on the SIPRNet that will enable mission planners to dynamically collaborate with the intelligence and combat support communities. An example of a managed service would be a Global Directory Service. So we have ongoing efforts to help with the transformational vision. All of these are geared to ensuring that we can provide interoperable capability down to the Joint Task Force Commander level and below — the guy on the battlefield — not just the people at headquarters.

CHIPS: What services would be in Global Directory Services?

Ms. McCoy: A Global Directory Service could contain information as simple as a person's name and e-mail address. As DoD information processing becomes ever more distributed, it could have information in terms of what types of capabilities, data services or databases are available or where they are staged. Directory Services is one of those capabilities that will increasingly become highly protected and more secure because it will contain information about what is available and perhaps even where it is located.

CHIPS: When you talked about a user getting information and content staging, are you talking about the user's ability to pull data rather than have it pushed at them?

Ms. McCoy: We are looking at the ability to do both because what we find is that in certain cases the user does not have the opportunity to go out and surf. The user needs to have certain pieces of information, which they can predefine, sent to them automatically. But we would have the capability to do either — a smart push or smart pull — or the user could surf the net.

CHIPS: How do Web-enabling databases, information and processes, and process improvement for business and support functions help support the warfighter?

Ms. McCoy: There are a multitude of things that Web services will allow us to do. First it is easier for the user to get to the information. It provides the information to a broader set of users, who are able to get the information whenever they need it and in a faster method of delivery. By using Web technology you have the ability to do more of a real-time collaboration because everyone can pull up tailored information. You can update the information more frequently. It also allows us to take advantage of wireless capability, which is the wave of the future. Another thing that we tend to forget about it is that there can be a very good return on investment. When you go to the Web environment you can carry more of these services in the NCES. So you can reduce the number of servers, which reduces the number of system administrators that may be required to manage those types of services. You also have the ability to do more configuration management to ensure that the same type of capability is being used across the infrastructure. This is key to net-centric warfare.

CHIPS: Do you have security concerns with using wireless technology in the Defense environment where security is our number one priority?

Ms. McCoy: You said it exactly; we do have concerns in how we employ wireless. We are looking at the security and coming up with approaches that will allow us to use wireless in a secure manner. We have turned these approaches into standards for deploying wireless as securely as currently possible. We are also working with industry to improve the security in commercial wireless products and they are responding to that.

CHIPS: In a recent interview I did with Grady Booch, chief scientist for Rational, (CHIPS Magazine Fall 2002; www.chips.navy.mil/archives/02_fall/index2_files/interview_with_grady_booch.htm) he commented that DoD does not fully exercise the influence they have in the marketplace in demanding secure technology products. He said that DoD shouldn't have to spend additional money to build security into commercial products, rather industry should ensure security is built in at the front end.

Ms. McCoy: When we moved to the Internet and the network environment the rules of security became different than when we were operating on a disconnected mainframe. I'm not sure anyone had a crystal ball on how security should be handled in a networked environment. This has really been a learning experience for industry as to what is needed in terms of security. I think we are demanding more of industry in terms of security. We are beginning to see the big companies, such as Microsoft, incorporate security as one of the key features of their products. We also have the NIAP (National Information Assurance Partnership) process that requires commercial products used in a certain way to be evaluated and certified. So I think we are getting there and vendors are responding.

CHIPS: I was just reading about the DoD debate over open-source software. Many in DoD believe open-source is the wave of the future for many reasons. One of the chief reasons is that the code is visible so it is easier to detect vulnerabilities.

Ms. McCoy: I think in some cases we really need to know the source code because it is the only way to know what is inside that code. There are some applications where that may become very important because of the way those applications are utilized and how they actually fit into the architecture.

CHIPS: There seem to be so many initiatives across Defense, with the Services working toward interoperability for command and control systems. Is there a plan or method of determining which are the most important to integrate first?

Ms. McCoy: That is exactly what the Joint Staff, in conjunction with the OSD principals, are working right now. They have reviewed the interoperability issues and analyzed which ones should be worked first. They are working a plan as to how we are going to get to interoperability faster. We work closely with JFCOM through experimentation and events like Millennium Challenge 2002 to demonstrate interoperability. We are also looking at a process that allows us to demonstrate interoperability through the development phase before we get to the operations phase so that interoperability is built in and then maintained throughout the life cycle. In terms of what capabilities or interoperability problems are worked first, DISA responds to prioritization decisions made by the designated approval authority.

In all these endeavors, we are working hard to provide capabilities that our customers want and use, and we ensure that we always keep in mind the users' experience so we can make our products and services even better.

CHIPS: Are there three top systems or programs that Defense is focusing on first for interoperability?

Ms. McCoy: I believe from a Web capability standpoint, we are looking at the GCCS family of systems — our GCCS program is part of that. They are focusing on what we call the C2 transformation, which looks at getting command and control information down to the JTF Commander and below. Another high priority is to ensure that we have the bandwidth capability down to the tactical level — so bandwidth expansion is high on the list of priorities.

CHIPS: In Dr. Myers' article she talked about the locations (CONUS/OCONUS) for the bandwidth expansion. Will the Fleet be able to share in this bandwidth expansion?

Ms. McCoy: This technology will support all warfighting. What we are talking about is ensuring that, as we transform and move to a net-centric environment, we have sufficient means and bandwidth to move the information wherever it's needed. So it would be applicable to all. What we have to work is how we get that information to the tactical level, to a warfighter on a ship or even one who could potentially be on horseback, so to speak.

CHIPS: Let's talk about the work of Applications Engineering ...

Ms. McCoy: The mission of the Applications Engineering Directorate is to provide responsive, secure and interoperable C2 and combat support capability for decision superiority to the President and Secretary of Defense, Combatant Commanders, Joint/Combined task forces, Services, Department of Defense and non-DoD agencies.

We provide a wide range of products, services and expertise. I already mentioned the Global Command and Control System which is DoD's Joint and interoperable C2 system, and the Defense Collaboration Tool Suite. These are providing situational awareness, readiness, planning, deployment support, collaboration and other capabilities for Combatant Commanders, JTF Commanders and below — today. The Global Combat Support System's (GCSS) Combatant Commander JTF (CC-JTF) capability is using portal technology with links to Service and Agency logistics and sustainment systems, to provide DoD users access to shared data, and applications, regardless of their location.

Over the next few years we are transforming the successful Common Operating Environment (COE) to fit OSD's Net-Centric Enterprise Services (NCES) concept. COE is currently used or planned to be used for/in 125 C2 systems and in support of GCCS, at 650 locations worldwide on 10,000+ joint and coalition workstations. The net-centric capabilities we provide will support the Power to the Edge vision of having tailored, fused information and tools available on the net, effectively supporting users wherever they are and with the means available to them.

In the Information Assurance area we are supporting "Defense-in-Depth" with expertise, products and services such as PKI, network and communications security, plus guards for cross-domain (e.g., Unclassified to Secret) and coalition information exchange. In addition to the Homeland Defense ACTD, we are also involved in Multiple Battlespace Awareness, Active Network Intrusion Defense, Coalition Theater Logistics, and C4I for the Coalition Warrior ACTDs, just to name a few. These are providing adaptive decision support, planning, and execution and collaboration tools through experimentation, demonstrations and spiral development. Our partnering with the Combatant Commanders and the operational community is very important. We are also partnered with the Defense Logistics Agency to provide a variety of eBusiness applications and services for paperless contracting, secure business transactions, wide area work flow, and electronic document access. In all these endeavors, we are working hard to provide capabilities that our customers want and use, and we ensure that we always keep in mind the users' experience so we can make our products and services even better.

Revolution Comes to the Teddy Roosevelt Battle Group

By JO2 Jd Walter, NPDC, Public Affairs Office

The USS Theodore Roosevelt (CVN 71) Battle Group, including the USS Saipan (LHA 2) Amphibious Ready Group, is about to get underway without ever leaving port. Their new mission is to test and evaluate Revolution in Training initiatives designed to enhance the Navy's mission readiness by providing Sailors with new tools and opportunities to develop both professionally and personally. Working with Task Force for Excellence through Commitment to Education and Learning (EXCEL), the battle group will implement and test the Sailor Continuum in an operational environment, as well as test incentives designed to increase performance and productivity. Additionally, the battle group will demonstrate the utility of a new learning management system, Navy Knowledge Online (NKO) that will track each Sailor's accomplishments.

"The innovations being touted by Task Force EXCEL are being driven by the Fleet and are for the Sailors. The acid test has to be at the waterfront. The Navy is bringing the Revolution in Training to Sailors, and it is happening now," said Director of Surface Warfare Rear Adm. Harry Ulrich. "This is the best opportunity to put these ideas and programs to the test." A working group consisting of executive officers (XO), command master chiefs (CMC) and other representatives from the Roosevelt battle group, Saipan ready group, Destroyer Squadron Two, and elements of Carrier Air Wing Eight (CVM 8) recently met in Norfolk, Va., to review and discuss the testing proposal.

"The testing proposals have generated a lot of excitement and enthusiasm," said Capt. Jamie Barnett, project leader for the beta test. "Private industry typically provides incentives for behaviors that enhance performance. That is what we will test within the battle group. We just need to work with the group to precisely define the tasks and how we will measure the outcomes." The goal of this effort is directed at increasing job efficiency and productivity — more time for ship's work by developing each Sailor professionally and personally.

At sea aboard USS Theodore Roosevelt (CVN 71) Oct. 28, 2002, MM3 Ryan Karlin checks the results of the September 2002 advancement exam for division personnel. U.S. Navy photo by PH3 Phillip Nickerson, Jr.

JITC Provides Essential Services to the Fleet

Joint Test Command's relationship with the United States Navy spans nearly three decades

By Chris Watson

For many years, the Joint Interoperability Test Command (JITC) has directly contributed to the success of U.S. Navy fleet operations through the execution of complex test events and on-demand warfighter support efforts. From a technical standpoint, the Navy and other military services view JITC as the preeminent evaluator of systems interoperability. JITC is one of the key organizational elements of the Defense Information Systems Agency (DISA) Interoperability (IN) Directorate and serves as DISA's developmental and operational test organization. As designated by the Joint Chiefs of Staff, JITC is also the authority that certifies that Department of Defense (DoD) Information Technology (IT) and National Security Systems (NSS) meet interoperability requirements for joint military operations.

JITC facilities are strategically located at Fort Huachuca, Ariz., and Indian Head, Md. The diverse capabilities of each location allow the Services to have access to a dynamic environment for laboratory tests and on-site field evaluations. Navy organizations from coast to coast have benefited from JITC's robust test environment and continue to leverage off of their vast resources and technical expertise.

To understand JITC's current relationship with the Navy, one must revisit the history of the organization and recognize how it has evolved over the past three decades. JITC's relationship with the Navy spans back to the 1970s when the Joint Tactical Command, Control, and Communications Agency (JTC3A) Joint Interoperability Test Facility (JITF) established a partnership with the Navy Center for Tactical Systems Interoperability (NCTSI) for the interoperability testing of Tactical Digital Information Links (TADIL). In 1988, the Defense Communications Agency (DCA) absorbed the Tri-Service Tactical Communications (TRI-TAC) Joint Test Element (JTE) and the JTC3A JITF. DCA consolidated these organizations in 1989 to form the "JITC" in Fort Huachuca, Ariz. JITC's primary mission was to provide interoperability compliance testing and certification. As the designated lead for DoD Command, Control, Communications and Intelligence (C3I) support, DCA tasked JITC to perform interoperability tests of various systems including High Frequency (HF) radio systems, Military Satellite Communications (MILSATCOM) systems, and the Worldwide Military Command and Control System (WWMCCS). On June 25, 1991, DCA was renamed "DISA" to reflect its expanded role in managing the Defense Information Infrastructure (DII), now known as the Global Information Grid (GIG). As a result, JITC's responsibilities for ensuring joint interoperability of all military systems began to increase as well, causing the need for growth and expansion within the organization.

In 1993, the Naval Computer and Telecommunications Command (NCTC) proposed an initiative to transfer the functions and resources of the Naval Telecommunications Systems Integration Center (NAVTELSYSIC) to JITC. Since 1976, the NAVTELSYSIC test facility had operated in Cheltenham, Md., and was the primary site for the Quality Assurance (QA) and Functional Certification testing of all Navy-messaging systems. DISA and the Chief of Naval Operations (CNO) agreed that the transfer of NAVTELSYSIC resources to JITC would improve both agencies' ability to enhance operational fleet support. Thus, JITC's East Coast arm, known as the Washington Operations Division, was established. In 1998, the Washington Operations Division moved its facility to the Naval Surface Warfare Center (NWSC) at Indian Head, Md., where they currently reside. Today, JITC's East and West Coast divisions work closely to provide valuable test and exercise support to the Navy and the other Services. The JITC organization is currently divided into eight divisions and a liaison office, each having unique responsibilities, these are shown in the text box on the next page.

JITC's superior test methodologies and extensive expertise are shown by the many success stories reported by various Navy organizations. For example, the JITC JDEP (Joint Distributed Engineering Plant) Division's TADIL Branch at Fort Huachuca continues to work closely with NCTSI detachments in Dahlgren, Va.; Dam Neck, Va.; and San Diego, Calif., for TADIL interoperability assessments and certification. JITC uses the Joint Interoperability Evaluation System (JIES) for TADIL-A/B/J testing and the Joint Operational C4I Assessment Tool (JOCAT) for operational assessment of tactical data links. With JITC's assistance, the Navy has been able to identify and correct deficiencies pertaining to Link 11 (TADIL-A) and Link 16 (TADIL-J) data exchange with AEGIS destroyers and E-2C aircraft. The Navy has also improved interoperability between their embarked forces and key allies, through TADIL tests conducted by JITC.

The JITC Washington Operations Division also continues to be the operational tester of all Navy legacy and transitional messaging systems, both strategic and tactical. JITC has been directly involved in the testing, training, and implementation of Navy shore-based systems such as GateGuard, Personal Computer Message Terminal (PCMT), Manual Relay Center Modernization Program (MARCEMP), Multi-Level Mail Server (MMS),

Above: JITC Headquarters, Fort Huachuca, Ariz. Right: JITC Washington Operations Division, Indian Head, Md.

Nova, and the Message Conversion System (MCS). JITC's consistent performance was demonstrated during the recent implementation of the Fleet Message Exchange/Directory Update & Service Center (FMX/DUSC), the replacement for the Naval Communications Processing and Routing System (NAVCOMPARS). JITC assisted the Space and Naval Warfare Systems Command (SPAWAR) in testing, troubleshooting, and bringing online this very intricate configuration at the three Naval Computer and Telecommunications Area Master Station (NCTAMS) locations under difficult conditions. Navy fleet systems such as the Common User Digital Information Exchange System (CUDIXS), Fleet SIPRNET Messaging (FSM) system, the Naval Modular Automated Communication Systems (NAVMACS - V2, V3, V5A and Version II), the Shipboard AN/SYQ-26 (V) Single Messaging Solution (SMS), and the Submarine AN/SYQ-28 (V) SMS have also gone through rigorous test evolutions at the Indian Head facility.

In the summer of 2002, Rear Adm. Kenneth D. Slaght, Commander SPAWAR, recognized the JITC Washington Operations Division for their outstanding contributions to fleet operations. Several JITC representatives received the SPAWAR "Lightning Bolt Award of Excellence" for their support of various mission-critical systems.

JITC divisions at Indian Head and Fort Huachuca execute the developmental and operational testing of the Defense Message System (DMS) on behalf of the DISA DMS Program Management Office (PMO). The Navy is an important stakeholder in the overall DMS program and JITC works closely with selected Navy DMS operational sites for the successful collection of data during DMS OT events, leading to subsequent DMS fielding decisions. JITC is also responsible for the developmental testing of Navy-developed non-core DMS products such as the Defense Message Dissemination System (DMDS). The SPAWAR developer and PM rely heavily on JITC's test processes and results, which ensure that fully operational DMDS software iterations are distributed to the field. Additionally, JITC validates unique Navy DMS strategic and tactical configurations and provides on-site training to Navy DMS Service Provider (DSP) sites.

In the fall of 2002, the Navy Operational Test and Evaluation Force (OPTEVFOR) will

The JITC Organization

Plans, Policies and Warfighter Support Division (PPWFS) directly supports the Combatant Commanders, Services and Agencies by providing interoperability, operational and technical support during exercises, deployments and contingencies. Lead division for combined warfighting issues. Develops and executes the command's strategic plan and establishes policies for testing and interoperability certification.

Operational Test and Evaluation Division (OT&ED) provides independent operational test and evaluation (OT&E) and assessments of DISA programs to ensure that only operationally effective and suitable NSS/ITS systems are delivered to the warfighter. DISA programs include Global Command and Control System (GCCS), Defense Information System Network (DISN) and Defense Message System (DMS). Also serves as the Operational Test Agent (OTA) for the Defense Logistics Agency (DLA), Defense Finance and Accounting Service (DFAS) and High Performance Computing Modernization Program (HPCMP), among others.

JITC Washington Operations Division (JWOD) provides NSS/ITS interoperability test, evaluation and certification support with a specific focus on Department of Defense Intelligence Information Systems (DODIIS), Navy Programs, DMS, DoD Health Affairs, Logistics, Information Assurance and the Joint Warfighter Interoperability Demonstration (JWID).

Combat Support and Information Systems Division (CSISD) provides developmental and interoperability test, evaluation and certification support with a specific focus on combat support, combat service support and information systems. Conducts standards validation and conformance testing of IT systems.

Networks, Transmission and Intelligence Division (NTID) provides NSS/ITS (National Security Systems/Information Technology Systems) interoperability test, evaluation and certification support to DoD and other federal Agencies. Programs/functional areas supported include the Global Information Grid, information security, networks, transmission systems, switches, radios of all types, wireless systems; and intelligence, surveillance and reconnaissance systems. Conducts and participates in joint and combined exercises such as the DoD Interoperability Communications Exercise (DICE), the Joint User Interoperability Communications Exercise (JUICE), Combined Endeavor and CID (Coalition Interoperability Demonstration) Borealis.

Joint Distributed Engineering Plant Division (JDEPD) leads DoD planning, coordination and engineering teams developing the JDEP. Provides management and oversight of investment, coordination and general support functions. Oversees JDEP software/hardware development and maintenance. Provides JDEP capability repository, network/simulation engineering, configuration management and infrastructure scheduling. Tests, evaluates and certifies command and control, and air and missile defense systems to interoperate with other Joint systems in accordance with tactical data link standards.

Automated Systems and Test Support Division (AS&TSD) provides system engineering support in the design, development, installation, modernization and maintenance of JITC automated test and test support systems, traffic and message loading devices, and strategic and tactical equipment. Manages, operates and maintains JITC test beds, laboratories, test systems, COMSEC account and related equipment in support of NSS/ITS testing. Implements and manages network management programs for JITC. Provides logistics support for JITC.

Resource Management Division prepares and implements business, contract, and personnel policies/guidelines. Manages the command's fiscal and human resource programs.

NCR Liaison Office provides support to JITC customers based in the National Capital Region (NCR). Liaison to DISA PMs and Directorates, Joint Staff, OSD-level boards and committees, Major Range & Test Facility Base (MRTFB) activities, T&E policy working groups, tiger teams, allied interoperability groups, Combatant Command/Service/Agency activities. Represents DISA's Central Test & Evaluation Investment Program (CTEIP) projects to OSD.

JITC Advanced Technology Testbed (ATT) incorporates state-of-the-art technologies such as Video Stream and Voice-over-IP.

conduct an Operational Assessment (OA) of the Navy Marine Corps Intranet (NMCI). In conjunction with this OA, the JITC Combat Services and Information Systems Division will coordinate with OPTEVFOR to assess the joint information flow of selected Critical Joint Applications (CJA) to determine NMCI interoperability. The assessment will take place in an operational NMCI environment using JITC-developed test procedures. JITC will conduct its assessment at: Naval Air Systems Command, NAS Patuxent River, Md.; NAS Lemoore, Calif.; and Naval Air Facility Washington, Andrews Air Force Base, Md. When the assessment is completed, JITC will issue a "Status of Interoperability" letter, which will help the Navy thoroughly review their target NMCI implementation strategy and develop lessons learned.

JITC's Information Assurance (IA) team conducts code vulnerability assessments, penetration tests, commercial product testing, and security tool assessments. Testers also provide assistance during the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), and the National Information Assurance Certification and Accreditation Process (NIACAP). The IA laboratory at the Indian Head facility employs four individual enclaves that are networked over a three-tier architecture. The IA lab can replicate almost any Navy operational environment, thus providing added realism when testing a system's reaction to an unauthorized intrusion. IA assessments of the Common Access Card (CAC) have been conducted relevant to the Navy's implementation of Public Key Infrastructure (PKI) tokens within the NMCI architecture.

The JITC NTID Surveillance & Reconnaissance Branch has begun to work closely with the Navy regarding developmental testing of the Navy's Vertical Takeoff and Landing Tactical Unmanned Aerial Vehicle (VTUAV). JITC became involved with this program early in the acquisition process, which will allow the Navy to mitigate much of the interoperability risks prior to future operational test events. JITC will soon work with the VTUAV Program Office to conduct interoperability assessments of the VTUAV at selected sites such as the Naval Weapons Center Detachment, China Lake, Calif. While conducting these assessments, JITC will determine the VTUAV's ability to interoperate with numerous strategic and tactical C4I systems.

To fulfill its interoperability mission, JITC has established laboratories and network connectivity to key DoD sites and employs state-of-the art technologies to replicate operational nodes. JITC's Risk Mitigation Network employs central connectivity from Fort Huachuca to Navy and other DoD sites, and provides the capability to test systems in a distributed manner with minimal impact to operational networks. The Advanced Technology Testbed (ATT), located at Indian Head, enhances JITC's current testing infrastructure. The ATT has positioned itself at the forefront of communication technology and keeps up with the latest communication innovations so JITC can mitigate the risk of introducing new technology within the DISN. The ATT includes modern communication technologies such as Gigabit Ethernet, Packet Over SONET (POS), Multi-Protocol Label Switching (MPLS), IP Telephony, Dense Wavelength Division Multiplexing and wireless LAN technology.

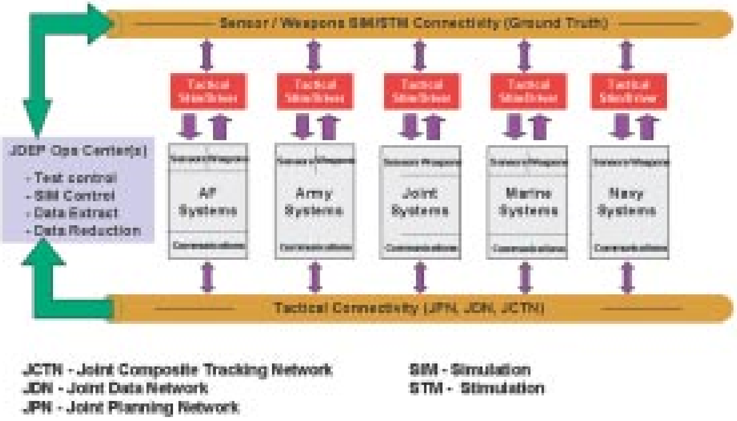
JITC observed a transformation in the IT industry that warrants changes to test methods. Because of spiral development, the timeline for bringing a product to the field has been significantly reduced, which requires the tester to become involved early in the process. This demands a testing environment that can closely emulate a production setting with development features. For these reasons, the ATT employs a multi-vendor/multi-technology layout. Connectivity to the ATT will allow the Navy to take advantage of the lab's many unique test capabilities.

In the near future, the Navy and other services will also establish connectivity via the Joint Distributed Engineering Plant (JDEP) to conduct distributed test events. To a certain extent, the JDEP program (a diagram of the JDEP architecture is shown on the next page) was initiated based on the success of the Navy's DEP. In accordance with Defense Planning Guidance, the JDEP program was established as a DoD-wide effort to link DoD and joint combat system engineering and test sites. It is designed to improve the interoperability of systems through rigorous testing and evaluation in a replicated battlefield environment. The DISA IN Directorate serves as the manager of the JDEP and oversees the execution of the program. The JITC JDEP Division serves as the JDEP Coordinator and is responsible for identifying candidate sites and federations, cataloging system and network capabilities, and defining the overall technical architecture. JDEP baseline sites include Navy activities such as NAVAIR Patuxent River, Md.; Naval Surface Warfare Center (NSWC) Dam Neck, Va.; SPAWARSYSCEN Charleston, S.C.; and SPAWARSYSCEN San Diego, Calif. JITC will work closely with these activities, as well as other DoD sites, during collaborative engineering team meetings and JDEP test events. JDEP strategies coincide with Joint Vision 2010 and 2020 initiatives. JITC is poised to support the collaborative test opportunities and interoperable environment that JDEP offers to joint warfighters.

JITC is well known for the exercise and operational contingency support they provide to Combatant Commanders worldwide. JITC supports seven to nine exercises each year in support of joint and combined interoperability initiatives aug-

JITC testers perform analysis of the Submarine AN/SYQ-28(V) Single Messaging Solution (SMS) and other tactical systems.

JDEP Joint Architecture



menting combatant commander staffs with on-site technical support. JITC has supported exercises such as Combined Endeavor, Unified Endeavor, Foal Eagle and Roving Sands, as well as operational contingencies such as Desert Storm and Operation Enduring Freedom.

The JITC NTID Networks and Integration Branch serves as the coordinator and test lead for the DICE on behalf of the Joint Forces Command (JFCOM). DICE represents a coast-to-coast joint service interoperability test that focuses on warfighting requirements. The DICE network is designed to emulate a Joint Task Force (JTF) architecture. DICE distributed tests are accomplished in phases using JITC laboratory resources, assets from active units, and other DoD test facilities. The overall purpose of DICE is to assess new/improved DoD tactical and strategic switching systems, transmission systems and terminal devices, and certify these systems for joint interoperability. Naval ships such as the USS Mount Whitney, USS George Washington and USS Nassau have been active participants in past DICE events.

The NTID Networks & Integration Branch also supports JUICE on behalf of JFCOM. JUICE allows the Services to evaluate deployable communication configurations and their interfaces to the GIG. Besides providing great training opportunities, this event affords the opportunity for the Navy and other Services to refine operational configurations, monitor the applicability of tool sets, and evaluate reporting procedures. JITC also provides 24-hour hot line support to Combatant Commanders and DoD personnel. For instance, if a Sailor needs technical assistance to restore a circuit, he/she may call **1-800-LET-JITC** to receive troubleshooting information. If the JITC technical expert cannot provide the necessary assistance over the phone, it is likely that he/she will be dispatched to the Sailor's location to resolve the problem.

JITC developed the Joint Interoperability Tool (JIT) to further assist the warfighter. The JIT is a Web-based repository of information that is available via controlled access over the NIPRNET or directly over the SIPRNET. The JIT has a powerful search engine that permits users to access test reports, interoperability certification letters, reference manuals and valuable lessons learned. The JIT is constantly updated with new information, allowing the Services to obtain vital information that is always current.

To ensure that warfighter objectives are satisfied, JITC must view its interaction with DoD services and agencies as a partnership. JITC works in tandem with some organizations by way of unspoken agreements or established written agreements. JITC recognizes the need to initiate "formal" partnerships with key Navy organizations in order to achieve joint interoperability goals.

In May 2002, JITC Commander, Col. Terry Pricer, USAF, signed a Memorandum of Agreement (MOA) with several organizations, making JITC the newest member of the Chesapeake Regional Ranges Cooperative (CRRC). As a member of the CRRC, JITC will assist the Navy and the other Services in providing a streamlined T&E process for program managers and the acquisition community in the Chesapeake region and beyond. JITC will soon collaborate with CRRC partners (NAVAIR Atlantic Test Ranges (ATR), NAVSEA Combat Direction Systems Activity (CDSA), CINCLANTFLT, Aberdeen Test Center (ATC) and Fort A.P. Hill) for cooperative testing, assistance during Joint Task Force Exercises (JTFEX), and support of programs such as the Tactical Tomahawk. This partnership will demonstrate how collaborative testing and resource sharing will enhance military readiness, reduce costs, and support the RDT&E and interoperability requirements of DoD acquisition managers.

In 2001, JITC and the SPAWAR CINC Interoperability Program Office (CIPO) began pursuing activities that would lead to closer relations with other DoD agencies responsible for joint interoperability. Both organizations determined that significant benefits could be gained by having a SPAWAR liaison on-site at JITC headquarters. In order to accomplish this, a JITC/SPAWAR CIPO Memorandum of Agreement (MOA) was staffed and signed in June 2002. It defined organizational responsibilities and established a CIPO liaison at the Fort Huachuca facility. This MOA strengthens the relationship between JITC and the Navy and encourages the sharing of information and resources. It is also seen as a way to enhance exercise coordination, offer SPAWAR direct access to the appropriate offices at JITC, provide an interface between the JITC testing community and SPAWAR Code 053, and enhance systems design prior to programmatic testing and implementation.

JITC Commander Col. Terry Pricer, USAF, (right) Capt. John Melear, USN (center) sign the JITC/SPAWAR CIPO MOA, while JITC Deputy Commander, Mr. Denis Beaugureau looks on.

Through a follow-on Memorandum of Understanding (MOU) signed in September 2002, JITC and SPAWAR officially established a partnership for facilitating DT, OT, and joint interoperability certification of the Navy's IT and NSS infrastructure. Ultimately, JITC will improve its fleet support posture and further cultivate its relationship with the Navy, as the Navy's acquisition, engineering, and operational communities fully understand and institute joint interoperability test processes, procedures and doctrine.

Chris Watson is an Information Technology Systems Project Officer at the Joint Interoperability Test Command.

East Timor: A Case Study in C4I Innovation

By Col. Lyle M. Cross, USMC with Col. Randy P. Strong, USA, Lt. Col. Clinton D. Wadsworth, USMC and Dave Delaunay

Introduction

U.S. involvement in East Timor is a success story of peacemaking and country-rebuilding. The United States Pacific Command (USPACOM) and U.S. Forces continue to play a critical role in the international effort to assist the people of East Timor. East Timor is more than 5,600 miles from Hawaii and another 3,000 from locations in CONUS where many of the U.S. Forces that provided communications support were based. Timor is the Malay word for Orient; it is part of the Malay Archipelago, as shown in Figure 1, and is the largest of the easternmost of the Lesser Sunda Islands. The population is 90 percent Roman Catholic, 4 percent Muslim and 3 percent Protestant.

East Timor was a Portuguese colony for more than 400 years until 1974, when Portugal sought to establish a provisional government and popular assembly to determine the future of East Timor. Civil war broke out between those who favored independence and those who advocated integration with Indonesia. Portugal withdrew when authorities were unable to maintain stability. Indonesia intervened militarily and integrated East Timor as its 27th province in 1976. The United Nations and the international community did not recognize this integration and both the U.N. Security Council and the General Assembly called for Indonesia's withdrawal, but for nearly 20 years little action was taken. During this time the East Timorese lived under threat of death at the hands of the occupying Indonesian military. In June 1998, Indonesia, prompted by pressure from the U.N. General Assembly, proposed a limited autonomy for East Timor within Indonesia. The two governments entrusted the Secretary-General with organizing and conducting a "popular consultation" to ascertain whether the East Timorese people were in favor of special autonomy within the Republic of Indonesia.

To carry out the consultation, the Security Council, by resolution 1246 (1999) authorized the establishment of the United Nations Mission in East Timor (UNAMET) June 11, 1999. On voting day, August 30, 1999, 98 percent of registered voters went to the polls — 78 percent rejected the proposed autonomy in favor of full independence. Immediately following the announcement pro-Jakarta militia groups aided by Indonesian armed forces began a campaign of violence, looting and destruction. Many East Timorese were killed and as many as 500,000 were displaced from their homes. Indonesian authorities did not respond effectively to end the violence. The Secretary-General and Security Council undertook intense diplomatic efforts to press Indonesia into action. International pressure mounted.

Finally, the U.N. Security Council voted unanimously Sept. 14, 1999, to authorize an Australian-led International Force East Timor (INTERFET) under Chapter 7 of the U.N. Charter. U.S. Forces, in support of OPERATION STABILISE (as the Australians called it), began deploying into Darwin. Brig. Gen. Castellaw, 3rd Marine Expeditionary Force on Okinawa, Commander of the U.S. Forces INTERFET (USFI) arrived Sept. 17, followed by the USCINCPAC MSQ-126 with 18 personnel Sept. 19.

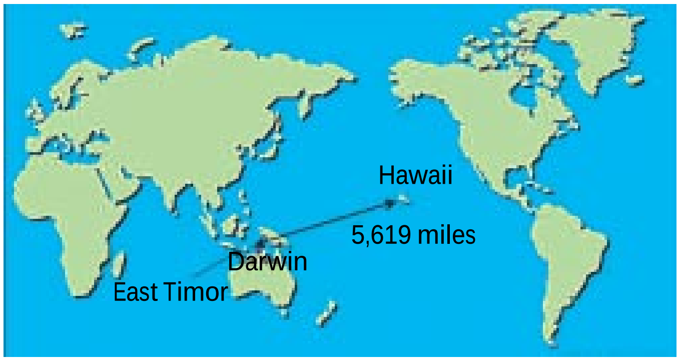


Figure 1.

Communications support provided by U.S. Forces played a pivotal role in the success of the U.N. mission in East Timor. The U.S. military's mission was to provide communications and intelligence planners, as well as ships and helicopters to move troops and equipment. The tyranny of distance, that is a constant factor in planning in the Pacific theater, was a distinct disadvantage to finding a solution to restore peace and a stable independent government to East Timor. The one saving grace of the geographical circumstances was the proximity of Darwin to East Timor and its capital, Dili. Darwin was used as an intermediate staging base and the location of the Commander U.S. Forces INTERFET headquarters. Essential to the success of our mission was the transition from military to a commercial solution for communications support.

The entire international force was comprised of more than 8,000 military members from 15 different countries including approximately 5,000 U.S. military, most of which were stationed offshore on ships. U.S. ground forces numbered about 300. At the height of the crisis, 40 different United Nations and humanitarian agencies were providing support. The timeline, shown below, illustrates significant events in East Timor's quest for independence and coalition assistance.

05 May 99 - Indonesia agrees to hold referendum in August
11 Jun 99 - UNAMET is established
30 Aug 99 - East Timorese reject autonomy via democratic election
31 Aug 99 - Violence erupts for the next several days
31 Aug 99 - USFI Liaison officers deploy to Brisbane
11 Sep 99 - Planners deploy to Brisbane
12 Sep 99 - Indonesian President requests international peacekeepers
15 Sep 99 - U.N. Security Council authorizes INTERFET
15 Sep 99 - Establishment of U.S. Forces INTERFET
18 Sep 99 - U.S. Forces Darwin HQ established
27 Sep 99 - COMUSF INTERFET Dili HQ established
Feb 00 - U.N. Transitional Administration East Timor assumes responsibility for peacekeeping operation

C4I Communications

The area of operations presented many challenges for the communications units. Five-hundred miles separated Darwin (ISB) and Dili (FSB). When the first servicemembers arrived, East Timor lay in ruins, there was little infrastructure of any kind remaining in

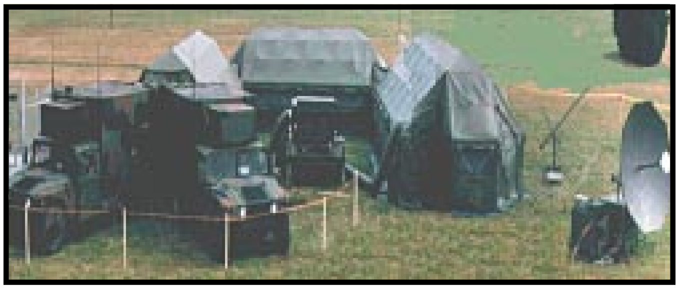


Figure 2. CINCPAC MSQ-126 Fly Away Command Post. The MSQ-126 can deploy via (1) C17, (1) C5 or (4) C130s. It can support a staff of 30 with the full range of DISN services.

Dili or the outlying areas due to the looting and arson, which had occurred. Almost total destruction of the infrastructure included electrical and sewage disposal systems. Most of the buildings had been burned and/or gutted of fixtures. (Within weeks U.S. Forces began to see the city recover due to massive humanitarian assistance administered by numerous agencies.) Additionally, the mountainous geography of East Timor hampered line-of-sight communications between tactical forces. These factors dictated the deployment of U.S. military communications assets. From September 1999 through February 2000, U.S. Forces INTERFET met the highly dynamic C4 support requirements for peacekeeping and the subsequent humanitarian assistance operations effectively.

This success was the result of effective planning and phasing of C4 forces. The CINCPAC MSQ (shown in Figure 2) is a USPACOM C4 asset designed for rapid deployment to provide DISN services for early entry forces. The MSQ-126 arrived in Darwin Sept. 19, and provided DSN, NIPRNET, SIPRNET, video, GCCS and AUTODIN messaging. The 31st Marine Expeditionary Unit's JTF Enabler arrived in Dili Oct. 9, to support COMINTERFET, Australian Maj. Gen. Peter Cosgrove. Another early entry C4 capability, the Enabler package provided DSN, NIPRNET and SIPRNET. It departed on Oct. 23, after lead elements of Task Force Thunderbird (shown in Figure 3) arrived in Dili Oct. 20, to assume the mission for INTERFET. This task force, comprised of the 86th Signal Battalion, and elements of the 40th and 504th Signal Battalions, all from Fort Huachuca, Ariz., provided the principle C4 support promised to the U.N. effort. PACOM's J6, Col. Randy Strong, USA, was assigned as the Commander, U.S. Forces East Timor. Five soldiers and one civilian contractor provided continuous support to INTERFET.

Thirty-seven personnel provided Counterintelligence/Human Intelligence (CI/HUMINT) support to INTERFET. This support capability, shown in Figure 4, provided threat information and counterintelligence operations, and ensured commanding officers had the information they needed to carry out operations throughout East Timor. The network configuration that was used is shown in Figure 5. The diagram represents the major pieces of the final architecture to support U.S. Forces. It reflects a robust configuration with redundant paths to the two key entry points within the Pacific theater.

Transition from military to commercial communications moved quickly with the approval of a detailed transition plan on Oct. 30, 1999. By Jan. 1, 2000 the communications commercialization was completed. Of the 300 U.S. personnel employed at the height of the operation, 150 of them were dedicated to the military C4 mission. The commercialization allowed them to return to their home stations with their equipment, which included seven SHF satellite terminals, six telephone switches and three data hubs, as well as numerous line-of-sight multichannel radios.

The impact on operational to strategic resources was also alleviated, as four standard tactical entry point (STEP) missions for DISN services were terminated. The timeline used to move to a commercial communications solution is shown below.

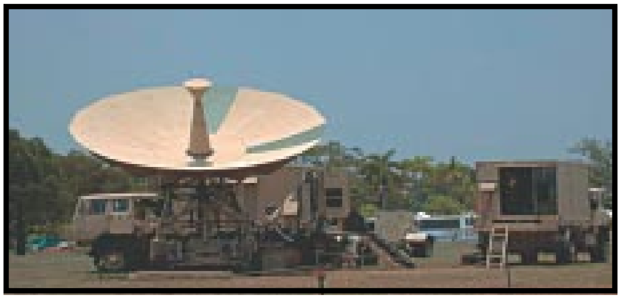


Figure 3. These are the assets of Task Force Thunderbird. Additionally, the 11th Signal Brigade used four satellite terminals, several voice and data switches and numerous line-of-sight multichannel radio systems.

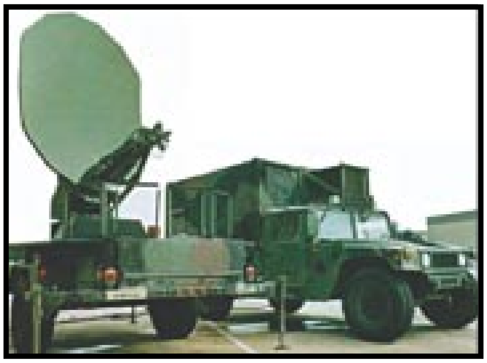


Figure 4. Intelligence support was provided by CINCPAC Unit 205th MI and JICPAC. The Trojan Spirit provided links to all-source intelligence and Intelink-C.

13 Oct 99 - Contract for Telstra let
21 Oct 99 - COMUS INTERFET C4 "green"
30 Oct 99 - C4 transition plan approved
15 Nov 99 - Redeployment of C4 units
15 Dec 99 - TF Thunderbird departs Dili
1 Jan 00 - Commercialization complete
26 Jan 00 -Transition of USFI to USGET
1 Feb 00 - USFI disestablished
USGET established

Telstra, jointly owned by the Australian government and private industry, installed the "Big Pipe" pictured in Figure 6. It was used to extend commercial bandwidth into Dili from Australia. Through this means, USGET (United States Support Group East Timor) had access to both the SIPRNET and NIPRNET through Cisco routers and Type 1 encryption devices (NES). Ericson provided commercial satellite telephones, which were later replaced by Iridium.

Using this capability COMUSINTERFET was provisioned with NIPRNET and SIPRNET service. Secure voice service was provided through the use of a public telephone exchange and encrypted using STU IIIs. Redundant secure voice services were added using Inmarsat and Iridium. Cellular telephones and hand-held radios were used for non-secure voice. As the mission transitioned from peacekeeping to humanitarian assistance, the commercial architecture changed as well.

In addition to a substantial savings in resources, equipment and personnel, commercialization resulted in a responsive and scalable C4 solution. COMUSGET has changed locations four times since their establishment, but each time the services were easily reinstalled to meet mission requirements. Central Command used commercial satellite deployable KU earth terminal (DKET), and encryption devices to provide DISN service in austere environments. The commercialization of communications for East Timor served as a prototype for future DoD commercialization efforts.

The international community's assistance in East Timor has been one of the most successful peace enforcement and country-rebuilding missions in recent years. As the mission in East Timor continues to evolve, U.S. Forces have sent in different assets. U.S. Forces have been instrumental in delivering food and other supplies, engaging in community projects and transporting diplomatic and peacekeeping representatives to East Timor.

Even though East Timor became an independent nation May 29, 2002, the work is certainly not over. The United Nations continues to maintain a presence in East Timor to ensure its security and stability. The successor mission, the United Nations Mission of Support in East Timor (UNMISET) is planning a gradual withdrawal of the territory and supports the East Timorese authorities to maintain democracy and justice, internal security and law enforcement, and border control. Humanitarian agencies continue to provide assistance as well.

Col. Cross is the Chief, C4 Operations and Plans Divisions, USCINCPAC.

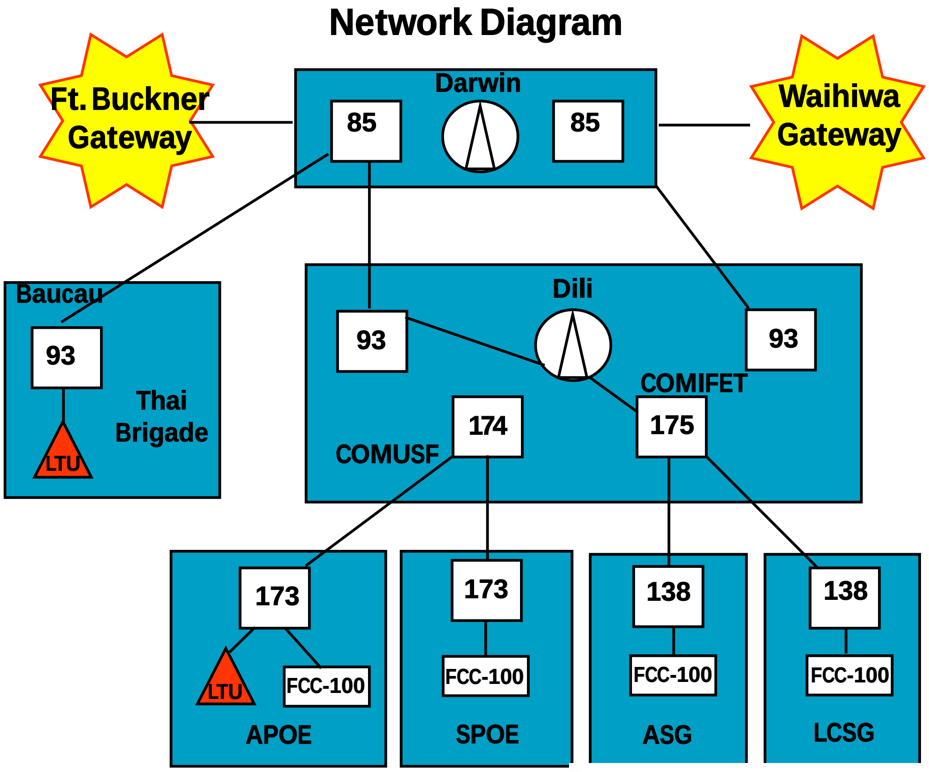


Figure 5.

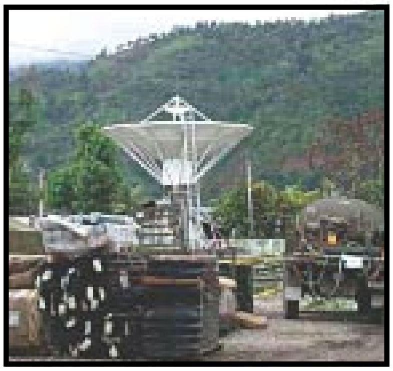


Figure 6. The "Big Pipe" used to extend the commercial bandwidth into Dili from Australia for USGET access to SIPRNET and NIPRNET using Cisco routers and Type 1 encryption devices (NES). This was the "longest pole" ever used in exit strategy, which combined the talents of the U.S. Joint Staff J6, 11th Signal Brigade Program, Telstra, Cisco and Ericson, and was certainly an example of capitalism working at its best.

Humanitarian and Civic Assistance

The United States has an ongoing commitment to the newly formed East Timor nation. U.S. Navy personnel have completed numerous community service projects including painting of the August School in Feb. 2001. Aug. 2001, the Seabees with Naval Construction Battalion 5, U.S. Pacific Fleet, Calif., worked on the Bemos water treatment plant in the effort to rebuild the nation's infrastructure. During this visit a local orphanage also benefited from structural improvements, and electrical and plumbing repairs. U.S. efforts have focused on assistance to improve basic health and social conditions, and the overall quality of life for the people of East Timor.

Clockwise from top left to right: Dili, East Timor - Feb. 2001, a U.S. Navy corpsman assigned to USS Juneau takes a young girl's temperature; Dec. 2001, U.S. Navy Seabees attached to the U.S. Support Group East Timor check an electrical panel at Bemos water treatment plant; Oct. 2002, a U.S. Navy doctor examines a patient as part of the Amphibious Ready Group's medical support during a three-day rotation in East Timor; Apr. 2002, a service member teaches basic math skills to some children.

Restructuring Naval Education

By JO2 Jd Walter, NPDC, Public Affairs Office

The Navy recently created the Naval Personnel Development Command (NPDC) to standardize and integrate the training processes and technology of its Learning Centers. NPDC evolved from the Task Force for Excellence through Commitment to Education and Learning (EXCEL) and its efforts to institutionalize the precepts of the Navy's Revolution in Training.

Currently, there are plans for 15 functional Learning Centers under NPDC with each being directly responsible for the end-to-end development of learning tools and opportunities within a given occupational arena. By providing the formal connection between the Fleet and individual training, the Learning Centers will facilitate a relationship with Fleet representatives to identify human performance deficiencies, build and deliver solutions, and evaluate results.

The Learning Centers comprise the core of the new organization. The centers will utilize the Sailor Continuum and Human Performance Systems Model to develop professional continuums and serve as the knowledge managers for all occupational fields and mission areas. Additionally, centers for leadership and professional development will be established to ensure the *whole person development* of Sailors. The Center for Naval Leadership in Norfolk, Va.; Center for Naval Intelligence at Dam Neck, Va.; and Centers for Naval Aviation Technical Training and Cryptology in Pensacola, Fla., all stood up on a provisional basis in September 2002. The remaining centers will be provisionally stood up in the near future. They will assume responsibility for the operations and functions of their core areas. Each center will have a Commanding Officer and the final organizational construct and manning will be determined billet by billet to best support mission needs.

So, just as the Navy's Revolution in Training steers toward the complete development of Sailors, it is likewise piloting the improvements to the Navy's training organization, giving both Sailors and the Navy the tools to learn, grow, lead and excel. To learn more about this revolutionary structure, visit Navy Knowledge Online, at https://www.nko.navy.mil □

Navy Knowledge Management Portal

Navy education and training created a new way for Sailors to manage their careers via the Internet. Navy Knowledge Online (NKO), the knowledge management portal, gives Sailors instant access to all training and educational information related to their occupational field.

Knowledge management is the gathering of organizational processes, systems, methodologies, visions and resources into a centralized location. For Sailors, the knowledge management portal will identify career paths, milestones, and educational tools and opportunities. For the Navy, this will result in greater operational efficiency and eliminate organizational redundancies. To develop the portal, the Navy teamed with Appian, a provider of large-scale software solutions. "We wanted to provide every Sailor with a personalized gateway to the Navy's knowledge base for all professional and personal development," said Rear Adm. Kevin Moran, Commander Naval Personnel Development Command/Director, Task Force for Excellence through Commitment to Education and Learning. "We selected Appian based on their track record."

The faceplate of the portal will be individualized Web pages that Sailors can customize. This portable Web page will be assigned to Sailors during boot camp and will remain accessible throughout their Navy careers. The portal will give Sailors access to the most relevant and up-to-date career information as easy as point, click, and learn. *To visit NKO go to https://www.nko.navy.mil. To learn more about the development of the knowledge management portal, visit www.excel.navy.mil.* □

Surface Combat Operations New Home

By George Dunn, CSCS, Public Affairs

The Navy's surface combat systems community has a new home, courtesy of the Revolution in Training. The Center for Surface Combat Systems (CSCS) has been established in Dahlgren, Va., and will be responsible for training the commissioned and enlisted personnel who operate, maintain, and employ the various combat systems found on the Navy's surface warships. Initially, CSCS is being staffed by Aegis Training and Readiness Center (ATRC) headquarters personnel, also located in Dahlgren, and key surface combat systems training activities' personnel from around the Fleet. Capt. Paul Stanton, ATRC commanding officer, will be dual-hatted as CSCS commanding officer. ATRC, which trains Navy personnel in the operation, maintenance, and employment of the Aegis Combat System found aboard the Navy's fleet of Aegis cruisers and destroyers, will be realigned and come under the auspices of the new command. Naval Sea Systems Command has overseen ATRC since its establishment in 1985.

"ATRC has had tremendous success in training the Navy's Aegis Combat Systems personnel," said Commander, Naval Personnel Development Command, Rear Adm. Kevin Moran. "Their approach to, and experience with waterfront training, acquisition support, and weapons systems interoperability training provides a great model for future successes of the Center. By leveraging the Aegis training model, the Center is poised to create a more dynamic training environment for other surface combat systems personnel, and will play an important role in developing the CNO's vision to revolutionize Navy training."

In addition to Aegis Fire Control Technician training and Aegis officer pipeline training, CSCS will train the Sonar Technician, Torpedoman, Gunner's Mate, Operations Specialist, Fire Control Technician, Electronics Technician and Mineman ratings. *For additional information on CSCS and the Revolution in Training visit https://www.nko.navy.mil* □

"The vision of the Revolution in Training is to increase Sailor proficiencies by providing the best training in the most efficient manner possible." Chief of Naval Operations, Adm. Vern Clark said, "What we have now is a structure that advocates excellence not only in the individual, but also excellence in the management of training and education."

VIRTUAL CONNECTING TECHNOLOGY FALL 02

Arming the Warfighter with 21st Century Information Technology

Virtual Connecting Technology Fall 2002, December 3-17, was engineered to arm the warfighter with 21st century Information Technology (IT). The CT staff provided loyal attendees and newcomers alike with an integrated avenue to keep abreast of emerging IT supporting the Navy's role in homeland security.

Visitors to Virtual CT at **www.ct.navy.mil** were informed and challenged with the latest in wireless technology, NMCI updates, the C4ISR vision, Knowledge Management, eBusiness, eCommerce, eLearning, Data Warehousing, professional development opportunities and much more. Our goal was to provide the warfighter, and those who support and direct the warfighter, with the most current IT resources needed to remain on the cutting edge of homeland defense.

The Virtual Connecting Technology Fall 2002 event was FREE to all attendees and exhibitors! Those who participated had the opportunity to:

♦Explore emerging products, Government and Industry visions, policies, and services that increase the effectiveness of the warfighter.

♦Gain perspectives on topics affecting the future of IT and Information Management (IM) throughout the Department of the Navy, Department of Defense, Federal Government, Academia, and Industry.

♦Explore the Virtual Exhibition and Presentation Halls using a variety of search functions.

♦Forge new partnerships with IT/IM Leaders by creating an eBusiness Card to deposit with exhibitors and presenters.

♦Send a Virtual eCard from the event to friends and colleagues.

♦Leave the event with an understanding of who can be contacted to provide their organization with the services and products they need.

Mark your calendar now for CT Spring 2003, May 20-22, planned for the Pavilion Convention Center Virginia Beach, Va., and CT Fall 2003, Nov. 18-20, planned for the Town and Country Resort Hotel and Convention Center, San Diego, Calif.

Please visit our Web site at **www.ct.navy.mil** for more information. You may also contact the Connecting Technology staff via e-mail at **conntech@spawar.navy.mil** or call (757) 444-9967.

Please join us as we support the 21st century warfighter through an exchange of IT ideas and innovations.

Connecting Technology is sponsored by the DON Information Technology Umbrella Program Visit us at www.it-umbrella.navy.mil

NAVAIR Response Center

By Vicky Falcon, NAVAIR Public Affairs

Onboard the deployed USS Boxer (LHD-4), AT1 Roger Rever was upgrading a computer processor on a CH-53D "Sea Stallion" helicopter as part of his job as a Quality Assurance Representative in the Aircraft Intermediate Maintenance Department onboard. The upgrade was part of an Avionics Change (AVC) ordered through a Navy Technical Directive for the AN/AAR-47 Missile Warning Set installed onboard. The AN/AAR-47 is a passive missile detection system that detects attacking missiles and provides an audio and visual approach sector warning to the crew.

"While upgrading from a -3 model to a -4 model we discovered that one of the processors onboard had never been upgraded from the -2 version," said Rever. "We suspected that we could update the -2 to a -4 through the incorporation of the current AVC, but we needed to be sure — after all, lives could be at stake!" Usually, Rever would find the Fleet Support Team (FST) for the item in question and contact them for direction. However, in this case he was unable to locate a contact for the AAR-47 system. Rever decided to take advantage of the Navy Distance Support infrastructure by submitting his request via an online form found at **www.anchordesk.navy.mil/index.htm**. The request was processed, given a tracking number, and forwarded to the NAVAIR Response Center (NRC) for action. Rever could also have reached the NRC by calling **877-41-TOUCH (press option 2)**, or by e-mailing **fleetresponse@navair.navy.mil**.

The NRC coordinates and facilitates the resolution of Naval aviation-related questions and issues, assisting customers who have been unable to find answers via their appropriate chains of command. According to Fillip Behrman, program manager for the NRC, the center links customers with experts across the Naval Aviation community, ensuring the most current, comprehensive and accurate responses possible in a timely manner. Delays can often be reduced or avoided by utilizing the resources of the NRC. "Our warfighters have the right to expect timely, accurate answers to their questions — and that's what we provide," said Behrman.

Rever was impressed with the efficient and timely response to his question. "I cannot speak highly enough about the outstanding job that these (people) do," said Rever. "I have employed the NRC on several occasions and their performance has been nothing less than outstanding — even amazing."

As part of the Navy's Distance Support program the NRC can support remotely located fleet, Federal Government agencies and contract customers. The NRC works around-the-clock across traditional organizational boundaries providing coordinated solutions to Naval aviation-related questions. For more information about the NAVAIR Response Center, authorized users can go to **http://nrc.navair.navy.mil**.

NAVAIR provides seamless, integrated, advanced warfare technology through the efforts of a worldwide network of aviation technology experts. Services include: professional training; carrier launch and recovery; sensor data and precision targeting; real-time communications; aircraft and weapons development; and successful deployment and sustainment. NAVAIR provides matchless combat capabilities to the warfighter. For more information about NAVAIR, go to **www.navair.navy.mil**.

CAP Launches New Web Site!

The Department of Defense (DoD) Computer/Electronic Accommodations Program (CAP) announced the activation of a new, user-friendly Web site, which provides information on assistive technology accommodations and related services for persons with disabilities within the DoD and other Federal agencies. The Web site, www.tricare.osd.mil/cap, showcases how individuals with disabilities may use accessible online tools to find information and accommodations to enhance job performance.

"When users log on to the CAP Web site, they will see a new and improved layout designed to be more accommodating to our users," said Dinah Cohen, CAP Director. "The CAP team worked to develop a site that allows customers, people with disabilities, and Federal managers to customize their personal search for program and contact information," she added.

The site features more resources — including an enhanced online accommodation process, a better assistive technology section, and an improved virtual CAP Technical Center (CAPTEC) tour — to assist individuals in selecting the most appropriate and reasonable accommodations. The Defense Department established CAP in 1990 to eliminate employment barriers for people with visual, hearing, dexterity and cognitive disabilities. Since its inception, CAP has funded and provided more than 30,000 accommodation solutions for individuals with visual, hearing, dexterity, and cognitive disabilities within DoD and about 50 other Federal agencies.

CAP SERVICES

CAP is the Federal Government's centrally-funded accommodations program. Much of CAP's success lies in its ability to provide reasonable accommodations to employees quickly, easily, and in a cost efficient manner. CAP can assist your organization by: Purchasing assistive technology and services; Conducting needs assessments; Assisting in technology integration; Assistive technology training; Assisting in accommodations for work-related injuries; Supporting Telework participants with disabilities; and Conducting presentations on CAP services and other accessibility issues.

THE TECHNOLOGY

CAP pays for a wide variety of assistive technology, devices, and services for people with disabilities, CAP also provides training on the technology and purchases software upgrades. Frequently requested accommodations include:

•Blind/Low Vision: Magnification systems, speech and Braille output systems, scanner/reader systems, Braille embossers, Closed Circuit Televisions (CCTVs), and Braille notetakers.
•Deaf/Hard of Hearing: Teletypewriters (TTYs), PC-TTY modems, telephone amplifiers, assistive listening systems, and visual signaling devices.
•Dexterity Disabilities: Alternative keyboards, alternative input devices, word prediction software, speech recognition systems, pointing devices, hands-free computer interface systems and keyguards.
•Cognitive/Learning Disabilities: Talking dictionaries and scanner/reader systems.
•Communication Disabilities: Electronic communication aids and speech output systems to augment communication.

TECHNOLOGY EVALUATION CENTER

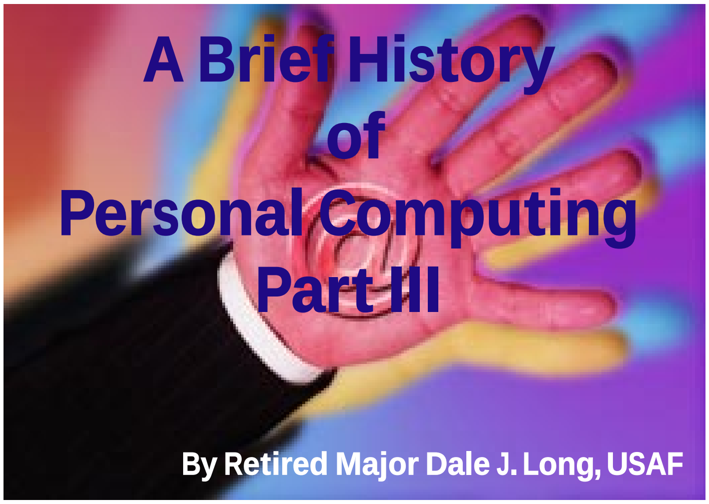
The CAP Technology Evaluation Center (CAPTEC) is a facility dedicated to the evaluation and demonstration of assistive technology. It was established to assist employees and supervisors in choosing appropriate assistive technology to create work environments that are accessible to persons with disabilities. CAPTEC also hosts open houses designed to highlight particular advances in assistive technology.

The CAP Staff conducts needs assessments to help identify the most appropriate solution to meet individual requirements. CAPTEC consists of computer workstations configured with a wide variety of assistive technology. People in the process of evaluating assistive technology who have questions about compatibility or functionality, or who need to compare several solutions, may visit CAPTEC to test and evaluate equipment.

Since the release of the new Web site, activity has increased dramatically. Over 400,000 hits were received in October 2002 and CAP continues to experience daily activity increases.

If you are interested in learning more about CAP services, disability accommodations, or other methods of impacting the recruitment, hiring, and retention of people with disabilities within the Federal Government, please visit the new CAP Web site!

All services are available by visiting CAPTEC, located in the Pentagon, Room 2A259, or by contacting CAPTEC at 703-693-5160 (V) or 703-693-6189 (TTY). Regular hours of operation are Monday - Thursday from 9:00 a.m. to 3:00 p.m. or by appointment. Services are also available online at **www.tricare.osd.mil/cap**



A Brief History of Personal Computing Part III

By Retired Major Dale J. Long, USAF

Welcome back to the third in a series of articles reviewing the history of personal computing. In the summer issue of *CHIPS*, we looked at the development of the modern personal computer. In the fall issue, we examined the evolution of personal computer (PC) operating systems and application software. In this issue, we will look at the technologies that tie our PCs together through networking.

We tend to think of digital networking as a relatively new concept, but the roots of modern networking extend back over 150 years. Many years before Charles Babbage created what is considered the first computer, his "Differential Engine," the telegraph ushered in the age of digital communications in 1844 when Samuel Morse sent a message 37 miles from Washington D.C. to Baltimore using his new invention. While the telegraph is a long way from today's computer networks, it was arguably the single most significant event in human communication since the development of language. For the first time in human history, we had a reliable method of communicating in real-time beyond line-of-sight. As long as you could connect two locations with wires, you could exchange information almost instantaneously without regard to distance. Much as modern data networks use 1s and 0s to encode and transfer information, Morse code was the language of the telegraph. Morse code is a binary-like system that uses dots and dashes in different combinations to represent letters and numbers. The big difference is, that while the telegraph operators of the mid-19th century could perhaps transmit four or five dots and dashes per second, computers now communicate at speeds of up to one billion 1s and 0s every second, which we refer to in digital shorthand as one gigabit or "1Gb."

Not long after Morse invented the telegraph, a Frenchman named Emile Baudot developed a typewriter-style telegraph machine that allowed users to key in their messages using the basic alphabet and print out received messages using automatic translators built into the machine. These early precursors to modern modems allowed virtually anyone to send and receive telegraph messages without having to understand the code used to transmit the message. However, Morse code did not lend itself well to automation due to the variable length of each character, so Baudot developed a more uniform code for his system. Baudot used a five-bit binary code to represent each character. As that only gave 32 possible characters (00000 to 11111 = 32), it wasn't going to be enough to include all 26 letters and 10 digits. He solved this problem by adding two "shift characters" for figures and letters that performed in much the same way as a typewriter shift key. This gave him 62 combinations (not quite six-bit computing) for letters, figures and punctuation marks. Western Union, the most famous telegraph company in history, eventually replaced all of its Morse telegraph equipment with Baudot's "teletypewriters." In honor of Baudot's pioneering contributions, the speed of serial communications is still measured today by measuring the "Baud rate."

However, despite being the dominant digital communications code for over a century, the Baudot five-bit code was not suited to 20th century computing. Computers, which were developed independently of the telegraph, needed the ability to discriminate between upper and lowercase letters. Baudot's code only provided for uppercase letters. In response to the need for a new standard information exchange format, a group of American communications companies got together in the 1960s to devise a new code. Their new standard used seven bits that could represent 128 characters. This new standard came to be known as the American Standard Code for Information Interchange (ASCII). ASCII was immediately accepted by virtually everyone in the communications world, with one notable exception: IBM. IBM decided to make its own standard, the Extended Binary Coded Decimal Interchange Code (EBCDIC). The IBM code used eight bits and could represent 256 characters. However, aside from IBM using it in their mid-range and mainframe computers, EBCDIC never really caught on. Once it became clear that IBM would not be able to force their proprietary standard on the rest of the world, they eventually adopted the ASCII code. However, as they still wanted the extra capabilities inherent in the 8-bit format, they "extended" ASCII by using an eighth bit so it could represent 256 characters and called it "Extended ASCII." Now that a common language for computer data had been invented, the stage was set for real computer networking to begin.

Early Networking

The origins of the Internet were distilled from the visions and work of computer visionaries of the 1960s. Three of the most influential were the Massachusetts Institute of Technology (MIT) trio of J.C.R. Licklider, Leonard Kleinrock and Lawrence Roberts. Licklider first proposed a global network of computers in 1962. Later that year he moved to the Advanced Research Projects Agency (ARPA) to head the work to develop it. Kleinrock developed the theory of packet switching, which would form the basis of Internet connections. Roberts confirmed Kleinrock's theory in 1965 when he connected a Massachusetts computer with a California computer over dial-up telephone lines. However, while this demonstrated the feasibility of wide area networking, it also showed that the circuit switching technology available through a standard telephone line was not sufficient to support any large-scale networking. Shortly after this project, in 1966, Roberts began work at ARPA and developed the plan for what eventually became ARPANET.

Finding True Believers

When ARPA sent out a request for proposals to build the initial network of four Interface Message Processors (IMPs), many of the large computer and telecommunications organizations did not bother responding, because they thought the task was impossible. Turning ARPA's networking theory into reality fell to another group of visionaries at a small company named BBN (Bolt, Beranek and Newman). We take much of the support activities that sustain the Internet for granted today, but BBN literally created most of them from scratch. They wrote code that would automatically reload crashed servers, pull packets into the machine, figure out how to route them, and send them on their way. They also developed a routing scheme that would automatically route data packets around troubled links in the network and update itself several times per second. BBN had to handle some stiff challenges, not the least of which was dealing with the timing and error-control problems associated with sending data over telephone lines. This was pretty cosmic stuff in an era where most engineers still carried a slide rule and the microprocessors that power modern CPUs had not been invented yet.

The key to the design of ARPANET was the construction of an autonomous subnet, independent of the operation of any host computer. An IMP can take on one of two distinct roles: Host or "store-and-forward." In any host-to-host connection, the IMPs at the respective host sites are the source and destination IMPs for that connection, and the IMPs in the network path between the host sites comprise the store-and-forward sub-network. The IMPs of the sub-network received packets, performed error control, determined the route and forwarded them to the next IMP in the network path. In addition to these tasks, the source IMP and destination IMP were responsible for end-to-end connection management and message processing procedures for the duration of the connection. These procedures included flow control, storage allocation, and message fragmentation and reassembly.

There were many factors that affected the development of message processing requirements. First, there was some likelihood of delay in acknowledging packets due to finite bandwidth or differing bandwidth at the source or destination. This would result in packets arriving out of order, becoming duplicated if they weren't acknowledged by the receiving host in time, or becoming just plain lost. Also, IMPs only had a limited amount of storage space, so they needed to pass packets on as quickly as possible. After spending months customizing software and systems, BBN eventually got the first two IMPs set up at the University of California at Los Angeles and Stanford. ARPANET was born on October 1, 1969, when the first characters were transmitted over the new network. The network quietly expanded to 13 sites by January 1971 and 23 by April 1972.

Outside of BBN and a small group of researchers, ARPA, the network that would transform the world was virtually unknown until the International Conference on Computer Communication in Washington, D.C., October 1972. The ARPANET was the only demonstration at the conference and conclusively proved the feasibility of packet switching networks. Though most of the world still did not know it, we had taken our first steps toward wiring the world for data.

Ethernet

The next big development in networking after ARPANET and packet switching was Ethernet, which is still the dominant network technology today. The roots of the modern Ethernet were planted in a 1973 Xerox Corporation patent memo that described a new protocol for multiple computers communicating over a single cable. Originally intended to help design internal computer-to-computer communications within Xerox copiers and duplicators, Ethernet eventually became a global standard for interconnecting computers on local area networks. Ethernet was developed by Xerox at their Palo Alto Research Center (PARC) in California. In 1979, Digital Equipment Corporation and Intel joined forces with Xerox to standardize the Ethernet system. The first specification by the three companies, called the "Ethernet Blue Book" was released in 1980. Ethernet was originally a 10 megabit per second system (10Mbps = 10 million 1s and 0s per second). It used a large coaxial backbone cable running throughout the building, with smaller coax cables attached at short intervals (usually around six feet) to connect to the workstations. The large coax became known as "Thick Ethernet" or "10Base5." The "10" refers to the speed, which in this case is 10Mbps. "Base" means it is a base band system that uses all of its bandwidth for each transmission, as opposed to a broadband system that splits the bandwidth into separate channels to be used concurrently. The "5" refers to the systems maximum cable length, in this case 500 meters. In 1983, the Institute of Electrical and Electronic Engineers (IEEE) released the official Ethernet standard, IEEE 802.3. This second version is commonly known as Thin Ethernet or 10Base2 (10Mbps, base band, 200 meters).

In 1985, the Computer Communications Industry Association (CCIA) asked the Electronics Industries Association (EIA) to develop a cabling standard which would define a generic telecommunications wiring system for commercial buildings to support a multi-product, multi-vendor environment. This would be a cabling system that would run all current and future networking systems over a common topology using a common media and common connectors. By 1987 several manufacturers had developed Ethernet equipment that could utilize twisted-pair cable, and in 1990 the IEEE released the 802.3I Ethernet standard 10BaseT (T refers to twisted-pair cable). In 1991 the EIA together with the Telecommunications Industry Association (TIA) published a standard for telecommunications cabling (EIA/TIA 568). It was based on Cat[egory] 3 Unshielded Twisted Pair cable (UTP), and was closely followed one month later by a Technical Systems Bulletin (TSB-36) which specified higher grades of UTP cable, Cat 4 and Cat 5. Cat 4 specified data rates of up to 20MHz and Cat 5 up to 100MHz, which at the time seemed like a lot of bandwidth. However, as George Carlin observed, "stuff accumulates to fill available space." Given the exponential growth of networking technology, even Cat 5 is being pushed to its limits. The current state of the art is Cat 6, and Cat 7 is waiting in the wings.

Despite being pronounced "about to be dead" several times in the last 15 years, Ethernet has successfully defended itself against all comers in the networking standards world, including LAN Token-Ring, Fiber Distributed Data Interface (FDDI) and Asynchronous Transfer Mode (ATM). You can tell who is winning simply by looking at the type of equipment people are buying. Network interface cards (NICs) and switches are generally replaced every two to three years. Since 1998, 90 percent of all NICs and switch ports shipped have been some flavor of Ethernet. Case closed, at least for now.

There are two basic reasons Ethernet still rules. First, the invention and installation of fiber-optic cable, with its huge bandwidth potential, means you can use a "cheaper, dumber" technology like Ethernet as efficiently as "expensive, smart" technology like ATM. Without fiber optics, we would need all of the ATM horsepower to squeeze every last drop of data into the scarce bandwidth available on copper wire. With fiber, that bandwidth constraint has pretty much gone away. Also, Ethernet has been getting smarter in useful ways. Because Ethernet adapters can auto-sense 10Mbps, 100Mbps and 1,000Mbps operations, it's now possible to establish a tiered Ethernet network that supports all three speeds using the same standard. For example, a LAN may have a Gigabit Ethernet backbone and departmental servers that are connected by Fast Ethernet, and then connected to conventional 10Mbps Ethernet switches and hubs that tie into desktops. Without that ability to automatically sense what speed your backbone is using, we might need to integrate three different network protocols to do the same thing Ethernet does on its own. There are other technologies and standards that I really wish we had time to review here, including FTP (file transfer protocol) and TCP/IP (Telecommunications Protocol/Internet Protocol, also developed at BBN). But the issue I've saved for last that incorporates both of those issues is the Big Kahuna of networking — e-mail.

You've Got Mail!

Seventeen years ago, when I first started fooling around with computers, the only people who had e-mail were the few thousand hardy souls who had access to ARPANET or large private or corporate systems like General Electric. Everything was in plain text and files were exchanged via FTP over Unix-based systems. Think about this: the Internet, with its millions of servers, and the World Wide Web, with its billions of pages, are all essentially the result of the human desire to communicate. I submit to the jury that e-mail, more so than any other single factor, is the application that is primarily responsible for the development of the modern Internet. Here is my case. E-mail first appeared in the 1960s when users on time-sharing systems wanted a way to leave messages for each other. These early e-mail systems were very simple. Mailboxes consisted of a text file, readable only by a single user, to which new messages were appended. There were no mail reader programs. Users had to scroll through the text file to the most current entries. If the reader didn't edit out old material fairly frequently large mail files could become very long and hard to get through. These primordial e-mail systems were initially limited to the physical reach of the local system.

ARPANET added "reach" to e-mail by connecting systems together. The first recorded case of e-mail traveling from one site to another occurred in 1972 when Ray Tomlinson, then an engineer at BBN, delivered an electronic message by copying it a across a network link connecting two DEC PDP-10s. Tomlinson, by the way, is also the person who decided to use the "@" symbol to separate the user from the host part of an e-mail address. E-mail caught on quickly. Less than a year later, 75 percent of the traffic on the ARPANET was e-mail. There were no protocols that specifically covered e-mail. Mail was sent via FTP, which had commands specific to mail transfer. Mail delivery and tracking information was included in the mail headers, but no defined mail header standards. Also, mail programs that disagreed over formats would often refuse to talk to one another. For example, Multics systems used the @ symbol as a "line kill" command.

At the time of most of these events, TCP/IP, which eventually provided a standard exchange format for all networks, had not yet appeared on the scene. The ARPANET used Network Control Protocol (NCP) as its core network protocol, and was not able to communicate with any other packet network in existence at the time. Deliverance from the e-mail Tower of Babel first appeared in the form of "delivermail," which was developed by Eric Allman and originally shipped with BSD (Berkeley Software Distribution) Unix versions 4.0 and 4.1 in 1979. Delivermail successfully handled e-mail using FTP over NCP and was soon incorporated into the ARPANET community. Delivermail eventually evolved into sendmail, which is arguably the most influential and important e-mail program developed to date.

About the same time that e-mail was developing on ARPANET, Vint Cerf (Father of the World Wide Web) and Bob Kahn (from BBN) were working on a way to connect packet networks together. The results of their work would become the TCP/IP protocol, which defined standards for data exchange and communication between networks. ARPANET transitioned to TCP/IP in 1982, and the widespread implementation of TCP/IP paved the way for today's standard for e-mail: Simple Mail Transfer Protocol (SMTP). In response to the development of SMTP, Allman evolved his delivermail program into sendmail, which extended the reach of e-mail beyond the ARPANET system and allowed users to communicate between all the various private packet networks that would eventually form what we now know as the Internet. The drive to communicate, coupled with the development of a universal system of point-to-point communications embodied in e-mail, are what brought the Internet together.

Billions, perhaps trillions of dollars have been spent over the last 150 years devising faster, more robust ways to allow people to set lunch dates, ask "whassup," send sales pitches, and — squabble. E-mail further evolved in the 1990s with the introduction of more feature-laden mail programs, including Lotus ccMail and Notes, Microsoft Outlook, and various other programs. But other than adding the ability to transmit richer types of information (including, unfortunately, potentially hostile payloads), they have basically just extended the functionality originally codified by sendmail and SMTP. The final evidence in support of my belief in e-mail's pivotal role in the development of modern networking is this: current estimates from people who watch Internet traffic patterns say that the Internet will pass over 36 billion e-mails this year. That comes out to 114 e-mails to roughly a second, every second of the year. And that figure will only grow as more areas of the world gain access.

Closing Words

There are various opinions on what it takes to build a network, but one that caught my eye recently was offered by Van Macatee, an executive at Level 3 Communications, in the November 1, 2002, issue of the Web magazine *America's Network*: *"Any schmuck can build a network."* I'm not sure how Macatee defines a schmuck, so I'll offer a definition: a network schmuck is someone who knows what the technology can do and how to plug it in and turn it on, but not how the technology works or what effect it will have on the people connected to it.

The Internet, is only relatively simple today because of the efforts of the pioneers in the field who had the vision to see the future, the skills and will to make it happen, and the wisdom to cooperate to achieve common goals. The development of the hardware, software, and transport protocols and technologies that make up modern networking are the products of many dedicated, intelligent, talented people whose efforts rival the building of the Pyramids and the Apollo space program as cooperative human endeavors. Schmucks did not build the Internet. Despite the probable difference in our salaries, I strongly disagree with Macatee's assertion. Perhaps just about anyone can buy a network out of a box and just plug it in. But plugging in and turning on a network are not the same as building one.

A modern parallel to the development of the Internet is the Navy's NMCI project. The goal is similar: build a single extended network to serve the entire service in much the same way that the Internet now serves the world. The Navy has many of the same challenges in building the NMCI that faced the people who built the Internet: defining common standards, integrating technologies, and getting everyone to agree on the one right way to do certain things. The Navy is at a pivotal point. In building the NMCI you can, right now, shape the work environment of the entire Navy for decades to come. Please remember, though, that simply building a big network that adheres to a single set of technical standards is not the goal. NMCI will ultimately be judged on how it supports the Navy as an organization. What the world has done with the Internet, I believe can be done with NMCI.

That's all for now. In the next issue, we will conclude this serial history of personal computing with a look at the development of the World Wide Web and what it means to be part of today's wired, interconnected world. Until then...

Happy Networking!

Long is a retired Air Force communications officer who has written for CHIPS since 1993. He holds a Master of Science degree in Information Resource Management from the Air Force Institute of Technology. He is the Telecommunications Manager for the Eastern Region of the U.S. Immigration & Naturalization Service.

Talking with Dinah Cohen Computer/Electronic Accommodations Program (CAP) Director

CHIPS: Many people talk about the "digital divide" separating those with access to computers and the Internet to those who do not have access opportunities for financial reasons. But isn't there another digital divide separating private citizens with disabilities from technology? CAP does such a great job assisting DoD and Federal employees with disabilities to bridge the gap, but is there an agency to assist private citizens with disabilities who may be cut off from technology?

Ms. Cohen: The digital divide falls into two categories. The first, people who have access to a computer, but cannot access the information. I hope and think that Section 508 is reducing this divide by working with industry and Federal Government to ensure that electronic and information technology is accessible and usable by people with disabilities. For assisting people in obtaining access to a computer, I am aware of some bold actions regarding universal design and assistive technology/computer access that are part of President Bush's New Freedom Initiative. You can see more on this issue at **www. disabilityinfo.gov**.

Editor's Note: The New Freedom Initiative was established to ensure that the more than 54 million Americans with disabilities learn and develop skills, find meaningful work, and realize the promises of the Americans with Disabilities Act. To achieve equality of opportunity, independent living, and economic self-sufficiency, this comprehensive plan promotes the full participation of people with disabilities in all aspects of American life. The Federal Web site, **www.disabilityinfo.gov**, provides resource information and links to agencies and programs designed to assist citizens with disabilities. Just a sampling of links follow. Comprehensive information about Federal job opportunities can be found at **www.usajobs.opm.gov** or call **1-478-757-3000/ TDD 1-478-744-2299**. A free service of the Office of Disability Employment Policy (ODEP) of the U.S. Department of Labor, the Job Accommodation Network available at **www.jan. wvu.edu** or **1-800-526-7234 (V/TTY)**, provides information about job accommodations, the Americans with Disabilities Act (ADA), and the employability of people with disabilities. The RESNA Alternative Financing Technical Assistance Project (Agreement No. H224C000200) is funded by the National Institute on Disability and Rehabilitation Research (NIDRR) under Title III of the Assistive Technology Act of 1998. This Web site, **www.resna.org/AFTAP/ index.html,** was developed with grant funds and is designed to assist individuals in receiving loans to ensure they can access assistive technology. The information on these pages does not necessarily reflect the position of NIDRR/U.S. Department of Education or RESNA, and no official endorsement of the materials should be inferred.

NAVAIR CONNECTS WITH ARMY SPECIAL FORCES

Kevin Morse, PMA-241's deputy assistant program manager for logistics, gave his first briefing on Fast Tactical Imagery to the Green Berets in a bombed-out building similar to those shown here in Afghanistan. The wall was painted white and window openings were covered with boards to block the light so the presentation could be seen clearly.

By Renee Hatcher

The Naval Air Systems Command F-14 Program Office (PMA-241) sent one of its own to the front lines of the war in June 2002 to help improve the situational awareness of Army Green Berets on the ground. "The thrust of PMA-241 has always been to provide service to the fleet," said Capt. Peter Williams, F-14 Program manager. "We have been the ultimate technology provider for the F-14 community, but when we can go beyond that and help our brethren in the Army, it's an exceptional thing."

Kevin Morse, PMA-241's deputy assistant program manager for logistics, and two contractor support personnel spent about three weeks in Afghanistan establishing connectivity between Army Special Forces and Navy tactical aircraft for the exchange of imagery and intelligence. NAVAIR loaned the Army four Fast Tactical Imagery (FTI) laptops, a technology developed by PMA-241, that can retrieve and send information in near real-time.

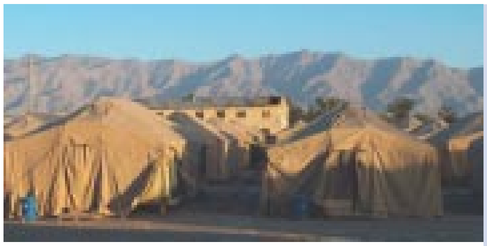
Kevin Morse, third from left, PMA-241's deputy assistant program manager for logistics, joins U.S. Army Special Forces and Afghanistan coalition force members in Kabul. Morse went to Afghanistan in June to establish connectivity between Army Special Forces and Navy tactical aircraft.

The need for such a capability was identified by an F-14 aviator from Carrier Air Group 7 who was on a one-month assignment with the intelligence center at the Army Air Base in Bagram. He saw that the Special Forces group in the Kabul area were not getting imagery intelligence as quickly as they needed. He recognized the challenge and knew who could meet it. The original request for support came to PMA-241 May 20, and the program office had the Navy and Army exchanging images by June 22.

"This is just one example of NAVAIR using its advanced warfighting capabilities to solve the problems of modern warfare," Williams said. "Working hand-in-hand with the Army against al Qaeda forces, PMA-241 demonstrated the value of network centric warfare capability in a real-time theater of operations." Morse left for Afghanistan on June 12. He located the equipment, made the necessary connections, and trained the Army Green Berets on how to use FTI laptops to communicate with Navy F-14 squadrons VF-143 and VF-11. "The special forces were not getting any near real-time imagery from tactical aircraft in the theater of operations," Morse said. "FTI enabled the F-14 crews to transmit images to ground troops within two minutes."

This is a two-way communication system that lets ground troops send images back to the Tomcats. This capability is also compatible with the Army's AH-64 Apache helicopter and FTI is expected to be used on the F/A-18E/F Super Hornet. "The Tomcat is mature, but it's still leading the way with new technology and it's setting the stage for the Super Hornet," Williams said. "We are helping to establish requirements in the spiral development of the Super Hornet." FTI was first used during operation Southern Watch in 1999. It allowed aircraft to launch from a carrier without a predetermined target, acquire a target, transmit imagery back to the ship and get permission to strike during flight. "This capability represents the highest standard in warfare technology," Williams said. "Our mission is to enable absolute combat power through technologies that deliver matchless capabilities."

Meeting these high standards and delivering superior technology is no small feat, but doing it in a third world country during a war presents unique challenges. A former Army Ranger, Morse is no stranger to hazardous and primitive conditions, but what he experienced in Afghanistan was unlike anything he had ever seen. He spent three weeks living in a tent with camel



Kevin Morse, PMA-241's deputy assistant program manager for logistics, and two contractor support personnel spent about three weeks in Afghanistan staying in tents like these at the Army Air Base in Bagram.

spiders the size of a hand in temperatures exceeding 106 degrees at 5,000 feet — where dust storms were a part of daily life. A harsh climate, however, was not the only challenge Morse faced. It took more than a week to locate the equipment after it arrived in Afghanistan and European electrical connectivity presented other problems.

Morse overcame these obstacles and gave his first briefing on FTI to the Green Berets in a bombed-out building in Bagram. He used a projector to show the presentation on a wall the team painted white so that the slides could be seen. Windows were covered with boards to block the light.

"It was a really bad place to be with a lot of people going through a lot of hardships," Morse said. "But, it was very rewarding to know I was doing something in support of the war against terrorism."

"It was a really bad place to be with a lot of people going through a lot of hardships," Morse said. "But, it was very rewarding to know I was doing something in support of the war against terrorism." The Army will continue to use Navy assets to collect imagery. While Morse was in Afghanistan, PMA-241 sent contractor support personnel from Signal Corporation to Fort Bragg to provide FTI training for another Army division preparing to leave for Afghanistan.

"The special forces were very grateful for the help we provided in performing their mission," Morse said. "There was no separation between Navy and Army — we were just Americans working together."

NASA Tests New Helmet Developed at NAVAIR

A pilot at NASA's Dryden Flight Research Center in Edwards, Calif., prepares for a flight test in an F/A-18 Hornet with the new two-part helmet concept developed by NAVAIR engineers in the Crew Systems Research and Engineering Competency Program. Photo courtesy of NASA.

By Renee Hatcher

Engineers from NAVAIR's Crew Systems Research and Engineering Competency Program (AIR-4.6), have developed a new helmet concept that they expect will enhance the stability and reliability of helmet mounted devices, ultimately improving the accuracy of information available to the aircrew on Navy and Marine Corps aircraft.

In July, pilots began wearing the modular, two-part helmet prototype during limited flight testing in an F/A-18 Hornet at NASA's Dryden Flight Research Center in Edwards, Calif. The helmet will be fully flight-qualified by the Navy before it can be transitioned to the warfighter through NAVAIR's Aircrew Systems Program Office (PMA-202). Continually evolving operational requirements for the Navy and Marine Corps call for a variety of helmet-mounted devices. These technologies often pose significant challenges in terms of aircrew systems safety, comfort and acceptability. Dr. James Sheehy is leading NAVAIR's Aircrew Systems Science and Technology Program effort to provide a stable platform to support the expanded range of helmet-mounted devices. The two-part helmet concept, originated by the Gentex Corp., was adopted and further developed by the Navy to meet the specific requirements of the warfighter. "It is lightweight, comfortable and stable," Sheehy said. "The helmet is easily adaptable to outer mission modules including the basic tactical outer helmet assembly recently flown in the F/A-18."

An F/A-18C Hornet assigned to Strike Force Squadron Two Five (VFA-25)— the "Fist of the Fleet." U.S. Navy photo by PHA Philip A. McDaniel.

Advanced materials, new suspension techniques, and precision fitting enable the two-part helmet to outperform current helmet technology. The inner helmet assembly is "eye-referenced" which means it is individually fit to each pilot to ensure that his or her eye is always in the proper location for the outer modules. The outer helmet is a shell that can be tailor-made to fit various missions and can range from a plain helmet for impact protection to a high resolution helmet mounted display. The ability to split the protection between the inner and outer modules allows the helmet to cross platforms between rotary and fixed wing aircraft.

"Providing the required tactical capability while preserving and advancing aircrew safety and protection is an extremely important objective," Sheehy said. "As the ultimate technology provider to the warfighter, our mission is to enable absolute combat power through technologies that deliver matchless capabilities."

Using Technology to Provide Better Support for the Federal Workforce

By Sandra J. Smith

The world of e-Government is full of exciting possibilities for how the U.S. Government can improve its interactions with its citizens. Concepts like one-stop shopping, online town hall meetings for direct contact with officials, or "OurTown.Gov" (which helps local leaders to coordinate community services) give new meaning to the phrase "of the people, by the people, and for the people." In the future, it seems almost inevitable that citizens and businesses will conduct more and more government interactions online. The transformations resulting from e-Government will continue to impact every facet of our lives, especially those of government employees. Training, recruitment, clearances, payroll, enterprise human resource system integration, and career planning are areas that are changing to provide better service and resources to government employees.

The nearly ubiquitous nature of the Internet affords a tremendous opportunity for agencies and communities alike to leverage and transform their operational procedures and processes. One such community benefiting from the Internet is the Federal Human Resources (HR) Community. As the Internet and Web-based services continue to marshal efficiencies and improve organizational processes, government employees will become the beneficiaries of the transformational power of e-Government.

The mandate of the President's Management Agenda to strategically manage human capital has helped to serve as a catalyst for the HR Community to examine how they conduct business and highlights them as a model for other agencies as they pave inroads into e-Government. A few key HR-related e-Government initiatives (shown in Figure 1) being led by the Office of Personnel Management (OPM) currently underway are:

e-Training

The Government Online Learning Center or, GoLearn is a Government-wide resource that supports developmental opportunities of the Federal workforce through simplified and one-stop access to high quality e-Training products and services. The creation of this center is the first phase of the President's Management Agenda e-Training Initiative and will continue to grow with the addition of products and services that meet the common needs of the workforce, including a competency-based individual career planning tool called the Information Technology (IT) Roadmap. The IT Roadmap will be a valuable tool for IT professionals and their managers to identify the right skills for optimal job performance and at the same time target professional development needed to obtain those skills. This site is designed as a virtual campus that houses free training courses and knowledge resources in each of its rooms. You can explore the center and all that GoLearn has to offer by going to www.golearn.gov.

e-Clearance

Security has taken on a greater significance since 9-11; now more than ever information security is crucial. The e-Clearance initiative will improve the processing of investigations for personnel who must have security clearances. The elimination of paper-based security applications will permit sharing of clearance information among other agencies, and accelerate the clearance process. The OPM e-Clearance project team expects the e-Government initiative to meet its next milestone early.

Office of Management and Budget (OMB) Director, Mitchell E. Daniels Jr., recently sent a memo to agencies requiring them to automate their security clearance systems and transfer employee files to OPM's Security/Suitability Investigations Index (SII) by Jan. 3, 2003. The memo is the latest in a recent series of letters invoking OMB's authorities under the Clinger-Cohen Act to prompt agencies to work together on e-Government initiatives.

Recruitment One-Stop

A significant challenge for government agencies is the difficulty in attracting and retaining skilled IT professionals. Despite the recent economic downturn, the private sector demand for IT workers — fueled by the Internet "gold rush" — continues to grow at a rate faster than the supply of newly educated IT professionals. In an attempt to simplify the government recruiting process and provide a one-stop approach to federal employment applications and job postings, OPM conducted a virtual IT fair for individuals interested in working in the Federal Government. The job fair was intended for positions in the GS-2210 IT Management Specialist series at the GS-7 through 13 grade levels. Approximately 20 Federal agencies participated in this first of its kind event which was held in April 2002. The entire application and assessment process was administered via the Internet at www.usajobs.opm.gov.

EHRI

The goals of the e-Government Enterprise Human Resources Initiative (EHRI) are to provide timely and accurate access to human resources data and deliver accurate, current data on all Federal employees — active and separated. EHRI will eliminate the need for a paper employee record through the creation of an electronic Official Personnel Folder that will eliminate more than 100 multiple forms that are currently maintained for a minimum of 65 years after employee separation. This initiative will enable the management of reporting benefits and electronic transfer of HR data throughout a Federal employee's career life cycle. These enhancements will fundamentally change the way in which employees, managers, and HR officers retrieve and use Official Personnel Folder data for transaction processing, workforce reporting and analysis. The Department of Defense has funded the Modern Defense Civilian Personnel Data System (DCPDS) to achieve the majority of the EHRI goals, and will eventually be funded to develop an interface with the EHRI.

The Modern DCPDS currently supports multiple HR applications and is designed to replace a number of information systems used today, throughout the Department, to manage civilian human

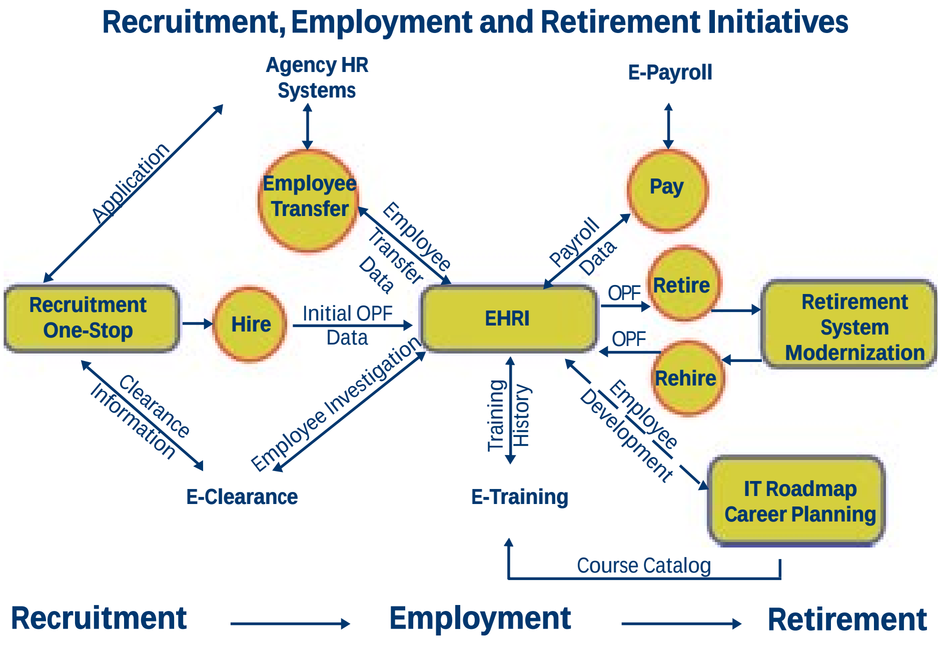


Figure 1.

resources. The Modern DCPDS will move the Department away from multiple systems to a single information system for civilian employees.

e-Payroll

OPM has established a Standardization Action Team, with officials from various Departments. The team's goal is to provide simple, easy-to-use, cost-effective, standardized, integrated HR/Payroll services to support the mission and employees of the Federal Government. The team developed a modernization plan using agency and industry best practices to identify data fields needed for payroll processing. The group also is identifying the methods for making changes, whether legislatively or through the regulatory process.

The Federal IT Roadmap

Recognizing the criticality of a skilled IT workforce, the Federal Chief Information Officer Council (CIOC) engaged OPM in the development of the Information Technology Group, GS-2200. Under this standard, the GS-2210, Information Technology Management Specialist series with 10 parenthetical titles was developed. As a follow-on thrust, the Federal CIOC, Workforce and Human Capital for IT Committee, sponsored the IT Roadmap initiative as a means to engage and provide a developmental resource for the Federal IT Workforce. The IT Roadmap Team spent several months exploring best practices within private and public sector products and recommended a way ahead in developing such a tool. After extensive review, the Roadmap Team recommended adopting the Department of the Navy Chief Information Officer (DON CIO) Career Planning Tool as a best practice.

The Committee adopted the recommendation and launched an effort to develop the IT Roadmap — a Federal career planning tool for current and prospective Federal IT employees. The tool is a Web-enabled, database-driven career planning tool that outlines general and technical competencies relevant to the various parenthetical titles (Policy & Planning; Information Security; Systems Analysis; Application Software; Operating Systems; Network Services; Data Management; Internet; Systems Administration; and Customer Support) associated with the GS-2210, IT Management Specialist Series.

The GS-2210 series is designed to cover all positions currently assigned to the Computer Specialist Series, GS-334, as well as positions classified in other series (e.g., the Telecommunications Series, GS-391, and the Miscellaneous Administrative and Program Series, GS-301), where IT knowledge is paramount. The tool will assist individuals in performing self-assessment of their proficiency in those competencies. Based on identified proficiency gaps, the IT Roadmap will assist users in developing career-long training and development plans to achieve their career goals. The career development plan will be derived from the user's self-assessment of competencies and the selection of professional development opportunities. Professional development opportunities will come from a compendium of federal training sources that are directly linked to one or more specific competencies. The IT Roadmap will provide an integrated approach toward training and career development, identify competencies required for successful job performance, and be flexible enough to support a variety of IT career development planning strategies and customization. The tool will include feedback from employees on courses and provide a source of aggregate statistics for agency planning. The prototype of the tool was released early December 2002 and initial operational capability is projected by spring 2003.

A Winning Proposition

An exciting future awaits the workforce of the future. Not only will systems and procedures be greatly enhanced by technology but the people who manage and implement those systems and procedures will be better equipped and more competent to do their jobs. President Bush has said that he will expand the use of the Internet to empower citizens by allowing them to request customized information from Washington when they need it, not just when Washington wants to give it to them. The President believes true reform involves not just giving people information, but giving citizens the freedom to act upon it. The DON CIO supports e-Government initiatives and believes they are winning propositions for using technology to gain efficiencies and provide better support for the DON and Federal Workforce of the future.

To learn more about e-Government go to:
www.gcn.com/egovernment
www.golearn.gov
www.egov.gov
www. senate.gov

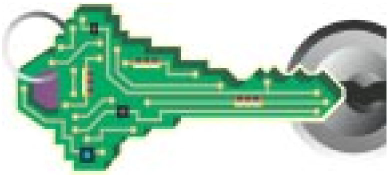
Sandra J. Smith is the DON CIO Competency Management Team Leader.

Security Made Easy with the NMCI, PKI, and the CAC

By Josephine Smidt with Rebecca Nielsen

The National Information Systems Security (Infosec) Glossary defines the following five security services. PKI provides all but authorization.

- *Authentication: Establish the validity of a transmission, message or originator.*
- *Authorization: Access privileges granted to a user, program or process.*
- *Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes or devices.*
- *Data Integrity: Data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.*
- *Non-Repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.*



You have heard of the Navy Marine Corps Intranet (NMCI), the Department of Defense (DoD) Public Key Infrastructure (PKI), and the Common Access Card (CAC). You may even have heard about Public Key Enabled (PKE) applications. Here at the Department of the Navy Chief Information Officer (DON CIO), these aren't abstract concepts. They are woven into daily workplace activities, ensuring that DoD Defense in Depth information assurance requirements are met. One of the benefits of working in my office is that we test the technology that will be deployed to the DON community. This is both good and bad: we use all the cool, new technology, but we have to work out the bugs prior to deployment.

I'll explain how implementation of the new PKI technology has helped me do my job better as a member of the Information Assurance Team at DON CIO. The PKI provides digital certificates to subscribers — people and computer systems. Digital certificates and their associated keys are credentials, similar to photo identification. Unlike a photo ID, however, digital certificates can also be used for electronic signatures and encryption — assuring secure communications between users. By itself, PKI doesn't do anything. However, the security services that PKI provides: authentication, data integrity, confidentiality, and non-repudiation (described in the text box above), transform time-consuming, insecure paper processes into streamlined, secure electronic systems. Applications like e-mail and the Defense Travel System (DTS), that are programmed to use digital certificates are PK Enabled.

Like any credential, my digital certificates are only useful if I have them when I need them. So, I carry them with me on my CAC. The CAC contains a small chip (almost as powerful as the first personal computers) that not only contains my certificates and associated keys, but also the processing power to use the keys and to protect them from unauthorized disclosure. The CAC also has other technologies, including a photo (for visual identification), a magnetic stripe and a bar code. Since all of these are on the same card, I will soon only have to carry one card and remember one password — the one that tells the computer chip that I am the authorized user. There is an icon at the bottom of my screen that changes color when my CAC is being used to verify or authorize something. This is especially helpful, when your workstation seems to take longer than usual to do something, as the verification process sometimes takes a couple of seconds.

I use my CAC and PKI on a daily basis. My office has recently been designated as classified, and as a result, we decided to test how easily the CAC can work with biometrics to enter the secure area. When I arrive in the morning, I swipe my CAC and put my thumb on the reader and the door opens. Right next to the reader that we currently use is one that we will be using in the not-too-distant future. This reader doesn't require swiping, but reads my CAC from the chain around my neck as I press my finger. How cool is that?

Our office has not switched over to NMCI yet, but we have been using the CAC to log on to the network — the CAC contains our userid and password. Some personnel use PKI to log on by inserting the CAC into a card reader located on the side of their laptop and typing in the CAC Personal Identification Number (PIN). The chip on the card communicates with PKE Microsoft Windows 2000 to authenticate the identity certificate. Since the PIN is useless without the card, they don't even have to change it every 90 days. We will all be using this method when we switch over to NMCI.

I digitally sign each e-mail I send so that the recipient will know that the e-mail came from me, and that the contents have not changed since I sent it. The NMCI workstation comes with both Outlook and the middleware needed for Outlook to work with the CAC. All I have to know is the PIN. Someone who wants to send me an encrypted e-mail, either can retrieve my e-mail encryption certificate from the Global Address List or from a signed e-mail I have already sent. This certificate can encrypt information that is sensitive and should not be sent in a manner that allows anyone to read it. When I receive an encrypted e-mail, Outlook communicates with my CAC to decrypt the information.

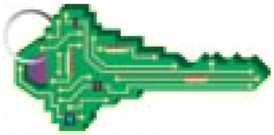
Since I used the CAC to log onto the workstation, if I have to step away from my desk, all I have to do is remove the CAC from the reader and my desktop is automatically locked so that no one else can access it. When I return, I put the card back into the reader and enter my PIN to return to where I left off. Since unattended workstations are not secure, and security is a primary concern, I really like this feature. Even if I forget to take my CAC out of the reader, my screen saver will kick in after fifteen minutes and I'll need both my CAC and my PIN to return to the desktop (since I need the CAC to get into my office, I try not to forget and leave it in the reader).

E-mail isn't the only application that is PKE. I use PKI to submit travel requests and process travel claims using DTS. Once I have filled out my travel voucher, I digitally stamp it. This is the equivalent of digitally signing an e-mail, and I can't do it without my CAC. I click on the button that says stamp, and the CAC and the PK Enabled DTS work together to verify who I am and to encrypt my authorization or voucher. Since the process is electronic, there are no paper forms to get lost and my reimbursement is sent directly to my bank account in about one week.

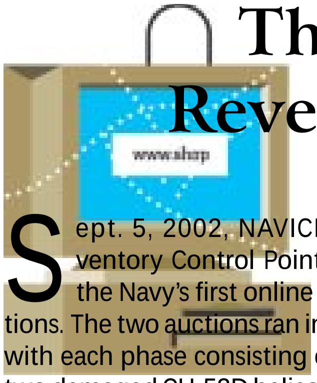
When I am on travel or working from home, I can use my CAC and my NMCI laptop for remote access to the network. I log on just as I would at work with my CAC in the card reader and dial in. The communication between my workstation and the network remote access server validates my identity, verifies that I am permitted to access the network, and establishes an encrypted communication link — all based on my identity certificate.

When I think about how many passwords I had to remember, how long it would take to get a travel authorization approved/reimbursed for travel expenses and, how it was not even possible to encrypt my e-mail outside of the SIPRnet, it hits me just how much this little card has simplified my daily work life. Not to mention how it will continue to influence my work in the future, with things like contact-less CACs (where I don't swipe the CAC, but it is read from a distance); using my CAC to send signed e-mails with my Blackberry and, using a variety of applications from personnel management software to financial programs and not having to remember a different password for each.

While technology is never a substitute for security awareness, the implementation of NMCI, PKI and the CAC show how implementation of robust security can make our jobs easier. It is definitely a very exciting time to be in the DON.



Josephine Smidt is a Management Analyst on the DON CIO IA Team.



The Navy's Web-based Reverse/Forward Auction

By Cmdr. Steve Dollase, SC, USN

Sept. 5, 2002, NAVICP (Naval Inventory Control Point) conducted the Navy's first online forward auctions. The two auctions ran in two phases, with each phase consisting of the sale of two damaged CH-53D helicopters and associated parts packages. Three firms registered to participate as bidders. The winning bidders are expected to refurbish the aircraft for commercial applications such as firefighting, a requirement that has generated significant demand for heavy lift aircraft in the past few years. The two contracts resulting from the auctions are valued at nearly $5 million. Naval Air Systems Command (NAVAIR) will receive the aircraft proceeds and NAVICP will retain the remaining proceeds to purchase similar helicopter parts.

The forward auctions, leverage the latest commercial technology and are part of NAVICP's innovative strategy to reduce U.S. Navy excess inventory, which consists of weapons system parts that the Navy might need later, but will most likely replace with state-of-the-art designs. The auctions also create a commercial marketplace for future sales. In fact, both of the winning bidders will have the option to buy additional CH-53D helicopters and parts within six months of contract award. This creative initiative allowed NAVICP to transform unusable assets that might otherwise deteriorate — into funding to support the next generation of weapons systems.

The forward auctions are the latest success story in NAVICP's Internet-based action program. In May 2000, NAVICP conducted the first Internet-based reverse auction in the Federal Government. The auction, which lasted 51 minutes, provided the competitive pricing mechanism for NAVICP to award a contract for aircraft ejection seat recovery sequencers (the "brains" of the ejection seats). The auction saved an estimated 28 percent from the historical price for recovery sequencers. NAVICP awarded the contract within an hour of the auction closing — a significant time savings.

NAVICP conducted four additional auctions under the pilot reverse auction program, resulting in estimated savings of 21 percent, or $14.8 million. Internet-based reverse auction technology allows online bidders to compete in real-time for contracts by lowering their price offers (or raising them in a forward auction) as they see other bids posted. Bidders are unable to identify competitors, only the current low bid is visible. The auctions are conducted in a secure, Web-based environment. Participants are screened in advance before granting access to the auctions to ensure that they are qualified sources for the items under consideration. This is particularly important with complex weapons systems. Auctions work best when there are three or more bidders, and when specifications permit easy comparison between products.

Convinced of the power of the concept, NAVICP, with the sponsorship of its parent command, the Naval Supply Systems Command (NAVSUP), awarded two five-year, best-value contracts for auction services; one to Procuri for a self-service, desktop tool and the other to eBreviate for a full-service tool. The eBreviate solution also offers market research services, helpful in determining suppliers for a particular requirement. In the first year, NAVICP contracts were used by NAVSUP activities and twelve other Federal Government agencies to conduct 43 auctions valued at over $144 million with typical savings of 8 to 24 percent. The auction tools are available, free of charge, to Navy and Marine Corps activities, and to other Federal Government activities on a fee-for-service basis.

The NAVSUP/NAVICP Reverse Auction Team earned a FY 2000 Department of the Navy Competition and Procurement Excellence Award for their success. NAVSUP/NAVICP recently launched a Navy auction Web site at **www.auctions.navy.mil**. These tools are just one more way that the Navy and Marine Corps team can maximize resources and improve combat readiness.

Cmdr. Steve Dollase is NAVICP's Director of Acquisition Policy.

CAC Middleware... Putting the CAC to Work for Information Security

By Tim Russell

As of July 2002, more than one million Department of Defense (DoD) users have been introduced to the Common Access Card (CAC) — the DoD's new standard identification and benefits card that provides active duty and selected Reserve, civilian and contractor personnel with physical access to buildings and secure areas, and authentication for accessing computer networks. While the card represents the most tangible element of the CAC program and the part most visible to DoD personnel, the software that functions to support a user's CAC card on PC workstations is an equally vital part of the equation, even though many users don't realize it or might not even know it's there. But without software, the CAC card can't perform the secure logical access applications for which the card is intended. This August, Datakey was notified, along with three other vendors (Schlumberger, SSP-Litronic and Spyrus), that it had been selected as an approved supplier of middleware for the DoD CAC program.

Working jointly under a partnership agreement with the National Institute of Standards and Technology (NIST) on behalf of DoD agencies, Datakey electronic memory key technology was revised and reengineered to develop a prototype secure token for computer workstation authentication in 1989. Based on this secure token, Datakey manufactured the first cryptographic Smart Card used for digital signatures in 1991. Former President Clinton used Datakey technology on two occasions while in office — to digitally sign an intergovernmental agreement with Ireland in 1998 — and to sign the Electronic Signatures in Global and National Commerce Act (E-SIGN), legislation that took effect Oct. 1, 2000, making electronic signatures as legally valid as signatures on paper in the United States.

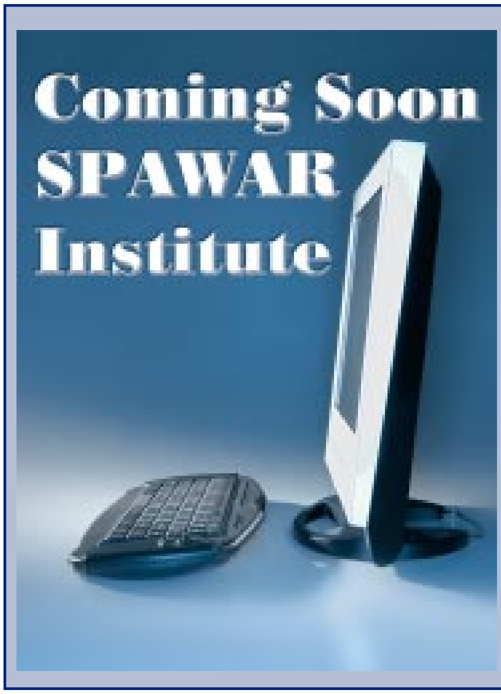
Datakey began developing a version of software specifically engineered for the CAC program following the specification requirements, and implemented PKCS #11, MS-CAPI and the DoD-defined Basic Services Interface (BSI), allowing users to take advantage of *any* DoD CAC card to run their information security applications, including encrypted and digitally signed e-mail, VPN access and PC login applications. Beyond supporting all on-card cryptographic operations, Datakey CAC middleware also includes its supporting software library to perform a complete range of cryptographic operations in software. The middleware provides users with the utilities that are necessary to manage their Smart Card, including a PIN manager, the ability to view digital credentials, and the ability to register certificates within Microsoft environments. Datakey CAC middleware can also be field-enabled to support the full list of current Datakey Smart Card/token options, including all configurations of its Model 330 cryptographic Smart Card, for seamless integration with leading PKI and VPN products.

Datakey also provides GSA-ready Smart Card technology for the Smart Access Common ID Card program. Government customers who have deployed Datakey Smart Card technology include: (1) The Department of State - 40,000 Diplomatic Security users will carry a Smart Card for facility access to DoS buildings and embassies and for secure network access. In addition to security, benefits include increased efficiencies and user productivity. Personnel can access corporate networks by using the same ID card that grants physical access to buildings. By using a single ID card for many applications and uses, the Department leverages its investment for the greatest possible return on investment. Old paper processes and applications can be securely transitioned online for time savings and 24x7 availability; (2) The Federal Deposit Insurance Corporation - 3,500 field agents and more than 7,000 internal users digitally sign/encrypt e-mail messages and documents, and access corporate facilities. FDIC field agents use an Electronic Travel Voucher (ETV) System application with Smart Cards and laptops for reimbursement of travel expenses. The electronic system interfaces with the National Finance Center (NFC). Previously, it took up to two months for field employees to be repaid, but by using Smart Cards it now takes two days for a direct deposit to an employee's account. The paper reimbursement costs about $50 per transaction to process, whereas the new process costs less than $10. Since the FDIC processes 80,000 to 100,000 vouchers every year, this results in savings of about $3.2 to $4 million. Due to the success of the ETV pilot program, the FDIC has expanded the program to a fully operational, ongoing cryptographic Smart Card endeavour. Other customers using Smart Card technology include: the Department of Energy, Rocky Flats Environmental Technology Site, the Bureau of Labor Statistics and the Canadian Department of National Defence, which deployed 90,000 Smart Cards.

As more and more DoD users (up to 4 million) receive the CAC card, the missing link is the software required to put the card to work in information security applications (secure network access, digitally signed and encrypted e-mail, etc.,). Datakey CAC middleware bridges that gap and enables a powerful, interoperable and CAC-compliant solution that works with any CAC-compliant Smart Card. Through Datakey's contract with the government, any DoD organization can order Datakey middleware and begin taking full advantage of the CAC card.

For more information on CAC Middleware contracts visit the DON IT Umbrella Web site at www.it-umbrella.navy.mil or the DoD ESI site at www.don-imit.navy.mil/esi. DoD organizations can order Enterprise Software Initiative (ESI) CAC Middleware directly from the DON Web site, ITEC-Direct, at www.itec-direct.navy.mil or by contacting a Datakey representative at 1-888-328-2539 or 1-301-261-9150 in Washington, D.C.

Tim Russell is vice president and general manager of Datakey Inc.



SPAWAR Systems Center Charleston Technology Training Center Norfolk is undergoing an exciting revitalization with a focus on arming the warfighter with 21st century technology. The transformation will result in the standup of SPAWAR Institute — delivering C4ISR training solutions. We are enthusiastically looking forward to meeting the training demands of the 21st century warrior and exceeding expectations for quality, service and professionalism.

With opportunity comes change, the popular column, "How Can I" by the training team of SPAWAR Systems Center Charleston Technology Training Center Norfolk will be phased out. Through the years many Information Technology users have come to depend on the expert advice the training team has shared, but it is time to move in a fascinating new direction to meet the warfighter's requirements with right on target C4ISR training. SPAWAR Institute will partner with Navy trainers and customers to bridge the gap between informal SPAWAR installation training and formal schoolhouse instruction. This nontraditional, integrated approach will provide timely and flexible C4ISR training to meet today's shipboard requirements.

Thanks to the following SPAWAR Systems Center Charleston Technology Training Center Norfolk instructors for their input: Alice Butler, Ronald Bailey, Katie Bierman, Gregory Browning, Colleen Jobe, Glynda Roffman and Muriel Taylor. Some of their most recent inquiries are listed below. If you would like further information or have questions, please call (757) 444-7976, DSN 564 or e-mail to forinfo@spawar.navy.mil. Visit their Web site at www.training.norfolk.navy.mil

Microsoft Access

QUESTION: Is there a way to create a shortcut on the desktop that will open Access, open a specific database and open a form?

ANSWER: Open the database. Use **Tools ... Startup** to set the opening form. Make a desktop shortcut to the Access database. When you click on the shortcut, Access will open the correct database and the selected form.

QUESTION: What should you do when you set the database to open to a form and want to then gain access to the other objects in the database?

ANSWER: Hold the shift key while opening the database to bypass any start-up settings.

Microsoft Outlook XP

QUESTION: I lost the envelope that pops up when you get new mail. How do I get it back?

ANSWER: To restore the Envelope icon in your system tray follow the steps below.

- Start Outlook.
- Click the **Tools** menu, Select **Options**.
- On the **Preferences** Tab, Click **E-mail Options**.
- Click **Advanced E-mail Options**.
- Check to select the **Show an envelope icon**.

Microsoft PowerPoint

QUESTION: How can I change things that are the same color in a piece of clip art into a variety of different colors?

ANSWER: To get pieces of the clip art to each be a different color, **double-click** the piece of clip art - click "**yes**" to convert to a Microsoft Office drawing object (this will ungroup the image) - **left click** outside of the image to deselect it - **double-click** on any piece you would like to recolor - **click** the drop down list to change the fill color - **regroup** the image when you're finished.

In order to regroup, click on each part of the image using both the shift and control keys until all pieces of the image have been selected. Then, right click on the image and choose the Grouping option and then Group.

Tip You can keep ungrouping and regrouping the image as often as you like to change the colors.

SPAWAR Institute

...C4ISR Training Solutions for the 21st Century Warfighter

The SPAWAR Institute provides professional instructors in Integrated Battle Force, Advanced Systems Training, Network Essentials, Unix Operating Systems, Microsoft Systems Engineer, A+ Certified Professional and Network + Certified Professional. SPAWAR Institute provides Curriculum Development services including requirements validation,training objectives development, alignment with governing standards and directives, curriculum production and delivery, and metrics for evaluation and modification based on student feedback. SPAWAR Institute delivers eLearning tools such as Computer Based Training and Web-enabled modules for C4ISR systems.

We can design customized training solutions for every requirement.

SPAWAR Intitute Services

Integrated Battleforce Training
Advanced Systems Training
Afloat Training Teams
Curriculum Development
eLearning Resources

757.444.4945
DSN 564.4945

Located Near Our Fleet Customers
on the Norfolk Naval Station

ViViD Contracts
N68939-97-D-0040
Contractor: Avaya Incorporated

N68939-97-D-0041
Contractor: General Dynamics

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

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

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

Modifications

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

Ordering Information

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

Authorized users: DoD and U.S. Coast Guard

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

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

Web Link

http://www.it-umbrella.navy.mil/

TAC Solutions BPAs
Listed Below

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

Compaq Federal, LLC (N68939-96-A-0005); (800) 727-5472

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

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

GTSI (N68939-96-A-0006); (800) 999-4874, ext. 2549

Hewlett-Packard (N68939-97-A-0006); (301) 258-2063

McBride and Associates, Inc. (N68939-96-A-0007); (800) 829-9409, ext. 7612

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

Ordering Expires: Indefinite with annual review for all BPAs.

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

Warranty: IAW GSA Schedule. Additional warranty options available.

Web Link

http://www.it-umbrella.navy.mil/contract/tac-solutions/tac-sol.html

Enterprise Software Agreements
Listed Below

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

In September 2001, the ESI was approved as a "quick hit" initiative under the DoD Business Initiative Council (BIC). Under the BIC, the ESI will become the benchmark acquisition strategy for the licensing of commercial software and will extend a Software Asset Management Framework across the DoD. Additionally, the DAR Council has approved a final rule which will incorporate the ESI into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74.

Authorized ESI users include all Defense components, U.S. Coast Guard, Intelligence Community, and Defense contractors when authorized by their contracting officer. For more information on the ESI or to obtain product information, visit the ESI Web site at http://www.don-imit.navy.mil/esi.

ASAP (N00039-A-9002) for Novell products; and (N00104-02-A-ZE78) for Microsoft products; Small Business; (800) 883-7413 for Novell products and (800) 248-2727, ext. 5303 for Microsoft products

GTSI (N00104-00-A-Q242) for JetForm products; and (N00104-02-A-ZE79) for Microsoft products; Small Business; (800) 999-GTSI

Crunchy Technologies, Inc. (N00104-01-A-Q446) for PageScreamer Software (Section 508 Tool), Crunchy Professional Services and Training; Small Business Disadvantaged; (877) 379-9185 or (703) 469-2010

CorpSoft, Inc. (N00104-01-A-Q506) for Adobe products; and (N00104-02-A-ZE82) for Microsoft products; Call (800) 808-1944 for Adobe products and (800) 677-4009, ext. 5248 or (781) 440-1000 (OCONUS) for Microsoft products

HiSoftware, DLT Solutions, Inc. (N00104-01-A-Q570) for HiSoftware Section 508 Tools; Small Business; (888) 223-7083 or (703) 708-9658

SAP Public Sector and Education, Inc. (N00104-02-ZE77) for SAP software, installation, implementation technical support, maintenance and training services; (610) 661-5711

Softchoice (Beyond.com) (N00104-02-A-ZE81) for Microsoft products; Small Business; (877) 804-4995, ext. 305

COMPAQ (N00104-02-A-ZE80) for Microsoft products; (800) 535-2563 pin 6246 or (317) 228-3424 (OCONUS)

DELL (N00104-02-A-ZE83) for Microsoft products; (512) 723-7010

Softmart (N00104-02-A-ZE84) for Microsoft products; (610) 518-4000, ext. 6492

CDW-G (N00104-02-A-ZE85) for Microsoft products; (703) 726-5011

Software House International (N00104-02-A-ZE86) for Microsoft products; Small Business Disadvantaged; (301) 294-9439

Datakey (N00104-02-D-Q666) IDIQ Contract for CAC Middleware products; (301) 261-9150

Litronic (N00104-02-D-Q667) IDIQ Contract for CAC Middleware products; (703) 905-9700

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

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

Ordering Information

Ordering Expires:

Microsoft products: 26 Jun 03
Novell products: 31 Mar 07
JetForm products: 23 Feb 03
Crunchy products: 04 Jun 04
Adobe products: 14 Aug 03
HiSoftware products: 16 Aug 04
CAC Middleware products: 06 Aug 05
SAP products: Upon expiration of the GSA schedule

Authorized Users: Adobe products, Microsoft products, Section 508 Tools, CAC Middleware and SAP: All DoD. For purposes of this agreement, DoD is defined as: all DoD Components and their employees, including Reserve Component (Guard and Reserve) and the U.S. Coast Guard mobilized or attached to DoD; other government employees assigned to and working with DoD; non-appropriated 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.

JetForm: All DoD and U.S. Coast Guard (excluding Air Force and Army).

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

Web Links

ASAP Software Express
http://www.it-umbrella.navy.mil/contract/msesa/asap/asap.html

Government Technology Services, Inc. (GTSI)
http://www.it-umbrella.navy.mil/contract/msesa/gtsi/gtsi.html

CorpSoft, Inc.
http://www.it-umbrella.navy.mil/contract/adobe/adobe.html

Crunchy Technologies, Inc.
http://www.it-umbrella.navy.mil/contract/508/crunchy/crunchy.html

HiSoftware, DLT Solutions, Inc.
http://www.it-umbrella.navy.mil/contract/508/dlt/dlt.html

SAP
http://www.it-umbrella.navy.mil/contract/enterprise/sap/sap.html

Microsoft Products
http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.html

Datakey, Inc.
http://www.it-umbrella.navy.mil/contract/middleware-esa/datakey/index.html

SSP-Litronic, Inc.
http://www.it-umbrella.navy.mil/contract/middleware-esa/litronic/index.html

Schlumberger
http://www.it-umbrella.navy.mil/contract/middleware-esa/Schlumberger/index.html

Spyrus, Inc.
http://www.it-umbrella.navy.mil/contract/middleware-esa/spyrus/index.html

Navy Contract: N68939-97-A-0008
Department of the Navy Enterprise Solutions BPA

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

Computer Sciences Corporation (CSC) (N68939-97-A-0008); (619) 225-2412; Awarded 07 May 97; Ordering expires 31 Mar 06, with two one-year options

Authorized Users: All DoD.

Web Link

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

Information Technology Support Services BPAs
Listed Below

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

Booz Allen Hamilton Inc. (N68939-97-A-0014); (415) 281-4942; Awarded 02 Jul 97; Ordering expires 31 Mar 04

Lockheed Martin (N68939-97-A-0017); (240) 725-5950; Awarded 01 Jul 97; Ordering expires 30 Jun 05, with two one-year options

Northrop Grumman Information Technology
(N68939-97-A-0018); (571) 203-6114; Awarded 01 Jul 97;
Ordering expires 12 Feb 05, with two one-year options

SAIC (N68939-97-A-0020); (703) 676-5096; Awarded 01 Jul 97; Ordering expires 30 Jun 05, with two one-year options

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

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

Web Link

http://www.it-umbrella.navy.mil/contract/itss/itss.html

Navy Contract: N00039-99-A-3193
Networking Solutions BPA

The Networking Solutions contract provides access to significant discounts on Cisco networking products and solutions. The items include a large variety of ATM and Ethernet switches, edge devices and software. This Networking BPA is primarily intended for equipment purchases. Customers requiring total solutions or significant integration services should consider placing their order(s) using the ViViD Contracts. A BPA has been awarded to:

Federal Data Corporation (N00039-99-A-3193); (425) 793-3847

Ordering Expires: Indefinite with annual review for BPA

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

Warranty: IAW GSA schedule. Additional warranty and options available.

Web Link

http://www.it-umbrella.navy.mil/contract/net-solutions/fdc/fdc.html

Research and Advisory BPAs
Listed Below

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

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

Acquisition Solutions (N00104-99-A-Q150); (703) 378-3226; Awarded 14 Jan 00; one-year base period with three one-year options.

Ordering Expires:
Gartner Group: Nov 06
Acquisition Solutions: Jan 04

Authorized Users:

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

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

Web Links

From the DON IT Umbrella Program Web Site:

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

Acquisition Solutions
http://www.acqsolinc.com

TurboPrep Messaging Solution
N00039-00-C-3112
Contractor: Ice Communications

TurboPrep software for generation, preparation, validation and formatting of messages has been purchased by the SPAWAR Program Office for the DON Enterprise. No additional cost to authorized users. Order issued to:

Ice Communications, Inc. (N00039-00-C-3112 of Feb 00); Small Business; (703) 938-1465; Awarded Aug 00

Ordering Information

Ordering Expires: 14 Feb 03

Authorized Users: All DON and U.S. Coast Guard

Warranty: 3-year which includes software updates and upgrades.

Web Link

http://www.icecomm.com.

SEWP III
Listed Below

NASA's Scientific and Engineering Workstation Procurement III government-wide contracts provide Class 10 Computer Support Devices and Class 12 Security Systems and Tools. SEWP III is an indefinite delivery, indefinite quantity (IDIQ) type contract. Contracts have been awarded to the following:

Hewlett-Packard (NAS5-01133) and (NAS5-01141); (781) 505-7676

GTSI/SUN (NAS5-01134); (703) 502-2172

IBM (NAS5-01135); (800) 426-2255

Silicon Graphics Federal, Inc. (NAS5-01136) and (NAS5-01140); (301) 572-1980

GMR/Cray (NAS5-01138); (703) 330-1199

Compaq Federal, LLC (NAS5-01139); (301) 918-5360

GTSI (NAS5-01142) and (NAS5-01146); (703) 502-2172

Logicon FDC (NAS5-01143) and (NAS5-01147); (301) 446-3100

UNISYS Corporation (NAS5-01144); (800) 398-8090

Government Micro Resources (NAS5-01145); (703) 330-1199

Ordering Expires: 30 Jul 06 (Contracts awarded for five years starting 30 Jul 01.)

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

Warranty: 36-month extended warranty available

Web Link

http://www.it-umbrella.navy.mil/contract/sewp3/sewp3.htm

The U.S. Army Small Computer Program (ASCP) Maxi-Mini and Database (MMAD) Program
Listed Below

The Maxi-Mini And Database (MMAD) Program is supported by two fully competed Indefinite Delivery/Indefinite Quantity (ID/IQ) contracts with IBM Global Services and GTSI Corporation. The MMAD Program is intended to be DoD's follow-on to the Navy administered Supermini Program in fulfilling high and medium level IT product and service requirements. Like its predecessor, MMAD provides items to modernize, upgrade, refresh and consolidate current systems, as well as to establish new ones.

Products include:

64-bit Servers (RISC and Itanium): HP, IBM, Compaq
64-bit RISC and NT Workstations: HP, Compaq
Routers/Network: Cisco, 3COM
Storage Systems: IBM, RMSI, Compaq, Dot Hill, System Upgrade, EMC

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

Services are geared toward providing solutions needed to effectively manage and support the complexities of agency or program system environments, to include: consultants, analysts, engineers, programmers, trainers and administrators.

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

Latest product additions include EMC and McData storage solutions, and Tivoli Storage Manager software. Both IBM and GTSI now provide HP, Cisco and EMC products and services with MMAD terms and conditions.

Awarded to:

GTSI Corporation (DAAB07-00-D-H251); (800) 999-GTSI

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

Ordering Information

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

Ordering Expires:
GTSI: 24 May 06 (includes three option periods)
IBM: 19 Feb 06 (includes three option periods)

Authorized Users: DoD and other federal agencies including FMS

Warranty: 5 years or OEM options

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

No separate acquisition, contracting and technical fees.

Web Links

GTSI
http://pmscp.monmouth.army.mil/contracts/mmad_gtsi/mmad_gtsi.asp

IBM
http://pmscp.monmouth.army.mil/contracts/mmad_ibm/mmad_ibm.asp

The U.S. Army Enterprise Software Initiative BPA DAAB15-99-A-1002

As of February, 28, 2002, the Navy holds inventory of Oracle Database Enterprise Edition (9i and 9ias) perpetual licenses (either named-user, multi-server or processor), and additional options and tools (i.e., security options, partitioning, spatial, clustering, diagnostics management packs, Tuning Management Pack, Change Management Pack, Internet Application Server Enterprise, Internet Developer Suite, and Balanced Scorecard). Initial orders will include a warranty period of March 1 through May 31, 2002, and software support for the period June 1 through May 31, 2003. Placing orders early will result in the best deal for end users. Four (4) additional out years of Silver Technical Support and product update support have also been negotiated.

The initial purchase price for end users is an average of a 64 percent discount off GSA prices and total package discounts (including out year technical support) average a 70 percent discount off GSA prices. Customers with small requirements can benefit from discounts normally reserved for customers with orders over $10 million. These licenses can be distributed throughout the Navy. In accordance with the Federal Acquisition Regulations (FAR) and DoD policy, Navy customers who have selected Oracle to satisfy new requirements must purchase the "new" Oracle licenses from the inventory.

This virtual inventory was established through the Department of the Navy Chief Information Officer (DON CIO) Enterprise Licensing Team and the Department of Defense Enterprise Software Initiative (DoD ESI). The DoD ESI is a joint initiative, which has been approved by the DoD Business Initiative Council (BIC).

This inventory will be managed by the Department of the Navy Information Technology (DON IT) Umbrella Program Office at Space and Naval Warfare Systems Center, San Diego.

For complete contract information go to the DON IT Umbrella Program Web site at: www.it-umbrella.navy.mil

SPAWAR

Systems Center Charleston

Computer Services Division

Located Near Our Fleet Customers
on the Norfolk Naval Station

Information Technology Services
757.444.1808

Knowledge Delivery
757.444.4945

Network Services
757.444.6233

Technical Specifications and Acquisition
757.445.2576

Fully integrated C4ISR and computer solutions with professional expertise in C4ISR training; Project Management; Web software and hardware system development and integration; acquisition; NMCI transition support; installation and testing; Task Force Web; and much more . . .

Call the Business Manager for a Free Consultation
Voice 757.444.3873
Fax 757.444.4017

SPAWAR

Coming Soon
SPAWAR Institute
Call 757.444.4945
DSN 564.4945

...Enabling Knowledge Superiority for the Warfighter

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

PERIODICAL
POSTAGE AND FEES PAID
SSC CHARLESTON NORFOLK OFFICE
USPS 757-910
ISSN 1047-9988