Forging a 21st Century USN and USMC :

C4ISR D as a Key Element for 21st Century Power Projection Force

THE FUTURE OF POWER PROJECTION

REPORT 4

Forging a 21st Century USN and USMC : C4ISR D as a Key Element for 21st Century Power Projection Force

The crafting of a connectivity "workspace" will be a central challenge, and the emergence of such a "workspace" among allied forces is a weapon system in and of itself.

By Dr. Robbin Laird and Dr. Scott Truver

The Expanding Global Network

Crafting an effective U.S. Navy and Marine Corps strategy for the 21st century––one that both supports national security and homeland security objectives and gains sustenance from them––requires a strong emphasis on networking in a broad and comprehensive context. Networks make U.S. forces more effective by enabling them to share more information on a timelier basis, thus leveraging the power of a limited numbers of units and small forces.

That said, seamless interoperability and comprehensive information sharing per se in single-service, Joint, inter-agency and combined operations will no longer, in themselves, suffice. With the growing dependence of the nation's top-level strategies on the contributions of allies and coalition partners to the maritime defense of the global commons and to multi-national, sea-air power projection, the U.S. Navy and Marine Corps will have a greater requirement to network with American allies, partners and friends in a significantly broader, more inclusive fashion than ever before.

At the heart of this challenge is the leveraging of globalization. The U.S. Defense Science Board (DSB) has defined globalization as "the integration of the political, economic, and cultural activities of geographically and/or nationally separated peoples." 1 As the world's only global naval and maritime force in these first decades of the 21st Century, the Navy and Marine Corps—and the U.S. Coast Guard, as well2 —have special, often unique, roles to play in shaping the forces of globalization, notably sea transportation, the protection of resources, the movements of people, protection of the American homeland, and projecting power world wide in the interests of the United States. Moreover, the DSB report continues,

As the ease of transportation, which is an element of modern globalization, makes the defense of our sea frontiers more important, globalization also makes actions in the more remote regions of the world even more important to Americans and their economy. The linkage be-

[1] OSD, Defense Science Board Task Force on Globalization and Security, *Report of the Task Force on Globalization and Security* (December 1999), p. 1.

[2] The October 2007 "tri-service maritime strategy," *A Cooperative Strategy for 21st Century Seapower*, expands significantly the 1998 "National Fleet Policy Statement" signed by the Chief of Naval Operations and the Coast Guard Commandant to include the Coast Guard as an equal "player" in global naval and maritime strategies, roles, missions, operations, and tasks.

tween economic growth and foreign trade increases American dependence on the oceans that physically connect it to these remote regions as well as the importance of control over the connecting ocean areas. This control is the forte of our globally deployed naval forces. Arguably, a direct effect of globalization has been to make the power and effectiveness of naval forces even more important than before. It is not simply a question of retaining the access to trade and resources; America's ability to sustain its influence over events in remote regions has become more maritime dependent…3

In short, we live in an increasingly globalized world, dominated by the maritime domain, and national strategies will increasingly require the United States to form coalitions in order to maintain the stability on which global prosperity depends. Not to put too fine a point on it, but five years after then-CNO Admiral Michael Mullen raised the possibility of a "thousand ship navy' global and regional maritime partnerships have become, in many ways, the sine qua non on maritime power.

The Magellan Star Operation typifies the diversity of USMC and USN operations and the need to use flexible tool sets in global operations. http://www.sldinfo.com/?p=12000

The collapse of the Soviet Union in 1989 caused epochal changes for the world. These changes have affected the roles, missions and tasks of the Navy and Marine Corps and—

[3] *Report of the Task Force on Globalization and Security, op.cit.,* pp. xxvii-xxviii.

particularly since "9/11" — the need for much closer collaboration with the Coast Guard, which has seen its own mission-set expanded greatly.

The three U.S. Sea Services now face a whole new set of challenges, driven largely by the growing need to influence events ashore and in the littoral, often in uncertain and dangerous environments, to a much greater degree than these factors have shaped Navy, Marine Corps and Coast Guard strategies and operations in the past.

Today, the uncertainty as to where U.S forces will operate in local crises and conflicts makes it nearly impossible to arrange basing in advance, and, moreover, the United States is likely to face more simultaneous contingencies. Thus, the 2002 *Sea Power 21* white paper envisaged a more distributed fleet, capable of dealing with more multiple contingencies more or less simultaneously. A key challenge is to ensure that these smaller dispersed formations, or even single units, retain sufficient capability, as Sea Power 21 explained:

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.4

However, the shifting geopolitical landscape has changed America's focus. The Navy and Marine Corps have had to shift from the narrow emphasis of countering a peer competitor––i.e., the Soviet Union––to broad and varied global engagements, often without clear geopolitical adversaries, such as amorphous terrorist groups intent on doing the United States harm. Rather than being the sole super power, the United States is now more realistically characterized as the sole global power in a regionally diversified world.

As President Obama put it in the May 2010 National Security Strategy:

It would be destructive to both American national security and global security if the United States use the emergence of new challenges and the shortcomings of the international system as a reason to walk away from it. Instead, we must focus American engagement on strengthening international institutions and galvanizing the collective action that can serve common interests.5

In this context, the task of managing the transition from a bipolar, super-power world to a new globally interdependent environment of shared responsibilities is a key challenge facing the United States.

As the National Defense Strategy explains:

---

[4] Sea *Power 21: Projecting Decisive Joint Capabilities* (Washington, D.C., U.S. Navy, October 2002), p. 9.

[5] *The National Security Strategy* (Washington, D.C., The White House, May 2010), p. 3.

The security of the United States is tightly bound up with the security of the broader international system. As a result, our strategy seeks to build the capacity of fragile or vulnerable partners to withstand internal threats and external aggression while improving the capacity of the international system itself to withstand the challenge posed by rogue states and would-be hegemons.6

The growth of the global economy has been paced by the diversification and expansion of a technical base that is primarily commercial in nature. However, this same expansion has brought with it the global proliferation of many of the same technologies needed for the widespread production of modern arms as well. Global sourcing is the norm in aerospace and defense systems.

The proliferation of these "dual-use" commercial technologies will make it harder for U.S. forces to operate in many regional settings in the years ahead. Notably, the deployment of significant air-defense and missile-strike capabilities and the global spread of modern communication and information technologies all create a new strategic environment for the operation of U.S. and allied forces. Defenses are becoming harder to overcome as competitors or adversaries add modern air defense systems, craft new information-warfare capabilities, and combine missile and space systems to generate much more challenging environments within which US forces would operate.

Consequently, the need to build effective regional coalitions among developed and developing states is a key requirement for U.S. policy in the years ahead. A major difficulty in shaping such a new security system will be maintaining a strong leadership role without generating anti-Americanism as a factor in stimulating new regional alliances against U.S. interests.

In this emerging and burgeoning "network-centric" context, the key to the effectiveness of the United States as a global power will be its ability to leverage relations in one region to achieve effects in another, i.e., its skill in reaching beyond itself in one region to engage the participation of corresponding states in other regions.

In contrast to the traditional strength of a global super power––the unilateral capacity to bring overwhelming military force to bear without regard to the requirement to work with regional states––it is this regional networking role that will now be critical for the U.S. capacity to defend its interests.

Specifically, the United States will seek to become the primary architect of a security zone extending from the Mediterranean, through Europe, across the Atlantic to the Americas, and across the Pacific into Asia and the Indian Ocean littoral. In this role, it will not act as a hegemonic power, but rather as a networking power.

---

[6] *National Defense Strategy* (Washington, D.C.: U.S. Department of Defense, June 2008), p. 6.

The crafting of a connectivity "workspace" will be a central challenge, and the emergence of such a "workspace" among allied forces is a weapon system in and of itself.

The Challenge

The strategic challenge in this unique historical situation is to combine global reach with growing deftness in putting together coalitions––networks––of "the willing" to meet specific threats. This blending of military and diplomatic skills to create netted regional security arrangements will be a key U.S. goal in the 21st Century. As the tri-service maritime strategy explains:

…maritime forces will be employed to build confidence and trust among nations through collective security efforts that focus on common threats and mutual interests in an open, multipolar world. To do so will require an unprecedented level of integration among our maritime forces and enhanced cooperation with the other instruments of national power, as well as the capabilities of our international partners. Seapower will be a unifying force for building a better tomorrow.7

In creating regional networks, the United States needs to maintain unilateral capabilities to protect specific national interests while also leading, participating in, or supporting allied coalitions.

Thus, for the United States to have an effective military role in the new setting of regional networking, a key requirement will be effective and assured combined command, control, and communications, linked by advanced computing capabilities to global, regional, and local intelligence, reconnaissance, and surveillance assets (C4ISR).

The services will need to ensure that there is broad synergy among U.S. global forces fully exploiting new military technologies and the more modest capabilities of regional allies and partners. Indeed, C4ISR is evolving to become C4ISR D, whereby the purpose of C4ISR is to shape effective combined and Joint decision-making. (http://www.sldinfo.com/?p=199)

The Department or Defense and the Department of the Navy have responded to this new "cyber" environment with a major change to how DoD and DoN are organized. The Department of Defense has established U.S. Cyber Command as the command primarily responsible for dealing with new threats – and opportunities – created by the technologies that allow friend and foe to operate in this new dimension. Concurrently, the Navy Department has re-established the U.S. Navy 10th Fleet under the leadership of Vice Admiral J. "Barry" McCullough, who is dual-hatted as Commander, U.S. Fleet Cyber Command, reporting to the U.S. Cyber Command Commander.8

---

[7] *A Cooperative Strategy for 21st Century Seapower, op.cit.,* p. 3.

[8] See, for example, "Talking with Vice Admiral J. "Barry McCullough III," *Chips*, April – June 2010

Additionally, for the U.S. Navy the response to this new environment has been proactive and dramatic and has been reflected by the most profound reorganization of the Navy staff in over a decade. The Chief of Naval Operations has established a new Directorate, N2/N6 the Deputy Chief of Naval Operations for Information Dominance. This represents a radical re-stricting of the way the Navy "does business" in this new environment. According to Vice Admiral David "Jack" Dorsett:

Navy's information capabilities will evolve from 20th century supporting functions to a main battery of 21str century American seapower. To be successful at 21st century warfare, the Navy will create a fully integrated C2, information, intelligence, cyberspace, environmental awareness, and networks operations capability and wield it as a weapon and instrument of influence. Information will be treated as a weapon across the full range of military operations. The transition to an information-centric Navy represents a new vision of who we are as a sea power.9

Chief of Naval Operations Adm. Gary Roughead and Marine Corps Maj. Gen. Walter Gaskin, commanding general of II Marine Expeditionary Forces (Forward), meet with the commander of troops of the Azerbaijan army detachment collocated with the U.S. Navy detachment at Haditha Dam. The Azerbaijani detachment provides force protection to the U.S. Navy's

[9] *The U.S. Navy's Vision for Information Dominance* (Washington, D.C., U.S. Navy, May 2010).

riverine unit on the dam. Roughead expressed his thanks to the Azerbaijan people and their army for their contributions to Iraq's future and their cooperation with U.S. forces in support of coalition efforts. Credit: USN Visual Services, 11/1/07

Concurrently, in his most recent CNO Guidance, Chief of Naval Operations Admiral Gary Roughead has made achieving "Decision Superiority" one of his top five goals for 2010. The U.S. Navy Vision for Information Dominance builds on this CNO Guidance and quotes Admiral Roughead regarding this sea change in the Navy's use of information as a weapon:

The biggest breakthrough of the current fight in OEF and OIF is the successful integration of intelligence with operations, and using the network to get information to the right person, at the right time, in the right way. That is where the power is.10

In part, this is the challenge of a technology gap; but it also means recognizing the difference of emphasis between a global power operating regionally and regional powers operating locally.

Building a Way Ahead for the USN and USMC

At a minimum, U.S. forces and those of America's friends must share and exercise common command and control, with regular participation of coalition officers trained to work on combined staffs. When these prerequisites are met, the introduction and integration of compatible C4ISR systems becomes a coalition force multiplier and enables cohesive and effective integration of U.S. capabilities with those of allies and partners.

These coalition requirements demand emphasis on achieving the global transparency of command and control that will be indispensable for supporting U.S. engagements in crisis and conflict situations. In the not-too-distant future, networking will link sensor grids with diverse and dispersed platforms and bases, and situational awareness will encompass so much information exchange that the line between information providers and consumers will blur.11

New Directions for Navy/Marine Corps C4ISR D

1. The implications of these challenging global C4ISR D and networking requirements for the Sea Services, in some respects, are influenced by several key factors somewhat closer to home. As military services, the Navy/Marine Corps Team––complemented increasingly by the Coast Guard––is growing more dependent upon "network warfare" for several reasons: (1) a Navy and Marine Corps with fewer platforms––ships, aircraft and submarines––will need to place increased reliance on dispersed, interactive operations;

---

[10] *The U.S. Navy's Vision for Information Dominance*, p. 4.

[11] *Team SPAWAR Strategic Plan 2008-2013* (San Diego, CA: Space and Naval Warfare Systems Command, 5 October 2007), p. 4.

2. the development of advanced communication and data transmission systems can only enhance the advantage of dispersed but interactive forces and tactics, such as the Cooperative Engagement Capability (CEC); and
3. the wider use of offboard/remote sensors, e.g., satellites and unmanned aerial, surface, and undersea vehicles (UAVs, USVs and UUVs), including armed, unmanned platforms, will create its own demand for networking.

Moreover, the new 5th-generation aircraft function as "flying combat systems," comprising substantial onboard distributed computing systems, rapid upgrades through chip/software insertions, and designed and built around a 21st-Century concept of man-machine operations. All of these trends can be expected to continue––and, indeed, to accelerate––for the foreseeable future.12

A MH-60S Seahawk helicopter takes off from the flight deck of the littoral combat ship USS Freedom (LCS 1) for a maritime security exercise during the at-sea phase of Rim of the Pacific (RIMPAC) 2010, the world's largest international maritime exercise. Credit: USN Visual Service, July 2010.

With respect to force levels, today's fleet of some 288 ships (as of September 13, 2010) is probably the maximum that can be expected in the near term, i.e., at least for the next dec-

[12] See, for example, the *Department of the Navy Naval Networking Environment (NNE)~2016: Strategic Definition, Scope and Strategy Paper,* Version 1.1. 13 May 2008. Another excellent source is the *Naval Network Warfare Command Strategic Plan 2006-2010*, Summary Version 2.1, 1 November 2007.

ade. Despite a Navy force goal of 313 ships by 2020, shipbuilding budgets are not likely to provide an increase in ship construction and force levels. Rather, delays in the aircraft carrier (CVN), landing ship (LPD), and littoral combat ship (LCS) programs – to say nothing of the Navy's truncating the DDG-1000 program at three ships – coupled with the early retirement of ships suffering from maintenance problems and exacerbated by the restructuring of the Navy's next-generation destroyer and cruiser programs, could lead to an even smaller fleet in the near term. Fewer ships, aircraft, and submarines will place a strain on the fleet as crises and conflicts arise and continue in various parts of the world. Widely dispersed naval forces will see an increase in the transmission of data of all types among naval forces and Joint forces/commands.

Further, the limited size of the current and future fleet has led to the "1000-ship Navy" concept, first espoused by Admiral Michael G. Mullen when Chief of Naval Operations. This concept seeks to employ allied and even neutral navies in support of mutual national interests. In his address at the 17th International Seapower Symposium at the Naval War College in September 2005, Admiral Mullen stated that an international fleet in excess of 1,000 ships, a Global Maritime Partnership, was needed to address new challenges. "As we combine our advantages," he explained:

I envision a 1,000-ship Navy––a fleet-in-being, if you will, made up of the best capabilities of all freedom-loving navies of the world. Can you imagine the possibilities if we worked toward increased interoperability through more standardized training, procedures, and command and control protocols? This 1,000-ship Navy would integrate the capabilities of the maritime services to create a fully interoperable force––an international city at sea."13

With a view towards recent think tank studies and other initiatives such as the Center for Strategic and Budgetary Assessments (CSBA) Air-Sea Battle Concept,14 and the Center for Naval Analysis (CNA) Tipping Point,15 it is increasingly likely that the United States in general and the U.S. Navy in particular will be increasingly focused on "high-end" warfare in two primary "hubs" – the Western Pacific and the Arabian Gulf – and will have even fewer ships available for "engagement" activities. The net result will likely be an even greater demand for the U.S. Navy to provide the networks and the C4ISR D backbone for cooperative coalition naval activities, placing and even greater premium on getting the "networking piece right."

---

[13] Admiral Mike Mullen, remarks as delivered for the 17th International Seapower Symposium, Naval War College, Newport, Rhode Island, 21 September 2005.

[14] See, for example, Andrew Krepinevich, *Why AirSea Battle?* (Washington D.C.: Center for Strategic and Budgetary Assessments, 2010), Jan Van Tol, et. al., *AirSea Battle: A Point of Departure Operational Concept* (Washington D.C., Center for Strategic and Budgetary Assessment, 2010), Christopher Cavas, "USAF, U.S. Navy to Expand Cooperation," *Defense News*, November 9, 2009, and Jose Carreno et al. "What's New About the AirSea Battle Concept?" U.S. Naval Institute *Proceedings*, August 2010, Vol. 136/8, pp. 52-59

[15] See Daniel Whiteneck, Michael Price, Neil Jenkins and Peter Swartz, "The Navy at a Tipping Point: Maritime Dominance at Stake," (Arlington, VA: Center for Naval Analyses, March 2010), accessed at <http://www.public.navy.mil/usff/Documents/navy_at_tipping_point.pdf>.

In turn, this will place additional burdens on U.S. naval networks with respect to procedures, protocols, security, language, and equipment. U.S. naval networks will operate within overall U.S. proprietary military capability, with growing reliance as well on an ability to leverage commercial networks. Global maritime security depends on global information sharing: the sea is vast, ships are far between, and to be effective they must see beyond their horizons. Networking makes that possible.

Advances in communications and data sharing must be fully exploited to enhance the effectiveness of available naval forces and to enable those forces to employ offboard/remote sensors and unmanned platforms.

This will require improvements and changes in procedures and protocols, as well as the need for increased automation, as additional circuits, sensors, and unmanned platforms demand service by the Naval Information Dominance Enterprise (NIDE) infrastructure.

Systems such as I Robot's robotic Sea Glider will provide significant maritime domain awareness and will need to be integrated with the fleet on flexible operations. Credit: I Robot.

Further, because available bandwidth will be hard-pressed to accommodate these requirements, new concepts in how U.S. services use the available bandwidth, including time-sharing, burst communications, data routing, assignment of priorities, and other advances will be needed in naval networks.

The wide use of remote sensors and unmanned vehicles––air, surface, and underwater––will increase the need for effective networks and data links. In 2010, the Navy and Marine Corps use a large number of tactical UAVs, primarily for ISR functions. In the near term the Broad Area Maritime Surveillance (BAMS) system (pictured below with credit to Northrop Grumann) will provide a high-altitude, long-endurance vehicle, with an endurance of more than 24 hours; future UAV concepts envision endurance measured in months and years. Even at the tactical level, the decision to procure large numbers of the MQ-8 Fire Scout UAV for the LCS––i.e., more than 100 aerial drones deployed on board the planned force of some 50 LCSs––will demand new levels of networking.

The LCS in particular will bring new demands on Navy networking because, in addition to the Fire Scout UAV and manned helicopters, the various LCS configurations will operate unmanned surface and underwater vehicles in the anti-surface (ASuW), mine countermea-

sures (MCM) and anti-submarine warfare (ASW) mission configurations, as well as for other future roles and tasks.

More to the point of LCS, it will sit at the center of a network of unmanned sensors and pass information into wider area networks affecting tactical decisions. Similarly, advances in underwater communications are making it possible to include underwater sensors in networks which can help a fleet with limited numbers dominate the undersea battlespace of a littoral region. Submarines, which now operate only mine detection/mapping UUVs, can also be expected to operate more unmanned vehicles in additional mission areas, especially in novel ISR operations and possible ASW roles.

And the expanded role of robotics to shape an insertion enterprise, with air, surface and underwater robotic vehicles operating together will require an enhanced information capability.

Notably, the new assets coming off of the amphib as a key element of the USN and USMC joint team, spearheaded by the F-35B will allow the management of the information system to operate within an enduring littoral presence mission set (http://www.sldinfo.com/?p=96)

Robbin Laird visiting the F-35 factory and talking with Lockheed Martin personnel building the final F-35B test aircraft seen here. Photo Credit: Lockheed Martin, September 2010

In the context of this increasing use of data transmission and communications by U.S. naval forces, potential adversaries will also have increased access to the means and techniques for interfering with advanced networks. This became evident when Iraqi forces attempted to interfere with Global Positioning System (GPS) weapon guidance in the 2003 conflict and in recent––and often successful––foreign cyber attacks on U.S. government agencies and Congress, including the Department of Defense and various military and national networks. U.S. adversaries have the advantage of agility in developing cyber-attack capabilities because of the nature of a large, complex, hierarchal institution such as the U.S. armed forces, and the ready availability of cyber-attack techniques (often disseminated on the Internet) and of commercial hardware and software.

As the perhaps overstated cliché goes, all it takes for potential enemies to devise and field cyber-attack weapons are a credit card and access to a local Radio Shack. (This is why the Marine Corps is embracing distributed operations and the Air Force is focusing on the deployed tactical network and cyber offensive operations to protect deployed forces.) Also, critical will be relying on the new F-35s to spearhead a distributed decision making system

which will make targeting a central node in the information management grid of limited effectiveness (http://www.sldinfo.com/?p=6099). Indeed, doing so will open the aggressor to counter strikes via electronic warfare means.

The Aegis combat system is a C4ISR D system par excellence. Credit Photo: Lockheed Martin

These security considerations will have profound implications for the Naval Information Dominance Enterprise.

The Two Revolutions in Warfare

Within the C4ISR D environment described above, NIDE bears the responsibility for transitioning the Navy and Marine Corps into the evolving world of 21st-century information technology.

As such, it lies at the nexus of two ongoing revolutions in warfare.

The *first* is the increasing centrality of the information network for sharing precise, accurate, and timely tactical information among all levels of forces––leading to decentralized, or what the Marine Corps calls distributed, operations.

The resulting tactical picture enables U.S. forces to overwhelm adversaries by maximizing the use of surprise and by closing observe/decide/act "loops" faster than adversaries can. This way of war made possible victory in Afghanistan in 2001 despite the limited forces deployed by the United States and its coalition partners.
It will be crucial to victory in future expeditionary wars, particularly given the ongoing adoption of unmanned vehicles in all warfare domains. The tactical picture is created from a network of information sources, and it is shared among a network of users, who then depend upon that same network for the commander's intent that guides the transformation of information into action.

The *second* revolution is the exponential increase in the commercial availability of information-handling and computing power that underlies today's proliferation of networks and their interconnection. Currently, the commercial development cycle for new capabilities is 18 months or less, and the trend to build hosted payloads for the military and security forces onto commercial buses could accelerate these dynamics. Military procurement, which includes an exhaustive requirements-setting process and extensive testing, typically requires about seven years, and when it gets to the operators the equipment is frequently behind the times.

Until recently, military computing systems were so much more advanced than their civilian/commercial counterparts in the commercial/industrial sector that this disparity had little practical effect. However, with civilian computers now so far in advance of the Navy's systems, that delay has become intolerable. This led Vice Admiral Mark Edwards to comment:

Consider the Arleigh Burke (DDG-51) AEGIS guided-missile destroyer. It is one of the most sophisticated and capable fighting ships the world has ever seen. With its advanced SPY-1 radar, 96 vertical-launch tubes armed with a variety of long-range weapons, an advanced sonar system and anti-submarine warfare capabilities, it has everything a naval warrior could want. Consider, now, the Blackberry that has become ubiquitous in our culture. The two-way communication bandwidth of a single Blackberry is three times greater than the bandwidth of the entire Arleigh Burke destroyer. Looked at another way, the Navy's most modern in-service multi-mission warship has only 5% of the bandwidth we have in our home Internet connection. And the bandwidth it does have must be shared among the crew and combat systems: the C5ISR conundrum.16

The challenge is to specify and procure military/naval systems that exploit the power of state-of-the art commercial computers without sacrificing the safety and reliability required in military applications.

---

[16] Edwards, "Lead or Get Out of the Way," U.S. Naval Institute *Proceedings*, April 2008, p. 18. At the time of his writing, Vice Admiral Edwards was Deputy Chief of Naval Operations, Communications Networks (N6). Edwards describes the fifth "C" as "Combat Systems."

At least in several specialized areas, the Navy is already achieving this goal on a single-platform basis with programs such as the submarine community's ARCI (Acoustic Rapid COTS Insertion) program––a concerted effort to insert state-of-the-practice COTS (Commercial, Off-The-Shelf) hardware into submarine combat systems to achieve startling improvements in capability.

The NIDE needs to do the same thing for the wide-area networks that will serve multiple platforms and command facilities. However, at every level the integration of COTS must be viewed with caution; applying COTS to a legacy system, or even to new equipment that will be upgraded multiple times during its service life, could introduce serious potential flaws into the system.

And, of course, by its nature, COTS components—hardware and software—will not be maintained and updated in the face of rapidly developing technology: they will simply be replaced and discarded in the commercial world, which is already posing significant logistical impacts on the Sea Services.17

The Navy and Marine Corps already employ a variety of networks that offer America's warriors and their commanders access to a growing surfeit of combat and intelligence information.

And it should be remembered that the Aegis is not simply a U.S. system. About 1/3 of the fleet will be foreign when all deployments of foreign partners are in place. The Aegis Global Enterprise lays a solid foundation for common connectivity among allied fleets.

A rapidly emerging problem is separating the wheat from the chaff––devising the means to identify and retrieve what users really need from the vast amount of information on offer.

This necessity will soon abolish the long-standing practice of hoarding virtually all information centrally and pushing it out sparsely only on a "need-to-know" basis. Increasingly, the Navy and Marine Corps are coming to recognize that only the information-user on scene can know what he needs and that he requires more flexible capabilities to access data of his own choosing.

For example, the Marine Corps 2008 vision publication explicitly underscores the need to refine tactics, techniques, and procedures for disseminating high-value, actionable intelligence down to the lowest tactical level in support of operational maneuver and precision engagements.18

---

[17] For example, the F-35 architecture has been built with commercial obsolescence in mind. Before the first F-35 is deployed there are two shifts in processing power anticipated, and this will require inserting new chips and software upgrades.

[18] *Marine Corps Vision & Strategy 2025*, p. 20.

Efforts to harness both of these ongoing revolutions in achieving an ideal network solution confront a fundamental problem. The U.S. Navy and Marine Corps have already invested enormous sunk costs in communications, sensor, and weapons hardware, and cannot afford to replace it wholesale.

For example, in six years the Navy will have to double its information technology budget –– about $5 billion in Fiscal Year 2008––just to maintain the same capability in service today.19 Somehow, the NIDE needs to transition gracefully to newer network approaches while making maximum use of existing hardware and software as rudimentary building blocks.

The services have already started using greater computer power to leverage latent capabilities in existing communications systems for vastly increasing their effective capacity. Programs such as the Global Command and Control System (GCCS) have already pointed the way, and progress is accelerating in the use of Internet-based communications networks under the IT-21 program.

But transitioning the NIDE into the mid-21st Century demands the flexibility of a capabilities-based approach––one that focuses on required warfighting functions and not the means of implementing them.

One of the most basic of these capabilities is that of accommodating the non-linearity of thought and action that increasingly characterizes young men and women of the Information Age, the "Millenniums" born after the dawn of the Internet. These young operators will demand the same kind of on-screen hyper-texting, multi-tasking, and on-line search functions that they find routinely on their laptops today. They will want real-world tactical planning and execution to approximate what they have come to expect in video games that already simulate identical warfare scenarios.

The NIDE looks to exploit their experience, rather than train them to make do with the much less impressive capabilities now on ships and in the field. To do that, the United States must exploit current civilian-world computer technology and accept the need for much greater bandwidth. The necessary protocols, algorithms, and application software already exist in the commercial and industrial worlds––and because of an implicit, underlying open architecture, they can be implemented on a growing variety of hardware platforms. This is exactly the paradigm that is being seized in implementing the NIDE vision.

By adopting a corresponding NIDE open architecture, all the flexibility, ubiquity, and expandability of the Internet will become available to naval information systems. Such an open architecture parses data, applications, and hardware into separate domains, each with its own protocols and standards, but with internal domain specifications chosen to guarantee interoperability across the domain boundaries. Thus, all data in certain standardized

---

[19] Edwards, "Lead or Get Out of the Way, *op.cit*., p. 19.

forms will be acceptable to all relevant applications, and the latter in turn will run on all relevant hardware configurations.

This architecture and its underlying partition of the network "system" into data, applications, and hardware will eventually bring under its umbrella all major facets of the NIDE––the totality of C4ISR assets and capabilities. In subsequent phases, there is no reason why ship- and airborne combat systems––presently inhabiting a world of their own––should not be included also.

A major first step in taking this idea to sea is the Consolidated C4I Computer Environment (CANES), which is a unified acquisition program for providing a single C4I computing environment and an enterprise-wide service bus for afloat platforms. This will enhance the movement of data and provide a network architecture that is open, secure, reliable, and capable––much as the Navy/Marine Corps Internet (NMCI) and the follow-on Next-Generation Enterprise Network (NGEN) are attempting to fill much the same need for the shore-based infrastructure.

An important element of the tactical picture is supplied by the outputs of national (i.e., satellite) sensors. Hitherto, however, these information products have been heavily redacted before they were released for use by warriors. For three decades, these restrictions have been mitigated by the TENCAP (Tactical Exploitation of National Capabilities) effort, but more needs to be done to give naval forces timely, usable information about enemy activity beyond their horizons.

More recently, the Navy initiated a rapid acquisition program to install the Automated Identification System (AIS) capability that enables ships to obtain information from commercial global sensor systems to enhance local and regional situational awareness throughout the maritime domain: According to the Chief of Naval Operations, "Key to maritime security is the awareness of everything moving above, on, and under the ocean, or maritime domain awareness."[20]

These capabilities will be shared with allies and partners to help safeguard the security of the maritime commons in peacetime, crisis, and conflict. Indeed, less restrictive use of the national sensors will be key to the success of future strike, expeditionary, and coalition operations, and more open networking of these systems' "products" will become a major goal of NIDE, as well as linking to non-Defense systems.

The establishment of the Office of Global Maritime Awareness in the Department of Homeland Security, for example, has as a key goal creating a collaborative global, maritime information-sharing environment through a unity of effort across all military, civilian and

[20] Statement by Admiral Gary Roughead, Chief of Naval Operations, before the House Armed Services Committee on *The Cooperative Strategy for 21st Century Seapower*, 13 December 2007, p. 7.

commercial entities––in the United States and other countries––engaged in managing security, safety, environment, and commerce in the maritime domain.21

Moreover, as precise navigation and positioning become increasingly vital to identification, threat assessment, targeting, attack, and assessment, the integrity of GPS must be guaranteed against enemy attempts to disrupt it. Because the data used by commanders and shooters comes not only from their own platforms, but also from others in the network, there is a continuing need to ensure that the information on our networks is valid.

It is far easier to feed data into a network than to produce credible outputs. Moreover, the typical tactical user immersed in an urgent, real-world operation has neither the means nor the leisure to judge the quality of information presented to him. He is unlikely to drill down to determine where this or that useful insight originated, and, in any event, much of the value of a network devolves from the fact that the user need not have personal knowledge of or experience with anyone on whom he is relying.

The evolution of the C4ISR D systems aboard the new USCG cutter will allow it to play the role of a crisis management system. http://www.sldinfo.com/?p=10225

Another barrier to achieving the ideal is a further concomitant to the sunk cost of legacy networks and communications: Virtually all existing networks were developed for limited or focused purposes and remain largely "stovepiped." The network that handles satellite

[21] Joe Keefe, "Standing Up: Office of Global Maritime Situational Awareness, *Maritime Executive*, July/August 2008.

photographs is not the same network used to transmit electronic intelligence, or the one that handles logistics (which tells a commander what resources he has available).

Specialists may be aware of gateways from network to network, but for the average user, the real need is a degree of unification and a set of software tools to make across-the-board access easier. The Navy and Marine Corps are making good progress in this direction with NMCI/NextGen, IT-21, CANES, and TENCAP, but challenges remain in ensuring that the current special-purpose software needed by many network users will survive on the unified Navy/Marine Corps (and Coast Guard) net.

More capable networks create unprecedented demands on bandwidth. In the expeditionary context, the U.S. military is increasingly deployed as a multiplicity of small, interdependent, mobile units, which need to share increasing amounts of information among themselves and frequently over the horizon.

The military satellite systems that have provided much of the needed bandwidth in the past are now overwhelmed and being replaced. Typical of the new systems coming on-line soon is the Mobile User Objective System (MUOS), which will adapt a commercial third-generation cellular phone network architecture to provide a large multiplicity of secure narrow-band (64kbps) channels to fixed and mobile users world wide. It will be augmented by the Commercial Broadband Satellite Program for allowing ships to access civilian satellites of opportunity and increase the amount of broadband two-way communications available for mission traffic of all kinds.

Optimum management of the RF bandwidth available to ships and shore stations will be ensured by the Automated Digital Network System (ADNS), which uses off-the-shelf protocols, processors, and routers to centralize and automate the operation of multiple independent radio channels to create an efficient radio-based, wide-area, packet-switched network. When fully implemented, it is expected to provide a four-fold increase in multi-spectrum throughput efficiency compared to legacy systems.

The civilian world, too, has a boundless appetite for bandwidth, and already several successful military radar systems have had to be phased out because their frequencies were reallocated to civilian use. New civilian satellite systems and new civilian wireless communication networks will demand bandwidth previously reserved for military and naval use.

Again, it will be up to the NIDE and other Department of Defense (and Homeland Security, particularly FEMA and the Coast Guard) agencies to make the most of what is left. An additional irony in the growth of civilian bandwidth is that warriors who are used to civilian wireless devices, including laptops and cellphones, are surprised by how little of the spectrum (hence bandwidth) is left to them once they come aboard ship or deploy to the field. Vigorous NIDE program planning and execution will be needed to redress this surprising and unwelcome disparity.

And yet, the proliferation of networking may also bring significant dangers. The more the services depend on a networked infrastructure, the more America's adversaries will see U.S. networks as primary targets.

When the services relied on many incompatible networks, the task of the cyber-attacker was relatively difficult, since success against one or another of them would generally bring only limited benefits. The more unified the system––and the more inter-connected––the more tactical advantage successful cyber-attacks will bring America's enemies.

Cyber-defense must be a continuing effort and focus not only on the information passing over the network but also physical means of entry, including satellite beams and the telephone system. The increasing use of wireless media in telephone communications is also a significant source of vulnerability. Thus, a major goal of NIDE developers is to make the network inherently difficult to attack and to devise the means of defending it against such attacks.

The events of 11 September 2001 brought a host of new requirements associated with homeland defense and security. The principal focus of the past has been on serving the Navy/Marine Corps and Joint communities in fighting conventional wars and deterrence far from American shores.

SPAWAR's PEO C4I Established a New Program Office on Information Assurance and Cyber SEcurity on July 20, 2010 Credit: USN Visual Service, July 20, 2010

Now the NIDE must also accommodate information interchange with the U.S. law-enforcement community, especially the Coast Guard. These concerns about society-wide cyber attacks have generated increased interest in the Department of Homeland Security Science and Technology Directorate for close inter-agency, civilian-military collaboration:

First is the need for seamless connectivity and interoperability among communications and information-sharing systems that virtually link all levels of support—from the White House to first responders. Recent natural and man-made events underscore strategic, operational and tactical impediments we face from a lack of interoperability in the nation's command, control and communications systems and communications protocols and architectures. Lack of communications interoperability can hamstring situational awareness, command and control and response efforts, however heroic….

Then there is the vulnerability of our cyber-enabled world to attack from outside as well as within. Computers and software are the linchpins of commerce, communications, care, education, defense…virtually all aspects of modern society. Worldwide, trillions of dollars are at risk. For example, the Supervisory Control and Data Acquisition (SCADA) systems used in petroleum refineries and other large industrial facilities are threatened by cyber-terrorists and criminal hackers lurking in the Internet…. We must understand and defeat these and other cyber-threats to our safety and security.22

Since its inception, CTF 150 has been commanded by France, Netherlands, UK and Pakistan and Canada. Pakistan Navy Rear Adm Zafar Mahmood Abbasi currently commands CTF 150. http://www.cusnc.navy.mil/cmf/150/index.html

Hitherto, security considerations created significant barriers to exchanging tactical information with entities outside the military. Now it is no longer clear who can and should

[22] *Science and Technology for a Safer Nation* (Washington, D.C.: Department of Homeland Security, March 2008), pp. 2-3. The second DHS S&T concern focused on the domestic threat of improvised explosive devices in ports and waterways and on land.

have access to a complete "picture." Law enforcement has specific requirements that do not affect naval operations, but naval information can often be useful to law enforcers, such as the Coast Guard. At the very least, selective access will need to be adjudicated and monitored in accordance with local need, and this will soon create an entirely new class of networking requirements.

Finally, "business systems" will be increasingly critical to the NIDE's success, linking shoreside intelligence, maintenance, and scientific/technical communities with operators at sea and in the field. This covers a wide range of interactions––reachback for imagery/analysis, distance maintenance and spare parts support, research and development, enterprise resource planning and budget/fiscal management software, and personnel and pay systems. The NIDE must continue to leverage business information technology investments, strategies, and efficiencies to reduce costs associated with knowledge sharing and to ensure alignment of business technology governance, policy and guidance. This will focus on information infrastructure tools to reduce rework and duplication and to enhance the utility of information and knowledge needed to reach broader goals and objectives.23

The Central Role of C4ISR D in the 21st Century

In implementing a worldwide networking architecture––crucial to implementing a corresponding worldwide military strategy––the capability to connect forces across an allied defense space is central. This connectivity will arise through the use of interoperable technologies, the spread of Joint and combined decision-making systems, effective coordination of air and maritime U.S. forces with allied forces, and the emergence of allied littoral defense zones.

A few U.S. allies have already deployed compatible weapon and command-and-control systems and are actively collaborating in building extended littoral defense zones over their national territory. As U.S. forces arrive or operate within these allied enclaves, they should be able to "plug" directly into allied/coalition networks––subsuming individual systems––to create a synergistic expansion of the capabilities of both U.S. and other-county units.

Thus, it is in the U.S. interest to encourage allies not build nationally unique and sealed defense entities, but rather craft "enclaves" into which U.S. forces, allies and partners can "plug and fight." This means that a core NIDE mission is shaping a global collaborative "connectivity" workspace.

And as Admiral Mullen's initial concept of a "Thousand Ship Navy"/Global Maritime Partnership morphs increasingly into globally-dispersed, regional maritime partnerships, the

---

[23] *Team SPAWAR Strategic Plan, op.cit.,* p. 12.

need for the United States and the U.S. Navy to spearhead these coalition networking efforts will only grow.

This new norm is best exemplified by the corporation in and around the Middle East where an international naval force operates together and where smaller, regional, navies often lead these forces.

For example the naval forces of the Combined Maritime Forces (CMF) conduct Maritime Security Operations (MSO) in support of the international rule of law as well as relevant United Nations Security Council resolutions. These operations are focused on countering violent extremism and terrorist networks, along with countering other activities that threaten the maritime domain.

In the summer of 2010, the CMF was commanded by Vice Admiral William Gortney, U.S. Navy and Commodore Tim Fraser, Royal Navy, who served as Deputy CMF commander as well as United Kingdom Maritime Component Commander. Smaller, regional, navies typically led these efforts.

For example:

- Combined Task Force (CTF) 150—operating in the Red Sea, Gulf of Aden, Indian Ocean, Arabian Sea and the Gulf of Oman. Rear Admiral Zafar Mahmood Abbasi of Pakistan commanded CTF 150 in the summer of 2010.
- CTF 151 operates in the Gulf of Aden and Somali Basin to deter, disrupt and suppress piracy and involves naval forces from NATO, EU and other nations. Rear Admiral Beom-rim Lee of the Republic of Korea navy commanded CTF 151 in the summer of 2010.
- CTF 152, in the Arabian Gulf, works with Gulf Cooperation Council (GCC) partners in order to prevent destabilizing activities. CTF 152's commander in the summer of 2010 was Kuwait navy Colonel Jassim M. Al Ansari.24

The role of common protocols and communication technologies in melding forces grows in strategic significance with every year. Surface, submarine, and air platforms––and supporting shore facilities––all have their own core competencies and capabilities. These individual competencies and capabilities are essential to the success of any air, land or maritime strategy, but, fundamentally, platforms are nodes in a network and need to be deployed and interconnected as such.

---

[24] See www.navy.mil for a link to the June 28, 2010 issue of *Rhumb Lines*, a product of the U.S. Navy Office of Information for more on Combined Maritime Forces activities. And clearly, these international maritime partnerships are not confined to the greater Middle East region, witness activities such as Pacific Partnerships and RIMPAC in the Pacific. In CTF 151's operations on average, participating navies combine to provide 25 vessels from approximately 16 nations dedicated to conducting counter-piracy operations off the coast of Somalia and Horn of Africa

Only a flexible open architecture––one that separates data, applications, and hardware––will make possible the seamless interoperability of all cooperating forces and facilitate the "plug and fight" integration of new arrivals, regardless of the internal details of their hardware or software applications. Simultaneously, the cyber-defense of networks, connectivity, and decision-making systems must become an essential element of our IT infrastructure, even as our own ability to attack adversary networks creates new opportunities.

U.S. national security, homeland security, and military strategies envision a 21st-Century maritime battlespace dominated by strongly networked sea-air-land forces comprising U.S., allied, and coalition assets. As the key provider of the pervasive C4ISR network needed to make this vision real, the NIDE remains the single most important enabler for creating and maintaining these critical maritime force networks of the future.

Dr. Robbin Laird is co-founder of Second Line of Defense and has worked with Dr. Truver on maritime issues since 1996

Dr. Scott Truver is Director of National Security Programs at Gryphon Technologies, LC