NETWORKING THE GLOBAL MARITIME PARTNERSHIP

Stephanie Hszieh, George Galdorisi, Terry McKearney, and Darren Sutton

We will be prepared to support and defend our freedom of navigation and access to the global commons. Our partners and allies are our greatest strategic asset.

ADMIRAL MICHAEL MULLEN

Six years after Admiral Michael Mullen, then Chief of Naval Operations, proposed his "thousand-ship navy" concept at the Seventeenth International Seapower Symposium at the U.S. Naval War College in 2005, his notion of a Global Maritime Partnership is gaining increasing currency within, between, and among navies.[1] As the Chief of Naval Operations, Admiral Gary Roughead, noted in his remarks at the Nineteenth International Seapower Symposium in 2009, navies worldwide are working mightily to enhance cooperation and interoperability on the global commons.[2]

Real-world operations, especially in the Pacific Rim, have demonstrated that networking maritime forces is crucial to the effectiveness of operations that run the gamut from humanitarian operations to dealing with insurgencies, to nation-building, to state-on-state conflict. Additionally, these operations often involve nations and navies that come together on short—or no—notice, and, as a *necessary condition* for success in these operations, this networking must be immediately available and robust.

The central themes of this article are that the technical challenges of netting maritime forces together are not trivial and that overcoming these challenges is more daunting today than at any time in history. Why? Simply because unlike the days when flag hoists or simple radio transmissions were all that navies needed to effectively work together, rapid technological change has reached nations and navies unevenly and has actually *impeded* the effective networking of coalition partners. To maintain the growth and development of global maritime partnerships around the world, this article proposes leveraging an example of one effort

among long-standing partners to address the issue of naval interoperability at the defense laboratory level.

Coalitions at sea are not new. However, globalization—one of the macrotrends of the late twentieth and early twenty-first centuries—has prompted many nations to join together to maintain the security and stability of the maritime domain. Globalization—generally understood as "the integration of the political, economic, and cultural activities of geographically and/or nationally separated peoples"—involves the international interaction of information, financial capital, commerce, technology, and labor at significantly greater speeds and volumes than previously thought, and it impacts the lives and fortunes of all humanity.[3] It is important to recognize that globalization has a significant impact in the maritime domain, where events in one part of the world can swiftly impact peoples and societies across the globe.

As globalization has grown over the past two decades, we have witnessed an increase in maritime trade on the global commons. The tonnage of goods carried across the oceans by the rapidly growing merchant fleets of the world has more than quadrupled in the past four decades. This global exchange of goods has brought ever-increasing prosperity to the community of nations.

With globalization and the concomitant dependence on reliable oceanic commerce come vulnerabilities. Those who would disrupt this trade and the rule of law on the global commons, whether for economic or political gain, now have far more opportunities to attack vessels on the high seas or in near-shore waters than ever before. The dramatic increase in this century of piracy, a scourge many thought no longer existed, is but one manifestation of the threat to the rule of law on the global commons that the international community—and especially navies—must address today.

Concurrently, the nexus of climate change, growing populations, and a demographic shift to coastal and near-coastal regions has resulted in a significant increase in the impact of natural disasters—hurricanes, tsunamis, coastal flooding, volcanic events, earthquakes, and a host of others—that bring suffering to millions. Often, only naval forces are capable of delivering relief supplies in a timely fashion and in the volumes necessary to relieve disaster victims.

No single navy—of any nation—is robust enough to enforce the rule of law on the global commons alone or respond adequately to a major natural disaster. Today, through practice, global maritime partnerships have become the sine qua non for nations working together as global forces for good in support of ever-increasing levels of security, stability, and trust.

When navies assemble as a global force for good, a prerequisite for their ability to work together is that their ships, submarines, aircraft, command centers, and forces ashore have the ability to exchange data and information—often in

vast quantities—freely and seamlessly. Their effectiveness is directly proportional to their ability not only to communicate but to network, at sea and ashore. But as nations and navies proceed along different technological development paths, the challenges to effective networking are greater today than they were years ago, when navies used simpler—and more common—communications and rudimentary networking means. Because of this, their ability to interoperate effectively is often challenged.

Nations and navies are proceeding along different technological development paths. As a result of this inexorable trend, naval cooperation is under increasing stress.

There are core reasons why navies have been especially impeded in their attempts to network effectively in this new century. While the will is there, and though these navies are aligned through doctrine, tactics, techniques, and procedures to work and network together at sea, the technical means to realize the promise of "network-centric operations" throughout coalitions remain elusive.[4] Achieving that promise means dealing with the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) issues that currently complicate this effective networking. Navies have overcome similar challenges in the past, however, and understanding where we have been can help the members of today's naval coalition avoid becoming "victims of limited experience."[5]

Naval coalitions have long been an important part of maintaining sea power and good order on the seas. During the Cold War it was a naval alliance, under the auspices of NATO, that was able, through the building of a credible nuclear and conventional deterrent, to check Soviet encroachment into Europe.[6] However, coalition operations have taken on renewed importance as the maintenance of good order at sea has become a pressing concern for the international community. Naval coalitions today tend to be heterogeneous with respect to the types of navies represented, while the operations naval coalitions undertake have also expanded to include antipiracy patrols, as well as disaster relief and humanitarian missions. The importance of the ability to communicate with coalition partners transcends warfare and impacts coalition naval partners in literally every endeavor. This was dramatically demonstrated in December 2004 and early 2005 during the Indian Ocean tsunami response, where eighteen nations worked together, primarily on and from the sea, to deliver relief supplies.[7]

As they do for naval coalitions in general, naval communications continue to represent an integral part of successful naval operations, because they allow commanders to create the all-important "operational picture." In the arena of naval warfare, communications are needed to maintain "dominant battlespace awareness"—knowledge of where one's enemies and one's own forces are. Out of this

knowledge comes the ability to plan and strategize to defeat the enemy. In 1904, Britain's First Sea Lord, Admiral Sir John Fisher, took advantage of the new communications technology of his time—the telegraph—and developed what Norman Friedman calls "picture-based warfare."[8] Admiral Fisher established two war rooms—one for the world, the other focused on the North Sea—to collate information received from telegraphic messages to plot where French commerce raiders were attacking British merchant ships. Armed with this picture-based view of the world, Admiral Fisher was able to direct battle cruisers to the spots.[9] Future British commanders built on Admiral Fisher's successful harnessing of communications technologies to construct a global tactical picture—one that served them well in the years leading up to World War I, as well as during that conflict.

The innovative use of communications technologies to better conduct picture-based warfare continues in contemporary naval operations. Throughout the 1990s and into the twenty-first century, other initiatives have included the National Defense University's Dominant Battlespace Concept; Admiral William Owens's "system of systems"; military transformation and the revolution in military affairs (RMA); and the concept of "network-centric warfare" popularized by Vice Admiral Arthur Cebrowski and John Garstka. All these have led to significant focus on using communications to provide U.S. forces and their coalition partners a better ability to build a common picture to conduct picture-based warfare and, in so doing, secure the tactical, operational, and strategic advantage. But what these reformers—and others like them—have really been talking about is moving beyond merely communicating between and among units to *networking* forces and forming them into single fighting entities.

COMMUNICATING EVOLVES INTO NETWORKING FOR MODERN NAVIES

> *Above all, the picture is what matters. Creating effective tactical pictures makes systems work, and it supports a new kind of warfare. The better the picture, the more efficient the operation.*
>
> DR. NORMAN FRIEDMAN

In the latter part of the twentieth century, the U.S. Navy, reflecting its traditional style of operations—which entailed the continuous forward deployment of a distributed force far from U.S. territory or supporting infrastructure—developed the concept of "networking" to ensure timely and reliable communications to enable the most effective employment of scattered forces.[10] This effort included experimentation with the Tactical Data Information Exchange System (TADIXS),

which was the progenitor of the tactical data systems, such as Link 11, shared by many navies today.

Armed with increasingly reliable tactical data links, global navies began to recognize the potential of this ability to link ships across vast distances to revolutionize naval warfare. As Loren Thompson pointed out in 2003, however, many of the concepts driving the networking of military forces today arose two decades ago:

> In 1990, long before network-centric warfare became a central feature of joint doctrine, the Navy established a program called "Copernicus" to assimilate emerging information technologies. . . . The admirals managing Copernicus understood that information technologies had the potential to revolutionize naval operations. The Navy adopted the phrase "network-centric warfare" to describe this nascent warfighting paradigm, because it stressed integration and communications over autonomy in conducting naval operations.[11]

Eight years later, Vice Admiral Cebrowski and John Garstka built on Copernicus to envision war fighting in the twenty-first century. Their 1998 U.S. Naval Institute *Proceedings* article, "Network-centric Warfare: Its Origin and Future," described the potential of network-centric concepts to alter the nature of warfare itself. Although the article was published well over a decade ago, their vision of network-centric warfare proved remarkably prescient:

> Network-centric warfare derives its power from the strong networking of a well-informed but geographically dispersed force. The enabling elements are a high-performance information grid, access to all appropriate information sources, weapons reach and maneuver with precision and speed of response, value-adding command and control (C2) processes—to include high-speed automated assignment of resources to need—and integrated sensor grids closely coupled in time to shooters and C2 processes. Network-centric warfare is applicable to all levels of warfare and contributes to the coalescence of strategy, operations, and tactics. It is transparent to mission, force size and composition, and geography.[12]

Theory met reality in the early part of the twenty-first century, when the United States, in response to the terrorist attacks of September 11, 2001, launched Operation ENDURING FREEDOM (known as OEF) to attack terrorist strongholds in Afghanistan. The ensuing campaign vindicated what the proponents of network-centric warfare had been advocating. As Admiral Vern Clark, then Chief of Naval Operations, later observed regarding the U.S. Navy's experience in OEF, "Eighty percent of the Navy strike sorties attacked targets that were unknown to the aircrews when they left the carriers. They relied upon networked sensors and joint communications to swiftly respond to targets of opportunity."[13]

Admiral Clark evolved a vision for the U.S. Navy called "Sea Power 21: Operational Concepts for a New Era."[14] Some critics described the three pillars of Sea Power 21 (Sea Shield, Sea Strike, and Sea Basing) as "old wine in new bottles," but with them Admiral Clark introduced a new term, "FORCEnet," which referred to "an initiative to tie together naval, joint and national information grids to achieve unprecedented situational awareness and knowledge management."[15] FORCEnet was clearly the next step in the evolution of the Navy's networking capabilities. Thompson noted that "Forcenet [*sic*] was the greatest system-integration challenge ever proposed in the history of warfare."[16] Whether this is true or not, the U.S. Navy made an enormous capital investment in FORCEnet and in the wide array of programs that instantiate the network-centric warfare concept.[17]

The ability of navies to network vast amounts of data at high speed over great distances—due to the advancement of C4ISR technologies over the past decades—has ushered in new capabilities, pushed the "information envelope," and expanded the "art of the possible" at sea. It is not an overstatement to say that C4ISR systems have become the sine qua non of success for most modern navies. In fact, navies have found conclusively that their effectiveness is proportional to their ability to network at sea and ashore. Accordingly, every modern navy has sought to install C4ISR networking technologies—often as rapidly as they can afford them—in order to gain that technological edge at sea.

Drawing on real-world results from the U.S.-led coalition conflicts in Kosovo, Afghanistan, and Iraq, the U.S. General Accounting Office (now the Government Accountability Office) summed up the results of these conflicts:

> Network-centric operating concepts have improved battlefield situation awareness for commanders and their forces. DoD [the U.S. Department of Defense] has indicated that technological improvements in information-gathering systems allow commanders an unprecedented view of the battlefield. Such improvements provide for greater shared situational awareness, which, in turn, speeds command and control. . . . Improvements in networking the force and the use of precision weapons are the primary reasons for the overwhelming combat power demonstrated in recent operations.[18]

C4ISR advances not only benefit so-called high-end navies, but any navy investing in naval C4ISR technologies can gain a tactical edge. As pointed out by Paul Mitchell in 2003 in this journal,

> Network-centric warfare aims at increasing the efficiency of the transfer of maritime information among participating units (or nodes). By optimizing the efficiency of operations through information exchange, even small naval formations can generate additional combat power. Data is manipulated by a series of dynamic and interlinked "grids": sensor grids gather the data, information grids fuse and process it, and engagement grids manage the operations generated.[19]

Network-centric concepts are also being applied to developing local and regional maritime situational awareness, through various maritime domain awareness (MDA) information-sharing efforts. In short, MDA efforts are also part of building global maritime partnerships, as various regional information-sharing partnerships are netting up the global maritime commons. Efforts such as the establishment of Maritime Headquarters with Maritime Operations Centers (MHQ/MOC) for the numbered fleets in the U.S. Navy are geared to provide the capability to support MDA operations globally. National programs in the United States—such as the Container Security Initiative, Automatic Identification System (AIS), Customs-Trade Partnership against Terrorism (C-TPAT), and Maritime Safety and Security Information System (MISSIS)—are part of the multiagency effort to build MDA capability to support the defense of the homeland.[20]

Other nations have similar efforts to build up regional situational awareness of the maritime domain. In the pirate-infested waters of the Malacca Strait, the trinational effort of Malaysia, Singapore, and Indonesia (MALSINDO) began as a means of protecting the sea-lanes in the region from illegal activities—piracy, smuggling, etc. The regional cooperation also brought about Project SURPIC in 2005, when Singapore and Indonesia developed a joint surveillance system to share information regarding vessel movements in the Singapore Straits.[21] Singapore also established the ACCESS system and the Regional Maritime Information Exchange (ReMIX) Internet-based system to encourage information exchanges with other nations in the region.[22]

The U.S. Navy is actively engaged with regional partners and longtime allies to build information-exchange agreements and relationships to enhance global maritime partnerships in order to support global maritime domain awareness. There is currently work under way between the U.S. Navy and the French Ministry of Defense to share information obtained from the U.S. Navy's AIS Program of Record and France's SPATIONAV coastal systems. This information-sharing agreement, spearheaded by the U.S. Navy's Space and Naval Warfare Systems Center Pacific (SSC Pacific), will extend U.S. awareness of vessel movement in the European region and also the French Caribbean. The latter will provide the United States with valuable information to support drug interdiction efforts in the Caribbean. The final phase of the plan would allow the United States and France to exchange information and analysis regarding noncooperative, or "dark," targets in order to identify maritime threats. Work is also under way with another partner nation, Singapore, to integrate satellite imagery with AIS information to track vessel movements.

Maritime domain awareness efforts within the U.S. Navy have also been extended to developing regions to build new partnerships. One example of this is a Sixth Fleet–sponsored project to provide the government of Ghana with the

ability to characterize vessel traffic in the Gulf of Guinea. SSC Pacific scientists and engineers supporting the Sixth Fleet work with the University of Ghana to train students on open-source image processing. There is also a project going on with the University of Ghana to track canoes fitted with radar reflectors and AIS transmitters. The small-boat detection trials and training of imagery analysts in that region help not only to build new relationships but also to develop a capability for persistent maritime domain awareness in the Gulf of Guinea.

Through these and other MDA efforts, the maritime domain is being netted and global maritime partnerships are being strengthened with these emerging information-sharing agreements. However, the ability of different naval forces to engage in similar information-sharing activities at sea remains a work in progress. As mentioned earlier, new C4ISR technologies have had a dramatic impact on the ability of many navies to network with their own ships, submarines, aircraft, and command centers. This has led to a situation where various components *within* each navy can exchange large amounts of information. In doing so, these navies have found that they become more effective across the spectrum of conflict, from peacemaking to counterinsurgency, to major conflict.

However, this rush to install cutting-edge technology in each navy has had just the opposite effect on its ability to network effectively with assets of *other* navies. The problem is exacerbated by the fact that nations and navies are proceeding along different technological development paths. As a result of this inexorable trend, naval cooperation is under increasing stress.

NETWORKING THE GLOBAL MARITIME PARTNERSHIP: HOW BIG A CHALLENGE?

> *In today's world, nothing significant can get done outside of a coalition context, but we have been* humbled *by the challenges of devising effective coalition communications.*
>
> DR. DAVID ALBERTS

The experience of the Canadian navy in numerous deployments with U.S. Navy carrier strike groups (CSGs) suggests the issues that persist even among two modern, technologically advanced navies, let alone between and among multiple navies at various levels of technological maturity.[23] This documented experience —as well as other compelling data—illustrates how the very technology that has helped each navy communicate internally has impeded effective communications with forces of other navies. Paul Mitchell, then director of academics at the Canadian Forces College, puts this dilemma in stark terms: "Is there a place for small navies in network-centric warfare? Will they be able to make any sort

of contribution in multinational naval operations of the future? Or will they be relegated to the sidelines, undertaking the most menial of tasks, encouraged to stay out of the way—or stay at home? . . . The 'need for speed' in network-centric operations places the whole notion of multinational operations at risk."[24]

In 2010 General James Mattis, then commander of U.S. Joint Forces Command, echoed Mitchell's themes as well as more general concerns regarding networking: "In this age, I don't care how tactically or operationally brilliant you are, if you cannot create harmony—even vicious harmony—on the battlefield based on trust across service lines, across coalition and national lines, and across civilian/military lines, you really need to go home, because your leadership style is obsolete."[25]

What reformers have really been talking about is moving beyond merely communicating between and among units to networking forces and forming them into single fighting entities.

But how important is coalition networking, and what is the "state of play" today, as U.S. Navy combat formations attempt to communicate and share data with coalition partners and to achieve shared situational awareness?[26] Some would say that it is not yet what it should be. As Mitchell predicts, absent more effective means to network and exchange data, navies may even stop attempting to operate together. He raises what is perhaps the most important question regarding coalition naval communications: What level of communications and networking is required to make coalition operations at sea effective?

Mitchell did not ask this question offhandedly. For a number of years the Canadian navy has deployed surface combatants with U.S. Navy CSGs for six-month deployments. In that environment the effectiveness of coalition interoperability moves from theory to the reality of high-tempo, forward naval operations—operations that often involved combat. Mitchell has interviewed the commanding officers of seven Canadian ships that deployed with U.S. Navy CSGs to determine how effectively they were able to communicate with their U.S. Navy partners. The results indicated that while significant progress has been made, more work needs to be done.

The experience of these Canadian commanding officers, as well as of others working with U.S. naval forces in NATO exercises or operations, is that the "need for speed" in network-centric operations may result in the exclusion of even close allies. Thus, Mitchell asserts, while the guiding principle of network-centric warfare is to increase the speed and efficiency of operations, coalitions as such are rarely concerned about combat efficiency. Rather, their fundamental realities are always the scarcity of operational resources or the limits of their political legitimacy, or both. This point led Mitchell to conclude that because of the impact

of slower networks or non-networked ships in a dynamic coalition environment, the prospects of the U.S. Navy's keeping "in step" with coalition partners is not high—absent enlightened efforts by all governments concerned.[27]

At a 2003 international C4ISR symposium, Mitchell put it directly during a question-and-answer period:

> We have been trying to work with the U.S. Navy for a long time. Ten years ago when we basically communicated by the red phone [tactical voice nets] we did all right because it was pretty much a level playing field. Five years ago, with CHALLENGE ATHENA and the beginnings of networked communications, it started to become more difficult for us as the U.S. Navy sped away from its partners. Today, with the emerging FORCEnet, the U.S. Navy is in danger of leaving behind other navies because all of the background and decision making that goes on over networks like SIPRNET [Secret Internet Protocol Router Network] is lost to us [;] thus, when the order is given to do something we have none of the background for it and we are not in the battle rhythm of the operation.[28]

The situation Mitchell describes represents the reality of current coalition operations at sea and indicates that there is important work yet to be done. This is consistent with what proponents of network-centric operations have been professing for some time. In a capstone publication of the Department of Defense Office of Force Transformation, the late Vice Admiral Arthur Cebrowski opined, "The United States wants its partners to be as interoperable as possible. Not being interoperable means you are not on the net, so you are not in a position to derive power from the information age."[29]

If this is such an important issue, why have naval professionals not worked harder and more vigorously to solve it, and why have we not found a solution yet? Part of the problem lies in the differing relative success that navies have had networking at sea. Even in the days of signal flags, ships at sea found ways to communicate to some degree. As technology advanced from flashing lights to radio Morse code, to tactical radio voice circuits, to tactical data links, ships at sea often had it better than forces ashore on expanded battlefields. The assurance that "we've communicated at sea before and we're doing so today" obscures how well we could communicate and exchange data if the right technology, doctrine, tactics, techniques, and procedures were in place.

The importance of coalition partners effectively networking has perhaps been best articulated by Commander Alberto Soto, of the Chilean navy, in an article in this journal: "The availability of a cooperatively created tactical picture has long been a 'dream of naval commanders who wanted to be able to see what was over the horizon.'"[30] He argues the criticality of building and sharing an effective common operational picture within a coalition, noting that "regional navies have disparate capabilities, with major differences in terms of C4ISR. . . . [A]llies

do not acquire or develop command-and-control systems or surveillance and reconnaissance assets with the main goal of exchanging information with other potential allies."[31]

For the U.S. Navy, there is another complicating factor. Almost all officers who attain high rank in that service have served as carrier strike group commanders, typically as their first afloat assignments as flag officers. As a CSG commander, they experienced the "best of the best" in the way of communications and data-exchange capabilities—with robust displays, ample switching and routing capabilities, and high bandwidth. Additionally, coalition nets such as CENTRIXS are likely to be installed on the flagship, the aircraft carrier, and that is where coalition naval officers embark for most exercises.[32] Thus, as carrier strike group commanders advance through policy and acquisition assignments, their collective memories of coalition communications and data-exchange capabilities are often quite positive, their operational experience rarely having given them first-person knowledge of significant problems. But their experiences constitute the exception—not the rule—for they have generally not experienced coalition networking from the position of international surface combatants attempting to work with U.S. Navy ships.

There is another, perhaps more important, reason why an effective solution still eludes operators who want to solve this issue. Coalition interoperability does not fit into any requirements "bin," for either the U.S. Navy or, most likely, coalition partners. It does not fly, float, or operate beneath the seas. It does not strike the enemy from afar, like cruise missiles. It does not enhance readiness, like spare parts or training. It therefore often does not have the requisite degree of high-level advocacy. This is not to imply that those in charge of setting requirements or acquiring weapons systems are not keen on doing the right thing—clearly they are. However, the definition of operational needs, the requirements-generation process, and acquisition practices have grown up over decades, even generations, and changing them to factor in coalition communications adequately takes a great deal of time and attention.

As yet, this is a journey that is incomplete, and part of the reason is an inability to quantify the "goodness" derived from coalition networking. With naval establishments and acquisition bureaucracies increasingly driven by the rules of the marketplace—measures of effectiveness, returns on investment, best business practices, and efficiency—the absence of quantification makes it difficult to argue for scarce research and development, and especially acquisition dollars.

But it is a process that must take place if the U.S. Navy and its likely coalition partners are to operate at sea effectively for the next century. As Mitchell points out, "In network-centric warfare information is the cornerstone of all action; the existence of separate networks operating at different speeds will have an

undeniable impact on battle rhythms."[33] Clearly, overcoming uneven or uncoordinated application of C4ISR technology by nations that would work together to form a global maritime partnership is an essential first step in making that partnership a reality.[34]

HARNESSING THE SCIENCE AND TECHNOLOGY COMMUNITY: THE AUSCANNZUKUS WAY

We will win—or lose—the next series of wars in our nation's laboratories.
ADMIRAL JAMES STAVRIDIS

For the U.S. Navy, the technical challenges of networking effectively with likely coalition partners are not trivial.[35] The problem is twofold in nature: first, quantifying the difference in operational effectiveness between that of a coalition force networked via U.S. Navy infrastructure provided by the Consolidated Afloat Networks and Enterprise Services (CANES, discussed below) and that of a coalition force less robustly networked; and second, finding a way for likely coalition partners to coevolve maritime systems in a way that enables maximum networking among ships and other platforms.[36]

The issue of coevolution is an important one, because for navies determined to work with other, often smaller, navies as global maritime *partners,* a cooperative arrangement regarding technology development is crucial.[37] This implies early and frequent collaboration among scientists and engineers in the laboratories of these navies, as well as those of other prospective global maritime partners.

One vehicle for such cooperation among Australia, Canada, New Zealand, the United Kingdom, and the United States—the five AUSCANNZUKUS nations—is The Technical Cooperation Program (TTCP). Although it has existed in various forms for over half a century, TTCP is not well-known, even among AUSCANNZUKUS naval personnel. Importantly, while an analysis of coalition interoperability along other lines is certainly possible, TTCP's organization and infrastructure provide a ready-made medium that makes success *probable*.

TTCP is a forum for defense science and technology collaboration. Established as a joint effort between the defense organizations of the partner nations, TTCP is one of the largest collaborative defense science and technology activities in the world. The statistics give some indication of its scope: five nations, eleven technology and systems groups, eighty technical panels and action groups, 170 organizations, and 1,200 scientists and engineers are involved. The forum's purpose is to enhance national defense and reduce costs. To this end, TTCP provides a formal framework that scientists and technologists can use to share information.

Collaboration within TTCP acquaints participants with each other's defense research and development programs so that national programs may be planned

in concert. TTCP has its center of gravity in the applied research domain but also encompasses basic research and technology development. Its scope extends to exploration of alternative concepts prior to development of specific systems; collaborative research; sharing of data, equipment, material and facilities; joint trials and exercises; and advanced technology demonstrations. Cooperation within TTCP can catalyze project-specific collaboration farther along the acquisition path.

Enhancing Coalition Interoperability: MAR AG-1 and AG-6

In response to a mutually perceived need to assess the quantitative value of network-centric naval forces, in 2002 TTCP's Maritime Systems Group (MAR) established Action Group One (AG-1) to conduct a three-year "Network-centric Maritime Warfare" collaborative study. The study produced robust quantitative assessments of the benefits of the adoption by coalition naval forces of a networked force structure. The report of AG-1 prompted leaders of the MAR in 2005 to charter a second investigative team, Action Group Six (AG-6), to examine the impact the U.S. Navy's FORCEnet concept would have on coalition operations.[38]

In establishing the basic requirements for the technologies to be included in the study, AG-6 began by seeking a common understanding of the operational environment facing a coalition naval force. The group developed a scenario that evolved from a disaster assistance/humanitarian relief effort to a counterterrorism operation, and finally a high-tempo conflict at sea. Four principal measures of effectiveness were devised to compare the success of a coalition force that fully leveraged the U.S. Navy's FORCEnet capability to that of one not networked.

In addition, AG-6 members shared the "technology on-ramps" of their respective national acquisition programs in order to find where complementary technological capabilities could be inserted into naval C4ISR systems. The impacts and value of alternative coalition network structures were modeled and assessed. The result was a set of quantitative tools that could be adopted by the acquisition branches of the AG-6 nations.

Similarly, TTCP nations have come to regard the early manifestations of maritime net-centricity, such as FORCEnet, as stepping-stones on a path—a path marked out by the TTCP's "Maritime Net-centric Roadmap"—to becoming "fully net-enabled." The next step is the implementation of an information architecture to deliver the military capabilities and benefits that nations perceive as offered by network-centric warfare.

For its part, the U.S. Navy is committed to transforming, over the next several years, its current afloat network capability and global C2 infrastructure into the Consolidated Afloat Networks and Enterprise Services. The development of CANES will produce a "service-oriented architecture" (SOA), wherein applications, services, and data are provided to "communities of interest." SOA leverages a "publish and subscribe" messaging pattern in which information services,

often external to any given system, are published to the network, which can then be subscribed to (i.e., utilized) by other systems and users. CANES incorporates information technology and network services currently provided to coalition partners under the CENTRIXS umbrella, making the development of CANES a critical concern to the AUSCANNZUKUS community as the pathway to the Maritime Net-centric Roadmap's goal of full net enablement and ultimate convergence with the future Global Information Grid.[39]

Networking maritime forces is crucial to the effectiveness of operations that run the gamut from humanitarian operations to dealing with insurgencies, to nation-building, to state-on-state conflict.

The AG-6 study quantified how disparities in C4I capability within a U.S.-led coalition force undermine its effectiveness in a range of missions, ultimately disenfranchising less capable units. The migration of U.S. Navy networking capabilities to new architectures like CANES could increase that disparity, even introduce invasive and disruptive effects not well understood by the United States or its allies. The conclusions of the AG-1 and AG-6 studies, as well as ongoing TTCP studies, should help allied nations stay aligned as the U.S. Navy transitions to CANES. The AG-1 and AG-6 studies have given the MAR an excellent appreciation of U.S. and allied maritime capabilities, along with modeling frameworks and tools that can support recommendations to national leaderships. A further MAR study is under way that will provide an analytical assessment of requirements, funding, and execution of national programs to sustain U.S.-allied interoperability in a CANES SOA environment. It will clarify for national decision makers the impact of such technologies upon future network architecture.

As it relates to the planned integration of coalition network services (e.g., CENTRIXS), this new study will inform the U.S. Navy's CANES development process by raising awareness of the value and impact of C4I technologies potentially incorporated into CANES. (It will raise the awareness of allied navies as well—such inclusive efforts are often more useful for informing important constituencies than for providing prescient new information.) Like previous studies, it will inform national acquisition agencies of what will be required, in terms of coalition SOA, to enable TTCP navies to participate in future global maritime partnership (GMP) net-enabled maritime operations. Also, it will provide validated analytical tools and techniques that nations can reuse to explore national service-oriented architectures for their own interservice operations.

Leveraging TTCP Efforts across Global and Regional Maritime Partnerships

TTCP represents the work of only five nations, and the MAR AG-1/AG-6 effort represents only a small fraction of that work. Nonetheless, the issue of coalition networking is sufficiently compelling and the TTCP process so plainly worthy of

emulation that outside observers consider it a best-practices example and argue for similar efforts by other national groups. Commander Soto writes,

> Since 2002 the Technical Cooperation Program . . . has focused the efforts of its Maritime Systems Group (MSG) on "Networking Maritime Coalitions" and "FORCEnet and Coalitions Implications." The MSG has become an important link among national naval C4ISR acquisition programs. . . . For that very reason these [Latin American and Caribbean] nations should tenaciously strive to become involved in initiatives like the MSG.[40]

Other nations and navies, in natural clusters, can indeed take advantage of the policies and processes that TTCP has instituted within the AUSCANNZUKUS nations. They can replicate the TTCP model where it makes the most sense for them. As Commander Soto suggests, the navies of South America represent one such grouping. The ASEAN nations offer another, one that already has several collaborative forums. NATO offers yet another, and given the wide range of similar efforts already under way there, such as the NATO Network Enabled Capability (NEC) C2 Maturity Model, the way forward may be easier than some think.

It is important and necessary to use work such as TTCP or NATO's NEC as a means to harmonize national C4ISR acquisition programs, because the challenge is so great. This challenge has persisted for quite some time, as pointed out over a decade ago in an analysis of Operation JOINT ENDEAVOR, in Bosnia:

> Coalition operations such as Joint Endeavor present a complex set of challenges for the military C4ISR system planners, implementers, and operators. The most difficult challenge is the provision of integrated C4ISR services and capabilities to support the needs of ad hoc multinational military force structures and politically driven command arrangements. Although integrated C4ISR services are the desired objective, the realities tend to drive the solution to stove-piped implementations. In spite of technology advances, this will likely be the case for some time to come. There will continue to be uneven C4ISR capabilities among coalition members who will continue to rely on systems with which they are most comfortable—their own.[41]

Lest anyone think this issue is already solved in 2012 (or will solve itself shortly), effective networking is now a "wicked problem" for navies attempting to deal not with a "high end" environment like antisubmarine, antiair, or antisurface warfare but with the basic task of combating piracy. The editors of a recent collected work on piracy and maritime crime highlight the importance of effective maritime surveillance in countering piracy: "Clearly, maritime surveillance is the key to gaining a better understanding of what is happening on the oceans, but currently, systems are not integrated within each country, let alone at regional or global levels."[42]

It is beyond debate that the U.S. Navy will continue to partner with other navies to secure the rule of law on the global commons and that the effectiveness of this combined global force will rise or fall on its ability to network at sea. The Technical Cooperation Program provides an example of how nations can plant the technological seed in making C4ISR systems compatible with their partners, just as they have been able to do within their own fleets. It is a model that must be applied—and quickly—to the navies with which the U.S. Navy will work at sea. If these networking challenges are not addressed, the Global Maritime Partnership will remain only a concept and never deliver its promise.

NOTES

This article is adapted from the authors' *Networking the Global Maritime Partnership,* a forthcoming book from Sea Power Centre–Australia as part of its Papers in Australian Maritime Affairs series. The book is intended as a contribution to the ongoing dialogue regarding the global maritime partnership, specifically to address the challenges and opportunities associated with networking this partnership in a manner that enhances its effectiveness.

1. Adm. Michael Mullen, "A Global Network of Nations for a Free and Secure Maritime Commons" (keynote address, Seventeenth International Seapower Symposium, Naval War College, Newport, R.I., 19 September 2005), available at www.usnwc.edu/. The epigraph is U.S. Navy Dept., *Chairman of the Joint Chiefs of Staff Guidance for 2011* (Washington, D.C.: January 2011), available at www.jcs.mil/. The CJCS Guidance is the annual publication of the priorities of the chairman of the Joint Chiefs of Staff to guide the work of the Joint Staff.
2. Adm. Gary Roughead, "Remarks at the 19th Biennial International Seapower Symposium" (Newport, R.I., 7 October 2009), available at www.navy.mil/. Admiral Roughead speaks to the extraordinary turnout—102 countries and ninety-two maritime leaders—at this event (up from sixty-seven countries in 2005) as compelling evidence of the rapidly growing global embrace of the GMP. See, for example, "Remarks of Chief of Naval Operations Gary Roughead during the Current Strategy Forum, Newport, Rhode Island, June 8, 2010," available at www.navy.mil/.
3. While the term "globalization" has been defined in many places, the Defense Science Board's definition is one of the most widely accepted. See Defense Science Board, *Report of the Task Force on Globalization and Security* (Washington, D.C.: December 1999), pp. xxvii–xxviii.
4. Norman Friedman, *Network-centric Warfare* (Annapolis, Md.: Naval Institute Press, 2009), p. 65. See also Norman Friedman, "Netting and Navies: Achieving a Balance" (paper presented at the Royal Australian Navy Sea Power Conference, Sydney, Australia, February 2006), p. 6.
5. Vice Adm. Russ Shalders, former chief of the Royal Australian Navy, coined this phrase during his welcoming remarks at the 2007 King Hall Naval History Conference: "Naval history and its analysis is an important subject that helps alleviate the tyranny of limited experience. Only by studying history can we properly understand our own strengths and weaknesses and those of our friends and enemies." See *Proceedings of the 2007 King Hall Naval History Conference,* available at www.navy.gov.au/spc/.
6. Bradford A. Lee, "The Cold War as a Coalition Struggle," in *Naval Coalition Warfare: From the Napoleonic War to Operation Iraqi Freedom,* ed. Bruce A. Elleman and S. C. M. Paine (New York: Routledge, 2008), p. 146.

7. Bruce A. Elleman, *Waves of Hope: The U.S. Navy's Response to the Tsunami in Northern Indonesia,* Newport Paper 28 (Newport, R.I.: Naval War College Press, February 2007), available at www.usnwc.edu/press/.
8. Friedman, "Netting and Navies," p. 6.
9. Ibid.
10. The section epigraph is found in Friedman, *Network-centric Warfare,* p. 240.
11. Loren Thompson, *Networking the Navy: A Model for Modern Warfare* (Arlington, Va.: Lexington Institute, 2003), pp. 3–4. At the core of Copernicus were four overriding goals: to provide a common tactical picture to all members of the naval force; to connect them comprehensively in a web of instantaneous voice and data links; to compress the steps involved in moving information from sensors to shooters; and to conduct information operations that would degrade enemy war-fighting capabilities.
12. Arthur K. Cebrowski and John J. Garstka, "Network-centric Warfare: Its Origin and Future," U.S. Naval Institute *Proceedings* (January 1998), pp. 29–35.
13. Thompson, *Networking the Navy,* p. 6.
14. See Adm. Vernon E. Clark, "Sea Power 21: Projecting Decisive Joint Capabilities," U.S. Naval Institute *Proceedings* (October 2002), pp. 32–41, available at www.navy.mil/.
15. See Vice Adm. Richard W. Mayo and Vice Adm. John Nathman, "ForceNet: Turning Information into Power," U.S. Naval Institute *Proceedings* (February 2003), pp. 42–46.
16. Thompson, *Networking the Navy,* p. 6. See also Loren Thompson, *Netting the Navy* (Arlington, Va.: Lexington Institute, 2008), pp. 1–7, for a more contemporary look at the same subject. Also, it should be noted that "Forcenet" is spelled in various ways in the extensive literature on the subject. Generally, in U.S. Navy parlance, it is spelled "FORCEnet." This is because Adm. Vern Clark, as Chief of Naval Operations, wanted to emphasize that it was to support "the FORCE" (meaning naval forces).
17. Until 2010, the *U.S. Navy Program Guide*s, the yearly overviews of the systems, programs, and initiatives the U.S. Navy was pursuing to deliver a future navy, were organized around the four Sea Power 21 "pillars": Sea Strike, Sea Shield, Sea Basing, and FORCEnet. Grouped under FORCEnet were all the U.S. Navy's C4ISR systems that supported network-centric warfare. While the *U.S. Navy Program Guide 2010* (available at http://www.navy.mil/navydata/policy/seapower/sne10/sne10-all.pdf) did not carry forward this Sea Power 21 taxonomy, the C4ISR section featured all programs supporting network-centric warfare, including CANES (Consolidated Afloat Network and Enterprise Services), JTIDS (Joint Tactical Information Distribution System), and CENTRIXS-M (Combined Enterprise Regional Information Exchange System Maritime), among dozens of others.
18. U.S. General Accounting Office, *Military Operations: Recent Campaigns Benefited from Improved Communications and Technology but Barriers to Continued Progress Remain,* GAO-04-547 (Washington, D.C.: June 2004), p. 10, available at www.gao.gov/.
19. Paul T. Mitchell, "Small Navies and Network-centric Warfare: Is There a Role?," *Naval War College Review* [hereafter *NWCR*] 56, no. 2 (Spring 2003), p. 85.
20. Cdr. Steven C. Boraz, "Maritime Domain Awareness: Myths and Realities," *Naval War College Review* 62, no. 3 (Summer 2009), pp. 137–46.
21. Maj. Victor Huang, "Building Maritime Security in Southeast Asia: Outsiders Not Welcome?," *Naval War College Review* 61, no. 1 (Winter 2008), pp. 87–105. See also Maj. Desmond Low, "Global Maritime Partnership and the Prospects for Malacca Straits Security," *Pointer* 34, no. 2 (2008), pp. 44–57.
22. Lt. Col. Irvin Lim, "Comprehensive Maritime Domain Awareness: An Idea Whose Time Has Come?," *Pointer* 33, no. 3 (2007), pp. 13–26.
23. The section epigraph is from Dr. David Alberts (opening remarks, Seventh International Command and Control Research and Technology Symposium, Quebec City, Canada, September 2002).
24. Mitchell, "Small Navies and Network-centric Warfare," *NWCR,* p. 83, 88.
25. Gen. James Mattis (remarks, Joint Warfighting Conference, Armed Forces Communications and Electronics Association and U.S.

Naval Institute, 13 May 2010), available at www.jfcom.mil/. As commander of U.S. Joint Forces Command, General Mattis was also Commander, Allied Force Transformation, an important NATO "hat" that involves seeking solutions to allied and coalition networking challenges.

26. U.S. Navy battle formations are most often deployed as CSGs or as expeditionary strike groups (ESGs). A CSG is built around a large-deck aircraft carrier operating tactical jet aircraft; an ESG is built around a large-deck amphibious ship operating vertical/short-takeoff-and-landing aircraft and helicopters.

27. Mitchell, "Small Navies and Network-centric Warfare," *NWCR,* pp. 88–89. See also Paul T. Mitchell, *Network-centric Warfare and Coalition Operations: The New Military Operating System* (New York: Routledge, 2009), expanding on the argument that coalition partners in U.S.-led operations will have to be networked.

28. Paul Mitchell, "Small Navies and Network-centric Warfare: Is There a Role? Canada and US Carrier Battlegroup Deployments" (briefing presented at the Eighth International Command and Control Research and Technology Symposium, Washington, D.C., 17–19 June 2003). Concerning the reference to FORCEnet, Admiral Clark's Sea Power 21 taxonomy has faded from use, as noted above. The C4ISR technologies once categorized under FORCEnet in previous *U.S. Navy Program Guide*s are now categorized under "Information Dominance."

29. U.S. Defense Dept., *Military Transformation: A Strategic Approach* (Washington, D.C.: 2003), pp. 1–36, available at oft.osd.mil/.

30. Cdr. Alberto Soto, "Maritime Information-Sharing Strategy: A Realistic Approach for the American Continent and the Caribbean," *Naval War College Review* 63, no. 3 (Summer 2010), p. 145. The internal quotation is drawn from *Networking the Global Maritime Partnership* (San Diego, Calif.: SPAWAR System Center, June 2008), p. 5.

31. Ibid. See also, for example, J. Thomas, *The Military Challenges of Transatlantic Coalitions*, Adelphi Paper 333 (London: International Institute for Strategic Studies, 2000).

32. CENTRIXS is the U.S. Navy's Combined Enterprise Regional Information Exchange System, the premier network (in various versions) for U.S.-coalition interoperability in support of military operations. See B. Carter and D. Harlor, "Combined Operations Wide Area Network (COWAN)/Combined Enterprise Regional Information Exchange System (CENTRIXS)," Space and Naval Warfare Systems Center San Diego *Biennial Review* (2003), p. 87, for a detailed technical description. See also Mitchell, "Small Navies and Network-centric Warfare," *NWCR,* p. 90, for another nation's view of CWAN (COWAN) and CENTRIXS.

33. Mitchell, "Small Navies and Network-centric Warfare," *NWCR,* p. 91.

34. See, for example, D. C. Gompert, R. L. Kugler, and M. C. Libicki, *Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs* (Washington, D.C.: National Defense Univ. Press, 1999), for one of the earliest works exploring the challenges of ensuring that network-centric warfare investments and technology lead to more effective networking between and among allies and coalition partners. See Thomas, *Military Challenges of Transatlantic Coalitions,* for a European point of view on this issue.

35. The section epigraph is drawn from Vice Adm. James Stavridis, "Deconstructing War," U.S. Naval Institute *Proceedings* (December 2005), pp. 42–45.

36. For more on FORCEnet see *FORCEnet: A Functional Concept for Command and Control in the 21st Century* (Norfolk, Va.: Naval Network Warfare Command, 2006), and *FORCEnet: A Functional Concept for Command and Control in the 21st Century: Annex Version 20 June 2006* (Norfolk, Va.: Naval Network Warfare Command, 2006), both available at www.enterprise.spawar.navy.mil/.

37. Gordan Van Hook, "How to Kill a Good Idea," U.S. Naval Institute *Proceedings* (October 2007), p. 33. Captain Van Hook, drawing on his experience working with coalition partners as a destroyer squadron commander, emphasizes the importance of a cooperative approach. He argues that the United States should "encourage regional maritime security arrangements to form at the grassroots level, without overt U.S. leadership."

38. In straightforward terms, FORCEnet refers to the systems and processes needed to enable fully networked naval command and control between 2015 and 2020. The objective of FORCEnet is to provide commanders the means to make better, timelier decisions than they currently can and to allow effective execution of those decisions.
39. For the Global Information Grid, see, inter alia, *Global Information Grid Architectural Vision: Vision for a Net-centric, Service-Oriented DoD Enterprise,* Version 1.0 (Washington, D.C.: DoD CIO [Department of Defense Chief Information Officer], June 2007), available at cio-nii.defense.gov/docs/GIGArchVision.pdf.
40. Soto, "Maritime Information-Sharing Strategy," p. 148.
41. A. Krygiel, *Beyond the Wizard's Curtain: An Integration Environment for a System of Systems* (Washington, D.C.: DoD Command and Control Research Program, 1999), quoting Larry Wentz, ed., *Lessons from Bosnia: The IFOR Experience* (Washington, D.C.: National Defense Univ. Press, 1998), p. 273.
42. Bruce Elleman, Andrew Forbes, and David Rosenberg, *Piracy and Maritime Crime: Historical and Modern Case Studies,* Newport Paper 35 (Newport, R.I.: Naval War College Press, 2010), p. 235, available at www.usnwc.edu/press/.

Dr. Hszieh is a Corporate Strategy Group Strategic Analyst at the Space and Naval Warfare Systems Center Pacific, San Diego, California. She earned a PhD in political science at the University of Southern California and is the author or coauthor of numerous articles.

Captain Galdorisi, USN (Ret.), is Director, Corporate Strategy Group, at the Space and Naval Warfare Systems Center Pacific in San Diego, California. He is a graduate of the U.S. Naval Academy, and holds master's degrees from the Naval Postgraduate School (oceanography) and the University of San Diego (international relations). Additionally, he is a graduate of both the junior and senior courses at the Naval War College as well as the MIT Sloan School's Program for Senior Executives. His most recent book is Leave No Man Behind: The Saga of Combat Search and Rescue.

Mr. McKearney is the president and founder of The Ranger Group. A retired naval officer whose service spanned the Vietnam era to the post–Cold War era, he holds master's degrees from the U.S. Naval Postgraduate School and San Diego State University. He is president of the Military Operations Research Society (MORS) and is past chairman of the MORS symposium composite group on joint warfare.

Dr. Sutton is Head, Combat Systems Simulation and Analysis, Maritime Operations Division, in the Defence Science and Technology Organisation. He is also the science and technology adviser to the Royal Australian Navy's Air Warfare Destroyer Project. Dr. Sutton earned his doctor of philosophy in science (laser diagnostics for hypersonic flows) from the Australian National University.