

**Paper**

**for**

**15<sup>th</sup> ICCRTS**  
***The Evolution of C2***

**For the paper entitled:**

**“The Global Maritime Partnership:  
Networking Challenges and Opportunities”**

**Topic:**

**Topic 4: Collective Endeavors**

**Mr. George Galdorisi**

Space and Naval Warfare Systems Center Pacific

**Dr. Stephanie Hsieh (Point of Contact)**

Space and Naval Warfare Systems Center Pacific

**Space and Naval Warfare Systems Center Pacific**

**53560 Hull Street**

**San Diego, California 92152-5001**

**(619) 553-4817**

**[stephanie.hszieh@navy.mil](mailto:stephanie.hszieh@navy.mil)**

## Report Documentation Page

*Form Approved  
OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE <b>JUN 2010</b>	2. REPORT TYPE	3. DATES COVERED <b>00-00-2010 to 00-00-2010</b>			
4. TITLE AND SUBTITLE <b>The Global Maritime Partnership: Networking Challenges and Opportunities</b>		5a. CONTRACT NUMBER			
		5b. GRANT NUMBER			
		5c. PROGRAM ELEMENT NUMBER			
6. AUTHOR(S)		5d. PROJECT NUMBER			
		5e. TASK NUMBER			
		5f. WORK UNIT NUMBER			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Space and Naval Warfare Systems Center Pacific, 53560 Hull Street, San Diego, CA, 92152-5001</b>		8. PERFORMING ORGANIZATION REPORT NUMBER			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)			
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)			
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES <b>Proceedings of the 15th International Command and Control Research and Technology Symposium (ICCRTS '10), Santa Monica, CA, June 22-24, 2010</b>					
14. ABSTRACT <b>Few strategic concepts have spurred more discussion than the notion of the global maritime partnership (originally called the 1000-ship Navy), a concept first introduced by then-U.S. CNO, Admiral Michael Mullen, at the International Seapower Symposium in September 2005. In the ensuing four years this concept has been broadly discussed in the international defense media and at conferences and symposia, including those sponsored by the CCRP. Admiral Mullen, now Chairman of the Joint Chiefs of Staff, took this idea even further, suggesting that global security partnerships are one of the most important considerations for the U.S. Department of Defense. The networking challenges to the global maritime partnership are manifest and will not succeed if the "power to the edge" concepts exposed by the CCRP are not addressed and if we fail to understand the lessons learned from past networking and coalition partnering. This paper will address that rich history and demonstrate how lessons learned from past networking and coalition efforts can inform global security efforts today. We will share the results of a "beta-test" among the five AUSCANNZUKUS nations, currently entering its seventh year, which provides one example of how to address these C4ISR challenges.</b>					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>21</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

**Abstract for  
“The Global Maritime Partnership:  
Networking Challenges and Opportunities”**

Few strategic concepts have spurred more discussion than the notion of the global maritime partnership (originally called the 1000-ship Navy), a concept first introduced by then-U.S. CNO, Admiral Michael Mullen, at the International Seapower Symposium in September 2005.

In the ensuing four years this concept has been broadly discussed in the international defense media and at conferences and symposia, including those sponsored by the CCRP. Admiral Mullen, now Chairman of the Joint Chiefs of Staff, took this idea even further, suggesting that global *security* partnerships are one of the most important considerations for the U.S. Department of Defense

The networking challenges to the global maritime partnership are manifest and will not succeed if the “power to the edge” concepts exposed by the CCRP are not addressed and if we fail to understand the lessons learned from past networking and coalition partnering.

This paper will address that rich history and demonstrate how lessons learned from past networking and coalition efforts can inform global security efforts *today*. We will share the results of a “beta-test” among the five AUSCANNZUKUS nations, currently entering its seventh year, which provides one example of how to address these C4ISR challenges.

## **“The Global Maritime Partnership: Networking Challenges and Opportunities”**

“In our efforts [to ensure the rule of law on the global commons] we cannot forget that while we are an independent and powerful Navy, we are not alone in our intentions or goals. Global Maritime Partnerships are setting the standard for international cooperation, in our globalized world and they are an important element to achieving stability in the global commons upon which we all rely. Over the past few years, through the diligent work of many, many leaders in this room and many international leaders, we have developed relationships that will help us tackle common maritime threats together. The success of the last International Seapower Symposium in Newport, Rhode Island was truly unprecedented. The presence of 102 nations and 91 chiefs of service demonstrated a global commitment and a global reach that no other service enjoys. As impressive as the number for the year’s symposium were, it was the discussion and commitment that was most notable.”<sup>1</sup>

Chief of Naval Operations Admiral Gary Roughead  
Remarks delivered at the Surface Navy Association Symposium  
January 14, 2010

### **Perspective**

“Most think that bigger, faster, and more is best when talking about providing technology to naval forces. But this is not always the case. What matters is not how *much* you communicate, but rather getting the right information to the right people at the right time.”<sup>2</sup>

Professor Nicholas Rodger  
Exeter University  
Keynote Address  
2007 King Hall Naval History Conference

“When John Fisher became First Sea Lord in 1904, his main pledge was to solve this intractable problem...Fisher in effect invented picture-based warfare. He created a pair of war rooms in the Admiralty, one built around a world (trade) map, the other around a North Sea map.”<sup>3</sup>

Dr. Norman Friedman  
“Netting and Navies: Achieving a Balance”  
*Sea Power: Challenges Old and New*

The rich history of naval cooperation between and among navies united in ensuring that the rule of law is maintained on global commons over the past century has an equally rich history of networking at sea, enabled by such innovative practices as First Sea Lord John Fisher’s use of “picture-based” warfare at the beginning of the last century. And further spurred by the exigencies of the two global wars of the past century, wars in which naval forces played a dominant role, these navies have adopted new technologies that have helped them coordinate their efforts at sea.

But as Professor Rodgers points out, it is *how* this technology is applied that determines not only how effective it is, but often, whether these navies face victory or defeat. For example, as nations – and

especially navies – adopted new technologies, they found that often the technological promise of a new system was accompanied by unintended consequences that sometimes made the net result a negative rather than a positive. In most cases, it is because these navies failed to ensure that “power to the edge” principles were applied.

But like globalization, rapid advances in technology – especially the command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) technologies – that link navies together, present a challenge that must be reckoned with if these navies seek to achieve the interoperability necessary to operate together seamlessly at sea in peace and war. As pointed out by Dr. Chris Rahman in *The Global Maritime Partnership Initiative: Implications for the Royal Australian Navy*, “To function effectively, the 1000-ship Navy (the precursor name for the Global Maritime Partnership)<sup>4</sup> will not only require high levels of international political support to foster the necessary levels of cooperation, but also will be heavily technologically dependent.”<sup>5</sup>

The rich maritime traditions shared by those navies united to ensure the rule of law on the global commons strongly suggests that policy or doctrinal differences that might impede seamless interoperability between and among these navies can be readily overcome. What is less certain is whether the technological challenges of linking navies that pursue different paths of technology development, insertion, and refresh can be successfully dealt with. The continuing challenges these navies have in working together at sea – especially over the last decade – suggest that solutions to these technical issues remain elusive.

As one especially significant historical example, the introduction of the telegraph, promised instantaneous communications across vast distances. No longer would messages take months to traverse continents as telegraph cables and networks made it possible for messages to be relayed in days. The Royal Navy found the telegraph to be an important tool in communicating with its global fleet, but that ease and speed of communications came with a price. During times of tension, fleet commanders were often found on their command ship docked at port in order to have access to telegraph messages rather than out at sea with their ships.<sup>6</sup>

But the telegraph, a breakthrough technology that all assumed would “cure” a universe of communications ills had another downside – and “unintended consequence” of its use.<sup>7</sup> Prior to the invention of the telegraph, expatriates at the far end of the British Empire received the news regarding events transpiring in the British Isles via bundles of newspapers that were delivered via sailing vessel. This typically took anywhere from four to six weeks but when the news arrived it was robust, detailed, and provided the reader with virtually all they could want to know about these events – absent being there in person.

The Victorians eagerly embraced the telegraph as something that was “faster and better” than waiting for newspapers to arrive via ship and something that would provide them the “news of the home islands” instantly and without the multi-week time delay. However, this new technology had a downside: telegraph transmissions were expensive so those putting together telegraph messages placed a premium on brevity and “news” was truncated to the bare essentials. Additionally, transmissions were sent from one way-station to the next where one operator had to manually key in what he or she had just received, a process that was fraught with error – and was doubly chancy since not all operators at these way-stations spoke English. The net result was that when the news finally arrived it was truncated, error-prone and often bore little resemblance to the initial information that was transmitted.<sup>8</sup>

The advent of wireless technology also brought the promise of better and speedier communications between command and fleets at sea. Navies were no longer bound by land-locked telegraph cables and signals could reach out into the vast expanse of the sea allowing for central command to better track their forces. This centralized control allowed for better vectoring of fleets based on a centralized information system, but also made it harder for fleet commanders to manage their ships. Professor Rodger of the University of Exeter tells of an incident in 1942 when the commander of the Royal Navy's Home Fleet, Admiral John Tovey, asked the Admiralty to take command of his ships as he had lost track of them while at sea.<sup>9</sup>

And not unlike the telegraph, wireless had a huge downside, another "unintended consequence" of new technology. While this wireless technology helped commanders reach far-flung units and communicate in real time, *enemy* units could also copy these same transmissions and thus gain the tactical advantage over the forces communicating via this wireless technology. History is replete with examples of navies and other forces suffering defeat because the enemy intercepted wireless communications. But clearly, none of this "downside" was anticipated when the new technology was initially developed and placed on naval units.

Naval forces today that are united in maintaining the rule of law on the global commons have embraced current communication technologies like the Internet and satellite communications to maintain situational awareness and track their fleets. However, much like the Royal Navy in the days of the telegraph and wireless communications, navies of today must also deal with the challenges posed by these new technologies. The challenge now is how can these navies – which are committed to effectively network at sea – ensure that their substantial investment in C4ISR technologies result in more – not less – interoperability? To understand the challenges, as well as the opportunities, facing navies in the 21<sup>st</sup> Century we must first understand how well these navies are able to interoperate *today*.

### **Naval Coalition Networking: How Big a Challenge?**

"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."<sup>10</sup>

Professor Paul Mitchell – Canadian Forces College  
"Small Navies and Network-centric Warfare: Is There a Role?"  
*Naval War College Review* Spring 2003

"The thorniest issue is to what extent participants are expected to contribute to the timely sharing of information to be used for the identification, monitoring, disruption or interdiction of illegal activities...Each nation can be expected, for example, to have clearly defined rules for releasing information about intelligence platform capabilities."<sup>11</sup>

Lieutenant Commander Chris Watson, RAN  
"How Might the World's Navies Contribute to and Benefit from the '1000-Ship Navy Proposal?'"  
*Australian Maritime Issues* 2007

Clearly, the available evidence suggests that navies united in maintaining the rule of law of the global commons recognize the importance of coalition networking and that naval operators of all nations, the men and women “on-point” in this effort, recognize it perhaps more so than others. As the headquarters, acquisition and operational staffs of these navies work to ensure their sailors can communicate seamlessly at sea, understanding the challenges to effective networking between and among navies – especially navies at different stages of technological development – is key to developing the right technical solutions. Looking to examples in the navies our nation works with, and extrapolating these examples to other navies united in maintaining the rule of law of the global commons is an important first step in this process.

From the perspective of the United States Navy, at the very pinnacle of the U.S. military, this notion is articulated perhaps most clearly in *The National Military Strategy*, which notes:

Achieving shared situational awareness with allies and partners will require compatible information systems and security processes that protect sensitive information without degrading the ability of multinational partners to operate effectively with U.S. elements.<sup>1 2</sup>

How important is coalition networking and what is the “state of play” of this networking today, especially when U.S. Navy combat formations attempt to communicate and share data with coalition partners and achieve “shared situational awareness?”<sup>1 3</sup> Some would say that it is not yet where it should be. As Professor Mitchell, formerly the Director of Academics at the Canadian Forces College, noted in his article in the authoritative *Naval War College Review*, absent more effective means to network and exchange data, navies may even stop attempting to operate together.<sup>1 4</sup> 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.

Professor Mitchell did not ask this question off-handedly. For a number of years the Canadian Navy has deployed a surface combatant with U.S. Navy Carrier Strike Groups (CSGs) for an extended six-month deployment. This was an environment where the effectiveness of coalition interoperability moved from theory to the reality of high-tempo, forward-deployed naval operations – and operations that often involved combat. As part of his research, Professor Mitchell interviewed the commanding officers of each Canadian ship that deployed with a U.S. Navy CSG 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.

As Professor Mitchell noted in his article, the experience of these Canadian commanding officers, as well as the experience of others working with U.S. naval forces in NATO exercises or operations, was that the “need for speed” in network-centric operations may result in the exclusion of even close allies. Thus, he notes, while the guiding principle of network-centric warfare (NCW) is to increase the speed and efficiency of operations, coalitions are rarely concerned about combat efficiency. Rather, they are always about scarcity in terms of operational resources, political legitimacy, or both. This led him to conclude that in a dynamic coalition environment, because of the impact of slower networks or non-networked ships, the prospects of the United States Navy keeping “in step” with likely coalition partners, is not high – absent enlightened efforts by all governments concerned.<sup>1 5</sup>

At a 2002 international C4ISR symposium, Professor Mitchell put it more directly when he said during the question and answer period following his presentation, “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 IT-21 and 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 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.”<sup>16</sup>

While some might say this is merely anecdotal information, for us and our colleagues from other navies the situation Professor Mitchell describes represents the reality of current coalition operations at sea and indicates that there is important work yet to be done. Additionally, this is consistent with what proponents of network centric operations have been espousing for some time. In a capstone publication of the United States Department of Defense Office of Force Transformation, the late Vice Admiral Arthur Cebrowski, considered by some to be the “father of network-centric warfare,” stated: “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.”<sup>17</sup>

If this is such an important issue then 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 relative success that navies have had networking at sea. Even in the days of signal flags, ships at sea found a way to communicate to some degree. As technology advanced from flashing lights, to radio Morse code, to tactical radio voice circuits, to the initial tactical data links, ships at sea often had it better than forces ashore on expanded battlefields. The fact that “we’ve communicated at sea in the past and we’re doing so today,” often obscures how well we could communicate and exchange data if the right technology, doctrine, tactics, techniques, and procedures were in place.

For the U.S. Navy there is another complicating factor. Almost all officers who attain high rank in the U.S. Navy have served as carrier strike group commanders at some time during their career, typically as their first afloat assignment as Flag officers. As a CSG commander embarked in a Nimitz-class aircraft carrier, the Admiral has experienced the “best of the best” in the area of communications and data exchange capabilities – with robust displays, ample switching and routing capabilities, and high bandwidth.

Additionally, from the U.S. Navy perspective – with respect to communicating and exchanging data with coalition partners – coalition nets such as CENTRIXS are likely to be installed on the aircraft carrier and that is also where coalition naval officers embark for most exercises. Thus, as CSG commanders mature through policy and acquisition assignments, their collective memory of coalition communications and data exchange capabilities is often quite positive: they don’t have the first-person knowledge of any problems associated with their operational experience. But their experience is the exception – not the rule – for they have not experienced coalition networking from the position of coalition surface combatants attempting to work with U.S. Navy ships.

Beyond the particular case of U.S. Navy Flag officers whose operational background may have obscured genuine challenges to effective coalition networking, there is another, perhaps more important, reason that an effective solution still eludes the operators who want to solve this issue. For a host of reasons, coalition interoperability does not fit neatly into any requirements “bin” for the U.S. Navy, or for other likely coalition partner navies. 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 just does not always 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, as clearly they are. However, defining operational needs, the requirements generation process, and acquisition practices have grown up over decades – even generations – and changing these processes to adequately factor in coalition communications takes a great deal of time and attention. As yet, it is a journey that is incomplete.

Part of the reason for this lack of advocacy and difficulty in reorienting requirements and acquisition practice is the 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, return on investment and best business practices – the lack of measures to quantify the benefits derived from effective coalition networking auger against spending scarce research and development, and especially acquisition, dollars to enhance something that has not yet been effectively quantified.

However, it is a process that must take place if navies united in ensuring the rule of law on the global commons are to operate at sea effectively for next century. Serendipitously, many of these nations have well-developed military laboratory organizations able to work on coalition networking challenges and also have well-developed processes for dealing with sister laboratories. This is especially true among the five AUSCANNZUKUS nations. And given the technological challenges of effectively networking these diverse navies, the military laboratories of these five nations must pursue this as a matter of priority.

### **Tell It to the Labs**

“We will win – or lose – the next series of wars in our nation’s laboratories.”<sup>1 8</sup>

Admiral James Stavridis  
SOUTHCOM Commander  
“Deconstructing War”

*U.S. Naval Institute Proceedings* December 2005

“The idea is that information gathering and handling can reduce the numbers of men and platforms and weapons. Information is not itself a weapon, it is an enabler that makes weapons more effective – if it is properly used.”<sup>1 9</sup>

Norman Friedman  
*Network Centric Warfare: How Navies  
Learned to Fight Smarter Through Three World Wars*

For Commonwealth navies – those nations who have worked, and will likely continue to work most closely with the U.S. Navy – the technical challenges to effectively network are not trivial. Specifically, when working with a 21<sup>st</sup> Century FORCENet-centric U.S. Navy and attempting to leverage the enormous capital investment the U.S. Navy is making in FORCENet, the challenge is twofold: quantifying the operational effectiveness of a coalition force networked via U.S. Navy infrastructure provided by FORCENet, versus the operational effectiveness of a coalition force less-

robustly networked, and finding a way for likely coalition partners to co-evolve maritime networking systems in a way that enables maximum networking among partner ships and other platforms.<sup>20</sup>

The issue of co-evolution is an important one because for Commonwealth navies determined to work together with other – often smaller – navies as global maritime *partners*, a cooperative arrangement regarding technology development is crucial.<sup>21</sup> And this implies early and frequent cooperation and collaboration at the grass-roots level by scientists and engineers working in laboratories of Commonwealth navies as well as those of other prospective global maritime partners to come up with technical solutions for challenging networking problems.

Government defence laboratories in the Commonwealth nations and in the United States are ideally positioned to lead the effort to co-evolve C4ISR capabilities that will enable their navies to effectively network at sea – and their success can be a model for many other naval coalitions. There are many reasons why these defence laboratories should lead this effort, and collectively, they strongly auger for increased reliance on these laboratories to lead this important effort.

First and foremost is wealth of talent in these laboratories. Government defence professionals have been at the forefront of developing *today's* C4ISR systems and thus have the talent and the pedigree to lead this effort in the future. Second, these government defence laboratories are not motivated by profit margins or meeting stockholder expectations, so they serve as “honest brokers” in tailoring solutions to the navies they support. This is especially important in developing, fielding and supporting C4ISR systems, for while ships, submarines, and aircraft are built by a discrete number of companies, virtually every large contractor will say that they are in the business of providing C4ISR solutions – and they are – but far-too-often there is a wide chasm between the solution they want to provide and the needs of the navies concerned.

The mandate for government defence laboratories to lead the development of C4ISR capabilities for their respective navies and help co-evolve these systems for the five AUSCANNZUKUS nations is strong in each of these nations, and raises the bar for what these laboratories are expected to accomplish. With this as a mandate, it is important to examine just how these government defence laboratories spread across five nations and three continents can effectively work together to ensure that their navies can network seamlessly for the next 100 years.

### **Out of the Labs: Achieving Coalition Networking**

“In today’s world, it is *inconceivable* that *anything* could be accomplished outside of coalition operations.”<sup>22</sup>

Dr. David Alberts  
Keynote address at the 7<sup>th</sup> Annual International Command and  
Control Research and Technology Symposium  
September 2002

Few would argue that the challenges to achieving effective networking at sea and to devising and co-evolving C4ISR systems for navies – even navies with such similar traditions, platforms and technologies as the five AUSCANNZUKUS nations – are simple to solve or demand anything less than a full-on effort on the part of government defence laboratories to work together to address these challenges.

However, the scientists and engineers working in these government defence laboratories also recognize that the ways and means for them to work with their colleagues in other nations must be well-developed and robust enough to ensure a coordinated effort. A primary means for accomplishing this work is through bilateral agreements between two nations in the form of Defence Exchange Agreements (DEA) or Information Exchange Agreements (IEA).

At the principal researcher level up through the leadership levels of these laboratories, scientists and engineers are keen to use these bilateral DEAs or IEAs to facilitate their work with their fellow scientists and engineers in laboratories in the other AUSCANNZUKUS nations. But the task of devising a DEA or IEA and then getting it approved through a substantial review chain in the respective nations involved is not a trivial task. We have first-person experience working these DEAs and IEAs in our respective laboratories and know forging these agreements is a time-consuming process and the time-lag in conjuring up the need for a DEA or IEA and having it approved and “in place” is often substantial. And once complete, these agreements are most often between just two nations.

Fortunately for AUSCANNZUKUS nations, recognizing the shared interests these five nations have, as well as the somewhat-limiting nature of bilateral exchange agreements, the respective governments have put in place a network of agreements that enable liberal exchanges of scientific and engineering information at the laboratory level. This network of agreements is captured in a not-well-known publication called *The Beginners Guide to the Technical Cooperation Program* which provides further links that explains the purpose and construct of each of these organizations in more detail.<sup>2 3</sup> While a full description of the work of these groups is beyond the scope of this paper, a listing of these groups is provided below:

- ASIC: Air & Space Interoperability Council (Australia, Canada, New Zealand, United Kingdom, United States) – focused on aerospace interoperability.
- ABCA: American, British, Canadian, & Australian Armies (Australia, Canada, United Kingdom, United States) – focused on Army interoperability.
- AUSCANNZUKUS (Australia, Canada, New Zealand, United Kingdom, United States) – focused on naval command, control, communications, and computers.
- CCEB: Combined Communications Electronics Board (Australia, Canada, New Zealand, United Kingdom, United States) – focused on military command, control and communications.
- MIC: Multinational Interoperability Council (Australia, Canada, New Zealand, United Kingdom, United States) – focused on military interoperability.
- MIP: Multilateral Interoperability Program (Australia, Canada, United Kingdom, United States) – focused on command, control, and interoperability.
- TTCP: The Technical Cooperation Program (Australia, Canada, New Zealand, United Kingdom, United States) – focused on military science and technology

Our personal and professional experience – while intersecting and mapping to several of the organizations above – is primarily focused on our years-long work on Technical Cooperation Program teams. Understanding how these teams evolved and focused this work in developing a way ahead for effective coalition networking at sea is necessarily preceded by an understanding of The Technical Cooperation Program writ large.

### *The Technical Cooperation Program*

“Our prime multilateral science and technology relationship is through The Technical Cooperation Program with the United States, United Kingdom, Canada and New Zealand.”<sup>2 4</sup>

*Defending Australia in the Asia Pacific Century: Force 2030*

Although it has been around in various forms for almost half a century, The Technical Cooperation Program (TTCP) is not universally well known, even by Commonwealth naval personnel, and some background is in order to explain how this program facilitates efforts to address coalition interoperability. Importantly, while conducting this sort of analysis in other fora is certainly *possible*, the extant TTCP organization and infrastructure provides a ready-made medium that makes success in these multinational collaborative endeavors *probable*.

TTCP is a forum for defence science and technology collaboration between Australia, Canada, New Zealand, the United Kingdom, and the United States. It is the largest collaborative defence science and technology activity in the world. The statistics alone give some indication of the scope of this effort: five nations involved; 11 technology and systems groups formed; 80 technical panels and action groups running; 170 organizations involved; and 1200 scientists and engineers directly accessed. By any measure, TTCP is a broad-based effort that tremendously facilitates science and technology cooperation among the five member nations.

On October 25, 1957, the President of the United States and the Prime Minister of Great Britain made a Declaration of Common Purpose containing the following:

The arrangements which the nations of the free world have made for collective defense and mutual help are based on the recognition that the concept of national self-sufficiency is now out of date. The countries of the free world are inter-dependent and only in genuine partnership, by combining their resources and sharing tasks in many fields, can progress and safety be found. For our part we have agreed that our two countries will henceforth act in accordance with this principle.<sup>2 5</sup>

Immediately afterward, the Canadian Government subscribed to this principle of interdependence and joined in the common effort. The resulting organization was called the Tripartite Technical Cooperation Program (TTCP). As a result, the WWII-era Combined Policy Committee (CPC) was reconstituted and the Subcommittee on Non-Atomic Military Research and Development (NAMRAD) was established. It comprised the heads of defence research and development organizations in Canada, the United Kingdom, and the United States. Australia joined the NAMRAD Subcommittee in 1965, and New Zealand joined in 1969, at which point the organization governed by the Subcommittee was renamed The Technical Cooperation Program (TTCP).

The aim of TTCP is to foster cooperation within the science and technology areas needed for conventional (i.e., non-atomic) national defence. The purpose is to enhance national defence and

reduce costs. To do this, TTCP provides a formal framework that scientists and technologists can use to share information amongst one another in a streamlined manner. And as noted in *Defending Australia in the Asia-Pacific Century: Force 2030*, TTCP is the *prime* multilateral science and technology relationship used by the Australian Defence Force.<sup>2 6</sup>

Collaboration within TTCP provides a means of acquainting the participating nations with each other's defence research and development programs so that each national program may be adjusted and planned in cognizance of the efforts of the other nations. This process avoids unnecessary duplication among the national programs, promotes concerted action and joint research to identify and close important gaps in the collective technology base, and provides nations with the best technical information available.

TTCP has its centre of gravity in the applied research domain, but it also encompasses basic research and technology development activities. The scope includes the exploration of alternative concepts prior to development of specific weapon systems, collaborative research, sharing of data, equipment, material and facilities, joint trials and exercises, and advanced technology demonstrations. Cooperation within TTCP often acts as the catalyst for project-specific collaborations further down the equipment acquisition path.

TTCP consists of three levels and thus has a streamlined hierarchy that promotes five-nation cooperation. Level 1 is the strategic policy level and comprises three groups of personnel: the Principals; the Deputies; and the Secretariat. Each nation has one representative to each of these groups, with the exception that the Australian Deputy also acts as the New Zealand Deputy. The Principals make up the NAMRAD Subcommittee. The Deputies and Secretariat are all based in Washington, D.C., and collectively form the Washington Staff.

Level 2 is the program planning and oversight level and currently contains 11 Groups, each focused on a particular technology or systems area. The Groups have an Executive Chair (appointed from any one of the nations), up to five National Representatives, and a number of Technical Advisors. Finally, each Group has one Deputy assigned to act as its Group Counselor (GC), who works with the Group to help communicate the Principals' strategic direction. The Groups are: Aerospace Systems; Command, Control, Communications and Information Systems; Chemical, Biological and Radiological Defense; Electronic Warfare Systems; Human Resources and Performance; Joint Systems and Analysis; Land Systems; Maritime Systems; Materials and Process Technologies; Sensors; and Conventional Weapons Technology.

Level 3 contains bodies that sit under each Group and actually perform the collaborative activities. There are three types: the semi-permanent Technical Panels (TPs); the temporary Action Groups (AGs); and the project-specific Project Arrangements (PAs). Technical Panels are designed to manage a continuing program of work and will generally oversee a number of subordinate activities. Action Groups are initiated to investigate a specific issue and, on completion, will recommend if and how any further work on the subject should be undertaken on a more permanent basis. Project Arrangements are a more binding form of cooperation, used to support a specific project or collaboration.

Technical Panels and Action Groups have a Chair, plus National Leaders for each participating nation and a varying number of Team Members. Not all nations participate in all TPs or AGs. The majority of personnel involved in TTCP operate at or in support of Level 3. The structure at Level 3 can and should evolve to remain relevant. Groups have the authority to initiate and terminate TPs and AGs, although the changes must be notified to the Principals at their next annual meeting.

TTCP operates by sharing the output from existing national science and technology programs for the greater benefit of the participating nations. It is therefore fundamentally a bottom-up organization, with collaborations occurring only where national programs and a willingness to cooperate already exist. The role of the Principals and National Representatives in managing TTCP therefore takes two forms: directing collaborations within areas where suitable national programs already exist; and directing their own national programs in order to provide the basis for future TTCP collaborations. TTCP is thus a “best endeavors” organization and can only be as good as the underpinning national programs.<sup>2 7</sup>

Today, TTCP operates under an updated Declaration of Common Purpose that informs the efforts of the organization’s Technical Panels and Action Groups. This declaration states:

No member nation possesses the total resources to provide for its own defense research and development (R&D) needs. Each must assist the others by sharing resources and tasks in many fields so that all can find progress and security. The aim of TTCP then is to foster such cooperation in the science and technology (S&T) needed for conventional national defense. The purpose is to enhance national defense at reduced cost.<sup>2 8</sup>

With this description of TTCP as background, we are ready to understand the work that has been conducted under the auspices of the Maritime Systems Group (MAR) Action Group 1 (AG-1) Net-Centric Maritime Warfare Study and Action Group 6 (AG-6) FORCENet Implications for Coalitions. This work goes directly to the issue described in the title of this paper: *Commonwealth Naval Cooperation: Are We Ready for the Next 100 Years?* and reports on the past six-plus years of activities and the way ahead for the ongoing research of this group.

#### *One-Example of Commonwealth Labs – Plus the United States - Finding Networking Solutions*

“The Technical Cooperation Program (TTCP), a longstanding forum for defence science and technology cooperation between Australia, Canada, New Zealand, the United Kingdom and the United States, has, for example, established an initiative to consider the ‘FORCENet Implications for Coalition Partners’”<sup>2 9</sup>

Dr. Chris Rahman  
*The Global Maritime Partnership Initiative:  
Implications for the Royal Australian Navy*

#### *Action Group 1 (AG-1) Net-Centric Maritime Warfare Study*

Much has been written, primarily from a qualitative perspective, about the perceived benefits to the military of transforming from a platform to a network-centric force structure.<sup>3 0</sup> However, few such studies have taken an analytic view and produced quantitative results, and fewer still have done so in the context of broadly based coalition operations.<sup>3 1</sup> In response to a mutually perceived need, the five allied countries of TTCP Maritime Systems Group established an Action Group One (AG-1) in 2001 to conduct a three-year (October 2001 to September 2004) “Network-Centric Maritime Warfare (NCMW)” collaborative study. The objectives of this study were to provide TTCP MAR Group, as well as national military customers, with guidance and analysis on the implications of NCMW for

coalition maritime force capabilities, C4I interoperability, and to help shape national acquisition strategies.

The Terms of Reference (TOR) for AG-1 charged the group to examine and help establish the foundational first principles of force netting from a coalition and distributed systems perspective, and to research the analysis methods needed to quantify the benefits of netting in coalition operations. Armed with the TOR, as part of its study definition, AG-1 members consulted with national and international military staffs to determine a priority list of issues to address. Ultimately, the group decided to analyze and quantify the military utility of selected parametric levels of network-centric capabilities by addressing tactical information exchange, in rigorous analytical detail, for three selected tactical situations associated with coalition maritime littoral warfare: Maritime Interception Operations (MIO), Anti-Submarine Warfare (ASW), and Anti-Surface Warfare/Swarm Attack (ASuW-Swarm).

AG-1 first met in October 2001 to review and understand the TOR and to map out methodology to address the MAR guidance. The group decided that to address the issue of NCMW properly, two studies were needed: Study A, a broadly-based higher level study addressing overarching NCMW analytical issues and “first principles” of force networking from a coalition and distributed systems perspective; and Study B, an in-depth focus on the three tactical situations noted above that, together, represented a spectrum of different types of coalition-force maritime tactical situations of high interest to the TTCP nations.

Understanding the *process* of selecting these studies provides insight into the dynamics of international cooperation in science and technology under the auspices of TTCP. Study A, the broad area study, selected operational planning and intelligence, surveillance, and reconnaissance (ISR) as the area of focus because all five coalition partners participated in to one extent or another. For Study B, the range of tactical situations to select from was quite extensive. One of the first orders of business for AG-1 was to conduct a survey of coalition contingency operations that occurred most frequently among the member nations. Once this list was compiled and the list of possible tactical situations to examine was narrowed, this candidate list was vetted with uniformed AUSCANNZUKUS professionals from the five member nations. Ultimately, three mission areas, MIO (maritime interception operations), ASW (anti-submarine warfare) and ASuW (anti-surface warfare – specifically against the swarming small boat threat), were selected for study. Additionally, and serendipitously, for each of these warfare areas, the partnership among the five nations was on a more-or-less equal footing.

While a full report on AG-1 efforts and results is beyond the scope of this paper, and releasability issues preclude directly citing many TTCP MAR AG-1 documents, it is instructive to understand the *process* that AG-1 used to obtain their results in order to have a clear window on this effort and to understand the “best practices” this group used to inform future efforts of this nature.<sup>3 2</sup> Significantly, in addition to investing substantial effort to select focus areas where all coalition partners were on an essentially equal footing, the study participants conducted due diligence in order to review and understand the various analysis methodologies available to conduct AG-1’s work. In fact, one of the AG-1’s early reports provided an extensive review of analytic techniques appropriate for the group’s work, and the contents of this report informed each of the studies undertaken by MAR AG-1.<sup>3 3</sup>

Armed with an agreement regarding the studies to be conducted and in possession of a number of analytic techniques that might be appropriate to apply to both Study A and Study B, MAR AG-1 set about addressing the MAR direction expressed in the TOR and conducted the two major studies in parallel. Within Study B, MIO, ASW, and ASuW were addressed in that order. Significantly, no one

nation provided all of the analytical techniques and tools that were ultimately applied. Rather, for each study, the group drew upon the analytical expertise of each member from a “nation-blind” perspective and ultimately selected the analytical technique most appropriate to the tactical situation at hand. Fortuitously, the operational requirement of the various tactical situations drove the team to select a mix of analytical techniques for the studies, ensuring that the work of the team was not narrowly focused on the preferred analytical methodology of any one nation.

The results of Study A were significant and important to the overall conduct of Network Centric Maritime Warfare and stemmed from the hypothesis that NCW is the core concept for enabling a new revolution in military affairs for the information age. This concept postulated that greatly increased combat power derives from the ability of highly connected system of entities, widely distributed throughout the battlespace dimensions of space, time, force, information, and cognition, to rapidly concentrate influences to deliver decisive effects on an enemy while minimizing the exposure of friendly entities.

Importantly from the standpoint of addressing the next 100 years of Commonwealth Cooperation, Study A was also based on the proposition that the complexity of the netted force will demand a co-evolution of systems, technology, and doctrine. It also noted that while force experimentation has been adopted as a co-evolution mechanism, it is not feasible to explore the requisite paths by experimentation because attempts to do so yield heuristics that create a risk of misunderstanding the gap between experiment-observed and battlespace-realized capability. Thus, Study A showed that appropriate analytical methods need to be applied to adequately explore the problem space in a timely, tractable, and affordable manner. Further, it showed that these may be based on systems-engineering techniques, but the conceptual description of distributed networked systems and their behavior requires further development before systems-engineering principles can be applied.

Thus, Study A mapped the broad parameters and issues that are addressed in quantitative modeling of NCW. It also showed that conceptualizing NCW requires paying much more attention than heretofore to the information and cognitive domains of warfighting – domains that have always been important – but have not had much analytical attention to date. Study A further noted that models of NCW must include representations of information, the manner in which it arises from data generated in the physical domain and its flow around the information domain.<sup>3 4</sup>

With Study A providing the broad, overarching underpinnings of the work of AG-1, the team undertook detailed analysis of the three aforementioned tactical situations (MIO, ASW and ASUW/Swarm). These TACSITS were each carefully designed to strike a balance to enable them to be generic enough to be of general relevance but also specific enough to support and inform each nation’s requirements-generation process and acquisition programs. This careful sculpting and dimensioning of each TACSIT was a key factor that enhanced Study B’s utility to each nation in particular and to the analytical community in general. A full description of these TACSITS and their development is well beyond the scope of this paper, but is part of the body of work maintained by the Command and Control Research Program.<sup>3 5</sup>

But as AG-1’s three-year tenure expired and team leader and Chairman, Ray Christian, reported the team’s results to the MAR leadership, an unusual thing happened. These senior leaders – representing all five AUSCANNZUKUS – recognized the value of this work and the importance of continuing to study and analyze the issue of networking maritime coalitions. Roughly concurrently, the U.S. Navy decided to make a major capital investment in FORCENet. Therefore, the MAR leadership directed the



standup of a new action group to focus specifically on the impact of coalition partners – the four Commonwealth nations – working with the U.S. Navy in a FORCENet environment.

### Action Group 6 (AG-6) FORCENet Implications for Coalitions

AG-6 took the MAR Terms of Reference (TOR) and developed three premises and a hypothesis to inform its work. The first premise, derived from the Naval Network Warfare Command's Capstone Document, *FORCENet: A Functional Concept for the 21<sup>st</sup> Century*, was that FORCENet will empower warfighters at all levels to execute more effective decision-making at an increased tempo, which will result in improved combat effectiveness and mission accomplishment.<sup>3 6</sup> The second premise, derived directly from the MAR TOR, was that the warfighting benefits of FORCENet in a coalition context can be assessed through analysis and quantified to provide input to national balance of investment studies of the five member nations. The third premise, derived from the aforementioned United States Navy Fleet Commanders' top C4ISR priorities, was that it is necessary that FORCENet address current and near term information system requirements that support operations in the joint and coalition environments. Coalition Communications was the clear number one priority of all numbered fleet commanders and is a critical enabler in leveraging coalition partners in the global war on terrorism.

Based on these premises, AG-6 developed a working hypothesis that has informed its work from the outset. This hypothesis: "Conducting modeling and simulation and detailed analysis to demonstrate the enhanced warfighting effectiveness of coalition partners (in this case – the AUSCANNZUKUS nations) netted in a FORCENet environment can help inform national naval C4ISR acquisition programs," not only set the tone for the group's work, but also provided visibility throughout the naval establishments of all five member nations regarding the group's efforts. The compelling nature of this hypothesis has caused other organizations not initially involved in AG-6's work to "jump on board" and join this team.

The full details of AG-6's efforts are beyond the scope of this paper. Briefly, a scenario was devised which coalition partners might likely participate in, one that began as disaster assistance/humanitarian relief, then morphed into a counterterrorism effort, and ultimately turned into high-tempo conflict at sea. Then, four principal measures of effectiveness were devised to measure the effectiveness of a robustly networked coalition force that fully leveraged the U.S. Navy's FORCENet capability over one that was not networked. These were Time to Capability (number of major amphibious units delivered on time in the area of operations); Economy of Effort (cost of munitions, fuel and other consumables used in the campaign); Risk (blue attrition in all phases of the campaign: assembly; littoral transit; anti-submarine warfare; anti-surface warfare; anti-air warfare; offload; naval fire support; and mine warfare); and Campaign Success (success in the aforementioned campaign phases and ultimately, the safe delivery of "campaign effectors" the landing force ashore).

AG-6 has generated analytical data and conducted modeling and simulation to demonstrate that if the U.S. Navy's FORCENet is developed in a way that is inclusive of likely coalition partners, who, in turn, build their national systems to be compatible with FORCENet, the naval forces involved will enjoy a quantum increase in capability. Team members were universal in their agreement that this message needed to be carried forward to the national defence leadership of each of the five nations involved.

Concurrently, the AG-6 members liberally shared the "technology on-ramps" of their acquisition communities to find those windows where similar technological capabilities could be inserted into

their naval C4ISR systems. By modeling the planned capabilities of these “on ramps” against the scenario, the impacts and value of alternative coalition network structures was assessed. The resulting analysis was presented to MAR principals at when the AG-6 team leader and chairman, Mr. Don Endicott, briefed the team’s results to the MAR leadership. The study’s results are currently being used by AG-6 members to make detailed C4ISR technology procurement recommendations in their respective countries.

The advantages that can accrue to the world’s peace-loving nations by leveraging the tremendous investment the U.S. Navy is making in FORCENet cannot be overstated. Far from a U.S. Navy-only standard, FORCENet – and especially a currently-fielded prototype called “Composeable FORCENet – is a publish-and-subscribe system based on open architecture and open standards that other nations can leverage with minimal investment.<sup>37</sup> An analogy familiar to most nations in the Pacific Rim involves Singapore. In 1998, Singapore made an enormous investment in the Singapore ONE project, which provided broadband infrastructure of high capacity networks and switches, with the goal of providing broadband access to the entire nation.<sup>38</sup> Singapore then went out to the international business community and said, in essence, “Come join us. We have made the investment in building a world-class infrastructure. This is a great home for your business.” Attracted by that world-class infrastructure, those businesses did come, and Singapore’s standing as a hub for international business and as a strong node in the Asian economy is a matter of record.<sup>39</sup> The question AG-6 raised – and a question that the MAR leadership wants addressed by AG-6’s successor group, AG-11 – is whether FORCENet can play a similar role in the development of maritime coalition capabilities.

Beyond the strong endorsement by the MAR principals to continue the AG-1/AG-6 efforts for another three years, the initial reviews of TTCP MAR AG-1/AG-6’s work within the naval and defence establishments of the five nations has been overwhelmingly positive. Within the U.S. Navy, in particular, one measure of the group’s success is the number of organizations – The Office of Naval Research, The Naval War College, The Naval Postgraduate School, and others – who have placed members on and who are vested in the ongoing work of this team because they recognize the importance of its work.

As AG-6 transitions to AG-11, the TTCP model continues to provide a means for the laboratory communities in the nations that will likely work together at sea to analyze technical communication and networking needs in an operational framework. The application of the TTCP model to current and future efforts to build effective coalition communication networks can be an important step in enabling Commonwealth nations to operate and cooperate at sea in this century.

## **A Way Forward?**

“A new idea is first condemned as ridiculous and then dismissed as trivial, until finally, it becomes what everyone knows.”

William James – 1879

“Conversely, operators often resist network- or picture-centric forms of warfare because they seem unnatural.”<sup>40</sup>

Norman Friedman  
*Network Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars*

The last 100 years of naval cooperation have resulted in a level of excellence in peace and in war that has set the standard for navies and nations to emulate. The bar has indeed been set high for the next 100 years of naval cooperation, cooperation that now includes the United States as an important partner.

As the AUSCANNZUKUS nations take a leadership role in securing the global commons as part of the nascent Global Maritime Partnership, effective networking among these allied and coalition nations will be an absolute requirement if the navies of these nations are to achieve anything worthwhile beyond just showing up in the same oceanic area at the same time.

This paper has demonstrated that if the five AUSCANNZUKUS nations turn to their defence science and technology organizations as primary stewards of conceiving and fielding compatible C4ISR systems for their respective nations, this will result in the best possible results as these government defence laboratories have a shared responsibility to deliver naval operators of the partner nations the best possible C4ISR systems – and most importantly – systems that are compatible with other AUSCANNZUKUS navies as well as with other likely coalition partners.

And this paper has also shown that there are many extant “five-eyes” organizations and taxonomies that greatly facilitate cooperation among the partner nations. At the science and engineering level, TTCP offers arguably the best forum for this ongoing cooperation. The experience of the TTCP group MAR AG-1/AG-6/AG-11 offers a bedrock and a best-practices example as a way ahead to ensure that Commonwealth/AUSCANNZUKUS naval operations in *this* century are the most effective they can possibly be.

---

<sup>1</sup> Admiral Gary Roughead, remarks as delivered at the Surface Navy Association Symposium Banquet, January 14, 2010, Chrystal City, VA. Accessed at Internet <http://www.navy.mil/navydata/people/cno/Roughead/Speech/100115%20CNO%20remarks%20at%20SNA%20Symposium.doc>.

<sup>2</sup> *Proceedings of the 2007 King Hall Naval History Conference*, accessed at: [www.navy.gov.au/spc/](http://www.navy.gov.au/spc/).

<sup>3</sup> Norman Friedman, “Netting and Navies, Achieving a Balance,” in *Sea Power: Challenges Old and New* (Sydney, Australia, Halstead Press, 2007), pp. 185-186. This publication provides the proceedings of the 2006 Royal Australian Navy Sea Power Conference. Dr. Friedman is an internationally-recognized expert on naval matters who speaks frequently at international symposia on network-centric operations. As Dr. Friedman points out, Admiral Fisher used the information gleaned from shipping reports and reports from his own fleets to build a tactical picture of where pirates were attacking British merchant ships. Information from these sources was fed into two different war rooms—the first war room tracked ship movements around the world while the second war room tracked ship movements in the North Sea. Armed with this “picture-based” view of the world, Admiral Fisher was able to direct warships to the spots where British ships were being attacked by pirates. See also, Norman Friedman, *Network-Centric Warfare: How Navies Learned to Fight Smarter through Three World Wars* (Annapolis, Maryland, Naval Institute Press, 2009).

<sup>4</sup> “A Global Network of Nations for a Free and Secure Maritime Commons,” *Report of the Proceedings of the 17<sup>th</sup> International Seapower Symposium*, 19-23 September 2005, accessed at: [www.nwc.navy.mil/cnws/marstrat/docs/library/ISS17web.pdf](http://www.nwc.navy.mil/cnws/marstrat/docs/library/ISS17web.pdf) >. The present day concept of a global maritime partnership can be traced back to Admiral Michael Mullen’s tenure as U.S. Navy Chief of Naval Operations. His original concept of “The 1000-Ship Navy”—a global navy composed of 1000 or more ships working cooperatively—evolved into the Global Maritime Partnership. Admiral Mullen introduced the concept at the 2005 International Seapower Symposium in Newport, Rhode Island, stating: “As we combine our advantages, I envision a thousand-ship navy—a fleet-in-being, if you will—made up of the best capabilities of all freedom-loving navies of the world...This thousand-ship navy would integrate the capabilities of the maritime services to create a fully interoperable force, an international city at sea.” See also George Galdorisi and Stephanie Hszieh, “Speaking the Same Language,” *U.S. Naval Institute Proceedings*, March, 2008, pp. 56-60

---

for a discussion of the origins of the Global Maritime Partnership concept that began with then Chief of Naval Operations Admiral Michael Mullen's introduction of the 1000-Ship Navy concept at the 2005 International Seapower Symposium.

<sup>5</sup> Rahman, *The Global Maritime Partnership Initiative: Implications for the Royal Australian Navy*, p. 6. Dr. Rahman writes authoritatively about the technical aspects on naval interoperability, noting; "Technical impediments to information sharing can embrace a range of factors." He uses examples of naval exercises held in the Asia-Pacific region such as RIMPAC and CARAT and the experiences of coalition partners such as Australia working with the U.S. Navy Combined Enterprise Regional Exchange System (CENTRIXS) to demonstrate that much technical (as well as policy and security) work remains to be done before coalition navies can communicate and exchange data in a way that facilitates a robust global maritime partnership (pages 36-43). See also, Brad Carter and Deb Harlor, "Combined Operations Wide Area Network (COWAN)/ Combined Enterprise Regional Information Exchange System (CENTRIXS)," *Biennial Review* (San Diego, CA: Space and Naval Warfare Systems Center San Diego, 2003), p. 87, for a detailed technical description of CENTRIXS. See also, Gordon Van Hook, "How to Kill a Good Idea," *United States Naval Institute Proceedings*, October 2007, p. 34 for an operational perspective on the CENTRIXS system. Captain Van Hook notes the limitations of CENTRIXS, stating: "We must move beyond limited approaches to link a few secure common systems with software applications like CENTRIXS, and get to a fully integrated regional picture from ports to harbors and into the commons."

<sup>6</sup> N.A.M. Rodger, presentation at the Royal Australian Navy King-Hall Naval History Conference, Sydney /Canberra, Australia, 24 and 26-27 July 2007, p. 6.

<sup>7</sup> It is difficult to overstate the importance of the invention of the telegraph. For the first time ever, it was possible to move information faster than people or goods. Therefore it is not difficult to understand how proponents – as well as users – of the telegraph did not thoughtfully consider the unintended consequences of its use.

<sup>8</sup> Rodger, presentation to King-Hall Conference, Canberra, January 24, 2007 (from Galdorisi notes transcription).

<sup>9</sup> N.A.M. Rodger, presentation at the Royal Australian Navy King-Hall Naval History Conference, Sydney /Canberra, Australia, 24 and 26-27 July 2007, p. 10.

<sup>10</sup> Paul Mitchell, "Small Navies and Network-centric Warfare: Is There a Role?" *Naval War College Review*, Spring 2003, pp. 83-99.

<sup>11</sup> Lieutenant Commander Chris Watson, "How Might the World's Navies Contribute to and Benefit from the '1000-Ship Navy Proposal?," *Australian Maritime Issues 2007* (Canberra, Australia, Department of Defence Sea Power Centre, 2008) p. 237. In his Peter Mitchell Essay Competition winning article, Lieutenant Commander Watson highlights the significant issues that come with navies of differing sizes and different agendas achieving effective networking and information sharing.

<sup>12</sup> *The National Military Strategy of the United States of America* (Washington, D.C.: U.S. Government Printing Office, 2004).

<sup>13</sup> United States Navy battle formations are most often deployed as Carrier Strike Groups (CSG) or as Expeditionary Strike Groups (ESG). CSGs are built around a large-deck aircraft carrier operating tactical jet aircraft, and ESGs are built around a large-deck amphibious ship operating VSTOL aircraft and helicopters.

<sup>14</sup> See, Paul Mitchell, "Small Navies and Network-centric Warfare: Is There a Role?" *Naval War College Review*, Spring 2003, pp. 83-99.

<sup>15</sup> Mitchell, "Small Navies and Network-Centric Warfare: Is there a Role?" pp. 88-89.

<sup>16</sup> Paul Mitchell, "Small Navies and Network-centric Warfare: Is There a Role? Canada and U.S. Carrier Battlegroup Deployments," briefing presented at the 8<sup>th</sup> International Command and Control Research and Technology Symposium, Washington, D.C., June 17-19 2003. Professor Mitchell's statement did not come from his prepared presentation, but from the question and answer period following his formal presentation.

<sup>17</sup> *Military Transformation: A Strategic Approach* (Washington, D.C.: Department of Defence, 2003), pp. 1-36, accessed at: [www.oft.osd.mil](http://www.oft.osd.mil). This publication is the capstone publication of the Office of Force Transformation, U.S. Department of Defence.

<sup>18</sup> Admiral James Stavridis, "Deconstructing War," *U.S. Naval Institute Proceedings*, December 2005.

<sup>19</sup> Norman Friedman, *Network Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars* (Annapolis, Maryland, U.S. Naval Institute Press, 2009), p. ix.

<sup>20</sup> For more on FORCENet see the following: *FORCENet: A Functional Concept for Command and Control in the 21<sup>st</sup> Century* (Norfolk, VA: Naval Network Warfare Command, 2006) and *FORCENet: A Functional Concept for Command and Control in the 21<sup>st</sup> Century: Annex Version 20 June 2006* (Norfolk, VA: Naval Network Warfare Command, 2006), both available at [www.enterprise.spawar.navy.mil/getfile.cfm?contentId=816&type=R](http://www.enterprise.spawar.navy.mil/getfile.cfm?contentId=816&type=R).

<sup>21</sup> Van Hook, "How to Kill a Good Idea," p. 33. Captain Van Hook, drawing on his experience as a destroyer squadron commander where he worked with coalition partners, emphasized the importance of a cooperative approach to instantiating the global maritime partnership, noting that the U.S. should; "Encourage regional maritime security arrangements to form at the grassroots level, without overt U.S. leadership."

---

<sup>2 2</sup> Dr. D. Alberts, keynote address at the 7<sup>th</sup> Annual International Command and Control Research and Technology Symposium, September 16, 2002, Washington, D.C., accessed at Internet [www.dodccrp.org](http://www.dodccrp.org).

<sup>2 3</sup> The Technical Cooperation Program: TTCP document DOC-SEC-3-2005, *A Beginner's Guide to the Technical Cooperation Program*, September 1, 2005, accessed at: [www.dtic.mil/ttcp/](http://www.dtic.mil/ttcp/). This document published on The Technical Cooperation Program's public website, is a concise explanation of TTCP's structure and purpose, as well as a useful capture of the purpose of other "five-eyes" organizations.

<sup>2 4</sup> *Defending Australia in the Asia Pacific Century: Force 2030*, p. 136.

<sup>2 5</sup> The Technical Cooperation Program: TTCP document DOC-SEC-3-2005, *A Beginner's Guide to the Technical Cooperation Program*, September 1, 2005.

<sup>2 6</sup> *Defending Australia in the Asia Pacific Century: Force 2030*, p. 136.

<sup>2 7</sup> TTCP, *A Beginner's Guide*, 2005.

<sup>2 8</sup> TTCP, *A Beginner's Guide*, 2005.

<sup>2 9</sup> Rahman, *The Global Maritime Partnership Initiative: Implications for the Royal Australian Navy*, p. 36.

<sup>3 0</sup> Importantly, some of this qualitative work has addressed coalition operations, confirming the importance of networking in the multi-lateral operations. See, for example, D. Gompert et al, *Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs* (Washington, D.C.: National Defence University Press, 1999); J. Thomas, *The Military Challenges of Transatlantic Coalitions*, Adelphi Paper 333 (London: IISS, 2000); G. Adams, "Strength in Numbers: The European Allies and American Defence Planning," in  *Holding the Line: U.S. Defence Alternatives for the Early 21<sup>st</sup> Century*, ed. Cindy Williams (Cambridge, MA: MIT Press, 2001); and G. Adams et al, *Bridging the Gap: European C4ISR Capabilities and Transatlantic Interoperability*, Defence and Technology Paper 5 (Washington, D.C.: National Defence University Press, 2004). These studies, and others like them, emphasize the importance of coalition operations and, by extension, coalition partners operating in a networked fashion.

<sup>3 1</sup> While little quantitative work on network-centric operations has been done based on from-the-ground-up modeling and simulation, the United States Assistant Secretary of Defense for Networks and Information Integration (ASD NII), under the auspices of the Command and Control Research Program (CCRP), has reviewed the results of both exercises and wartime events to draw some quantitative results regarding the value of networking. MAR AG-1 and AG-6 reviewed this CCRP material in evaluating "best practices" for the conduct of their studies, and this CCRP work informed much of the group's work. See [www.dodccrp.org](http://www.dodccrp.org) to access the totality of the CCRP effort, including several books that describe these early efforts to quantify the benefits of networking.

<sup>3 2</sup> Some TTCP MAR AG-1 reports, including the final *Network-Centric Maritime Warfare Study Capstone Report* (TR-MAR-12-2004) are labeled "For Official Use Only" because the document(s) "Contain information that is provided in confidence to the TTCP Governments." However, some of these reports do allow for unlimited distribution. Due to the focused outreach efforts by MAR AG-1, the results of the team's work were reported in open venues such as the International Command and Control Research and Technology Symposia (ICCRTS).

<sup>3 3</sup> Ian Grivell et al., *A Review of Analytic Techniques Applicable to the Study of Network Centric Warfare*, TTCP TR-MAR-9-2003, May 2003.

<sup>3 4</sup> Chris Davis et al., *Key Issues in Coalition Network-Centric Maritime Warfare*, TTCP TR-MAR-10-2003, January 2004.

<sup>3 5</sup> See George Galdorisi and Darren Sutton, "A Technical Approach to Coalition Interoperability," paper presented at the 11<sup>th</sup> International Command and Control Research and Technology Symposium, Cambridge, United Kingdom, September 2006, accessed at [www.dodccrp.org](http://www.dodccrp.org). See also Mark Hazen et al., "The Analysis of Network-Centric Maritime Interception Operations (MIO) Using Queuing Theory," presentation at the 8<sup>th</sup> International Command and Control Research and Technology Symposium, Washington, D.C., June 17-19, 2003; Ralph Klingbeil et al., "Utilizing Network-Enabled Command and Control Concepts to Enhance ASW Effectiveness," presentation at the 9<sup>th</sup> International Command and Control Research and Technology Symposium, Copenhagen, Denmark, September 14-16, 2004; and David Galligan et al., "Net Centric Maritime Warfare – Countering a "Swarm" of Fast Inshore Attack Craft," presentation at the 10<sup>th</sup> International Command and Control Research and Technology Symposium, McLean, Virginia, June 13-16, 2005. These three latter papers and briefings are also accessed at [www.dodccrp.org](http://www.dodccrp.org).

<sup>3 6</sup> *FORCENet: A Functional Concept*, [www.enterprise.spawar.navy.mil/getfile.cfm?contentId=816&type=R](http://www.enterprise.spawar.navy.mil/getfile.cfm?contentId=816&type=R). See also; *A Functional Concept for Command and Control in the 21<sup>st</sup> Century* and *FORCENet: A Functional Concept for Command and Control in the 21<sup>st</sup> Century: Annex Version 20 June 2006*. See also, Admiral Vern Clark, "Sea Power 21: Projecting Decisive Joint Capabilities," *U.S. Naval Institute Proceedings*, October 2002; and Vice Admiral Richard Mayo and Vice Admiral John Nathman, "FORCENet, Turning Information into Power," *U.S. Naval Institute Proceedings*, February 2003.

<sup>3 7</sup> See Jeffrey Clarkson, George Galdorisi, Jeffrey Grossman, Michael Reilley and Christopher Priebe, "Composable FORCENet," in *SSC San Diego Biennial Review 2006* (San Diego, CA: SPAWAR Systems Center San Diego, 2006); David Alberts and Richard Hayes, *Understanding Command and Control* (Washington, D.C.: DoD Command and Control Research Program, 2006); *Department of the Navy: Information Management and Information Technology Strategic Plan* (Washington, D.C.: Department of the Navy Chief Information Officer, 2006); and George Galdorisi et al., "Composable

---

FORCEnet Command and Control: The Key to Energizing the Global Information Grid to Enable Superior Decision Making,” *Proceedings of the 2004 Command and Control Research and Technology Symposium, June 2004*, accessed at [www.dodccrp.org](http://www.dodccrp.org).

<sup>38</sup> See, for example, Kim-Song Tan and Sock-Yong Phang, "From Efficiency-Driven to Innovation-Driven Economic Growth: Perspectives from Singapore" (April 2005). World Bank Policy Research Working Paper No. 3569. Available at SSRN: <http://ssrn.com/abstract=712623>. See also Michael Kanellos, "Singapore: One Nation under Wi-Fi," *c/net news.com*, 28 August 2006, < [http://news.com.com/2100-1039\\_3-6110189.html](http://news.com.com/2100-1039_3-6110189.html) > (9 July 2007).

<sup>39</sup> Singapore has attracted a number of IT companies like Hewlett Packard and Motorola who have established an R&D division to team with Singapore companies to develop new networking technologies. Hewlett Packard's Singapore R&D division is working on next-generation networking servers and Motorola has teamed with the Singapore Design Center to work on new mobile equipment designs. (Intelligent Nation 2015 Steering Committee, "Innovation. Integration. Internationalisation," June 2006, [http://www.in2015.sg/pdf/01\\_iN2015\\_Main\\_Report.pdf](http://www.in2015.sg/pdf/01_iN2015_Main_Report.pdf) (Accessed 10 July 2007)).

<sup>40</sup> Friedman, *Network Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars*, p. 242.