11th ICCRTS

Coalition Command And Control In The Networked Era

Coalition Interoperability: How Much Is Enough and How to Quantify It

For Topical Areas

C2 Concepts and Organizations
C2 Architecture
Coalition Interoperability

Mr. George Galdorisi (Point of Contact)
Dr. Darren Sutton

Space and Naval Warfare Systems Center San Diego
Office of Science, Technology and Engineering
53560 Hull Street
San Diego, CA 92152-5001
(619) 553-2104 (voice)
George.Galdorisi@navy.mil

Coalition Interoperability:
How Much Is Enough and How to Quantify It

Abstract

The statement 'the future of warfare is coalition' implies that the past wasn't, which is patently untrue. While obviously there have been single state-on-state conflicts, in the more recent past – the last few hundred years – in the overwhelming majority of conventional state-on-state conflict, at least one side has been a coalition.

The issue is not that the future of warfare will be coalition, but the level of interoperability between those coalition forces. Historically, that level has ranged from not interoperable to relatively high interoperability. Where it existed, interoperability began at the macro level, with the independent assets assigned to a coalition activity interoperating predominantly in terms of command and control. More recently, and this is an area where naval forces have led the way, interoperability has been migrated to the tactical level through the use of, for example, link communications. Increasingly ubiquitous advanced communications technologies offer the potential to integrate at the systems level. This new capability is expected to further enhance interoperability between assets at all levels of operations.

The potential advantages of these increased 'technical' levels of interoperability are widely addressed in the Network Centric Warfare literature, and therefore this paper will not address them directly. Instead this paper will focus on the questions of 'How much interoperability is enough?' and 'How can we quantify it?'

The United States Navy (USN) has embarked on an ambitious program to develop a fully networked force. The technical means by which it will achieve this is known as FORCEnet. More recently, the USN has started to engage its allies in exploring the issue of how interoperable they will be with FORCEnet when it is delivered, and what will be the consequences, in terms of the ability to conduct particular operations, of any deficiencies in that interoperability.

To address these questions, the Maritime Systems Group (MAR) of 'The Technical Cooperation Program' (TTCP) – five-nation (Australia, Canada, New Zealand, the United Kingdom, and the United States) defense science collaboration – has established two action groups, AG-1 and subsequently AG-6. This paper will report on the progress of those groups and on the plans for the way ahead. TTCP is a well-established venue for international 'five eyes' R&D cooperation and coordination. The fact that this group operates under TTCP auspices makes it a good example of a 'process model' that can be followed by other international groups with similar goals.

Coalition Interoperability:
How Much Is Enough and How to Quantify It

'Countering global terrorism and providing humanitarian relief for natural disasters is a tall order. It will take many ships and no single nation can do it all.'[1]

Vice Admiral John Morgan, USN and Rear Admiral Charles Martoglio, USN
"The 1000 Ship Navy: Global Maritime Network"
United States Naval Institute Proceedings, November 2005

The Importance of Coalition Interoperability

Much has been written and spoken about coalition interoperability, but the quotation above, by two U.S. Navy officers at the centre of their Navy's strategy and policy formulation and execution, captures the essence of the challenge. Like-minded peace-loving nations must work together to deal with a host of challenges. Since the oceans cover 70% of the globe, much of the focus on accomplishing these missions will be at sea. To ignore the challenge of coalition networking, especially at sea, is to court disaster.

Some think of coalition warfare as something new, an artifact of the 20th century, when nations banded together twice during the century to fight aggression and totalitarianism. But this is decidedly not the case. Coalition warfare goes back over two millennia. The Peloponnesian War pitted a coalition built around Sparta against one built around Athens in a duel for mastery of what was essentially the known world at that time. Importantly, as Thucydides relates in *The History of the Peloponnesian War* and as Victor David Hanson describes more recently in *A War like No Other*, much of this coalition warfare occurred at sea.[2] That theme of coalition warfare at sea has prevailed through countless conflicts to the present day.

The importance of coalition interoperability has recently been addressed even more starkly and directly by, among others, Dr. David Alberts, Director of Research and Strategic Planning in the U.S. Office of the Assistant Secretary of Defense for Networks and Information Integration – and one of the 'intellectual heavyweights' behind the theory of network centric warfare – who has opined that: 'In today's world, it is *inconceivable* that *anything* could be accomplished outside of coalition operations.'[3] This theme is well understood within the U.S. naval service as it increasingly recognizes the importance of coalition operations. At a conference in late 2005, the heads of both the U.S. sea services articulated where coalition operations stood with respect to the U.S. sea services. U.S. Chief of Naval Operations, Admiral Michael Mullen, noted: 'The essence of the 1000 ship navy is how do we marry with our coalition partners on the global

---

[1] Vice Admiral J. Morgan and Rear Admiral C. Martoglio, 'The 1000 Ship Navy: Global Maritime Network,' *United States Naval Institute Proceedings*, November 2005, pp. 14-17.

[2] Thucydides, *The History of the Peloponnesian War* (New York: Henry Regnery Company, 1948) and Victor David Hanson, *A War Like No Other: How the Athenians and Spartans Fought the Peloponnesian War* (New York: Random House, 2005).

[3] Dr. D. Alberts, keynote address at the 7th Annual International Command and Control Research and Technology Symposium, September 16, 2002, Washington, D.C., accessed at Internet <dodccrp.org>.

commons,' while U.S. Commandant of the Marine Corps, General Michael Hagee, reflected: 'The most significant challenge to joint and coalition operations is the ability to communicate and exchange data. We shouldn't be fixing this on the fly when we cross the line of departure.'[4]

From the perspective of the United States Navy, coalition operations are an increasingly important consideration. This comes not from 'policy wonks' or from those working in various parts of the shore establishment, but from the operators, those 'on point' and charged with achieving mission success when undertaking an important operation with coalition partners. Each year, the five numbered fleet commanders in the United States Navy submit their 'top ten C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) requirements.' For years, these 'desirements' have been literally all over the map, with 'more bandwidth,' often taking top billing. Today, these fleet commanders are universal in identifying one C4ISR issue as their top priority – coalition communications. These warfighters recognize that the ability to communicate and exchange data with coalition partners is important to their success across a wide range of mission areas, especially as a shrinking U.S. Navy is stretched increasingly thin to carry out its myriad missions.

From our experience with colleagues in the Australian, Canadian, New Zealand, United Kingdom, and the United States navies, there is recognition at the working level that there is a need for better coalition networking, especially at sea. The discussion usually involves one or another of our colleagues saying to the U.S. member, 'Look, we want to work with you folks in the United States Navy, but we can't buy all the gear you have on your ships. What is the price of *admission* to work with you U.S. Navy guys? What do we have to buy or install so that we can communicate with you and exchange information?'

But this is only half the question. We should also be addressing this in precisely the opposite manner, asking; 'What is the price of *omission* if our navies go off and do things individually and as a consequence cannot communicate and exchange data as members of a coalition?' It was not that long ago, at the height of the Cold War, when coalition partners worked together, or in the naval parlance, steamed together, with ineffective communications. That might have been all right then, for in the Cold War standoff, there was a high premium on coalitions and alliances from a political standpoint – how many nations were on each side of the line. Sometimes it did not matter greatly whether coalition partners could actually *work together*, what was important was that each nation had chosen sides.

Today, we have moved beyond merely political considerations. While politics can never be ignored, it is now operational necessity that dictates the importance of coalition operations, and it is the operators who are saying that the price of *omission* – of having coalition partners who cannot operate together seamlessly – is far too high. This was put most directly by Admiral Robert Natter, USN, then Commander of the United States Navy's Fleet Forces Command, when he noted: 'The significant involvement of coalition forces in Operation Enduring Freedom (OEF) – including over 100 ships deployed in Central Asia for an extended period – has reemphasized

[4] Chief of Naval Operations and Commandant of the Marine Corps remarks at the 10th Annual Expeditionary Warfare Conference, October 25-27, 2005, Panama City, Florida.

the requirement for improved internet protocol data systems' interoperability with allied and coalition forces.'[5]

Admiral Natter could not have picked a more striking example. A snapshot of ships deployed to the United States Central Command's Area of Responsibility during Operation Enduring Freedom included 91 ships of 12 nations. Sixty ships belonged to one of 11 U.S. coalition partners while only 31 ships were from the U.S. Navy, one indicator of how heavily the United States depends on its coalition partners, especially in the maritime domain.[6] More recently, U.S. Marine Corps Lieutenant General Michael Mattis, Commanding General of the U.S. Marine Corps Combat Development Command, referenced this major coalition operation when he pointedly noted: 'You cannot do *anything* today without being part of a coalition. In OEF the majority of forces were coalition forces. This is a military consideration, not a political one. Coalition warfare is a reality and a fact.'[7]

Networking Coalitions is an Operational Challenge in Need of a Solution

Clearly, the available evidence suggests that like-minded peace-loving nations 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. 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.'[8]

But 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 this 'shared situational awareness?'[9] Some would say that it is not yet where it should be. Writing in the authoritative *Naval War College Review*, Professor Paul Mitchell, Director of Academics at the Canadian Forces College, asked the key question: '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'[10]

---

[5] Admiral R. Natter, Interview, *Combat Systems Clips*, Summer 2002.

[6] The coalition partner navies deployed during this snapshot in time in early 2005 included Australia, Bahrain, Canada, France, Germany, Greece, Italy, Japan, Netherlands, Spain, the United Kingdom, and the United States.

[7] Lieutenant General M. Mattis, Commanding General, Marine Corps Combat Development Command, remarks at the 10th Annual Expeditionary Warfare Conference, October 25-27, 2005, Panama City, Florida.

[8] *The National Military Strategy of the United States of America* (Washington, D.C.: U.S. Government Printing Office, 2004).

[9] 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.

[10] P. Mitchell, 'Small Navies and Network-centric Warfare: Is There a Role?' *Naval War College Review*, Spring 2003, pp. 83-99

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 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.

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 keeping 'in step' with its likely coalition partners, or even its allies, is not high – absent enlightened efforts by all governments concerned.[11]

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.'[12]

While some might say this is merely anecdotal information, for these authors and our colleagues from other navies, the situation Professor Mitchell describes represents the reality of current coalition operations at sea and indicates that there important work yet to be done. Additionally, this is consistent with what proponents of network-centric operations have been exposing for some time. In a capstone publication of the Department of Defense Office of Force Transformation, the late Vice Admiral Arthur Cebrowski, considered by some to be the 'father of network-centric warfare,' opined, 'The United States wants its partners to be as interoperable as

[11] Mitchell, 'Small Navies and Network-Centric Warfare: Is there a Role?,' pp. 88-89.

[12] P. Mitchell, 'Small Navies and Network-centric Warfare: Is There a Role? Canada and U.S. Carrier Battlegroup Deployments,' briefing presented at the 8th 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.

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.'[13]

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 before 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 communications and data exchange capabilities – with robust displays, ample switching and routing capabilities, and high bandwidth – the admiral has experienced the 'best of the best' in this area. Additionally, 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 these officers mature through policy and acquisition assignments, their collective memory of coalition communications and data exchange capabilities is often quite positive – but it should not be, for they have not seen it from the position of coalition surface combatants attempting to work with U.S. Navy ships.

Given the importance of coalition networking and in the face of the operational challenges to achieving the requisite degree of networking, it might seem that like-minded, peace-loving navies would be on a sharp trajectory to solving these problems. However, this is not always the case. For the U.S. Navy, part of the problem could be the aforementioned collective experience of senior flag officers. But 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. 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 aren't keen on doing the right thing – 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.

---

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

Part of the reason for this lack of advocacy and difficulty in reorienting requirements and acquisition practices in the case of the U.S. Navy – and perhaps on the part of likely coalition partner navies too – 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.

Fortunately, some grass-roots efforts *are* underway to do just that – quantify the degree of benefit delivered by effective coalition networking. These efforts have not received much visibility outside of the communities of interest working the issue, but excellent work is underway in a number of venues, primarily among five English-speaking nations: Australia, Canada, New Zealand, the United Kingdom and the United States. 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, and the link to *The Beginners Guide to the Technical Cooperation Program* provides further links that explains the purpose and construct of each of these organizations in more detail:[14]

1. ASIC: Air & Space Interoperability Council (Australia, Canada, New Zealand, United Kingdom, United States) – focused on aerospace interoperability.

2. ABCA: American, British, Canadian, & Australian Armies (Australia, Canada, United Kingdom, United States) – focused on Army interoperability.

3. AUSCANNZUKUS (Australia, Canada, New Zealand, United Kingdom, United States) – focused on naval command, control, communications, and computers.

4. CCEB: Combined Communications Electronics Board (Australia, Canada, New Zealand, United Kingdom, United States) – focused on military command, control and communications.

5. MIC: Multinational Interoperability Council (Australia, Canada, New Zealand, United Kingdom, United States) – focused on military interoperability.

6. MIP: Multilateral Interoperability Program (Australia, Canada, United Kingdom, United States) – focused on command, control interoperability.

7. TTCP: The Technical Cooperation Program (Australia, Canada, New Zealand, United Kingdom, United States) – focused on military science and technology.

[14] The Technical Cooperation Program: TTCP document DOC-SEC-3-2005, *A Beginner's Guide to the Technical Cooperation Program*, September 1, 2005, accessed at: Internet: <dtic.mil/ttcp/>. This recent document published on The Technical Cooperation Program's public website, is a concise explanation of TTCP's structure and purpose.

Much of the work of the aforementioned groups deals with near-term solutions to emergent operational interoperability issues, and many of the groups are populated by uniformed professionals from all of the nations involved. However, there is one group that is chartered to look for longer term solutions to interoperability among the military forces of Australia, Canada, New Zealand, the United Kingdom, and the United States and one that is populated by scientists and engineers with an understanding of the science and technology issues that need to be addressed in order to achieve the desired level of interoperability. That organization is The Technical Cooperation Program (TTCP). The remainder of this paper will illuminate these TTCP efforts and present them as a potential 'process model' to achieve similar results in other fora – particularly in the area of coalition naval interoperability.

The Technical Cooperation Program: One Vehicle to Achieve Coalition Networking

Although it has been around in various forms for almost half a century, TTCP is not well known, and some background is in order to explain how this program facilitates the current efforts to address coalition interoperability. Importantly, while conducting this sort of analysis in other fora is certainly *possible*, the extant TTCP organization and infrastructure provided a ready-made medium that made success in this endeavor *probable*.

TTCP is a forum for defense science and technology collaboration between Australia, Canada, New Zealand, the United Kingdom, and the United States. It is probably the largest collaborative defense 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 up and 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.

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 defense 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 defense. The purpose is to enhance national defense 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 quick and easy fashion.

Collaboration within TTCP provides a means of acquainting the participating nations with each other's defense 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, DC, 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.[15]

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.

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; *Coalition Interoperability: How Much Is Enough and How to Quantify It* and reports on the past four-plus years of activities and the way ahead for the ongoing research of this group.

AG-1/AG-6 Work as a Model for International Defense Cooperation

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

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.[16] However,

[15] The Technical Cooperation Program: TTCP document DOC-SEC-3-2005, *A Beginner's Guide to the Technical Cooperation Program*, September 1, 2005, accessed at: Internet <dtic.mil/ttcp/>.

[16] 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*

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.[17] 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.

Transatlantic Revolution in Military Affairs (Washington, D.C.: National Defence University Press, 1999); J. Thomas, *The Military Challenges of Transatlantic Coalitions*, Aldelphi 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 21st 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.

[17] 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 Internet <dodccrp.org> to access the totality of the CCRP effort, including several books that describe these early efforts to quantify the benefits of networking.

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.[18] 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.[19]

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 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. Serendipitously, 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.

---

[18] 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). The results presented herein for the MIO, ASW, and ASuW studies were all drawn from ICCRTS presentations made by AG-1 principals.

[19] I. Grivell et al., *A Review of Analytic Techniques Applicable to the Study of Network Centric Warfare,* TTCP TR-MAR-9-2003, May 2003.

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 notes 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.[20]

With Study A providing the broad, overarching underpinnings of the work of AG-1, the remainder of this section of this paper will discuss the three tactical situations (TACSITS) agreed upon by the TTCP principals. 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. Maritime Interception Operations (MIO) TACSIT

The first tactical situation examined by MAR AG-1 was that of Maritime Interception Operations (MIO). This represented a tactical scenario familiar to all the member nations, and one that all believed they would be involved with in the future. Additionally, the member nations recognized that the results of this study would also be important to each nation in the Global War on Terrorism (GWOT) since the operational experience of all navies was increasingly focused on an a particular aspect of MIO, Leadership Interception Operations (LIO). Thus, MIO provided an excellent first study for the participants. The results of this study reported in this paper are extracted primarily from the report of the MIO TACSIT Group presented at the 8th International Command and Control Research and Technology Symposium.[21]

---

[20] C. Davis et al., *Key Issues in Coalition Network-Centric Maritime Warfare*, TTCP TR-MAR-10-2003, January 2004.

[21] M. Hazen et al., 'The Analysis of Network-Centric Maritime Interception Operations (MIO) Using Queuing Theory,' presentation at the 8th International Command and Control Research and Technology Symposium, Washington, D.C., June 17-19, 2003. The majority of the detailed analysis of the TACSIT contained herein is excerpted directly from this paper, as it is the primary repository of this TTCP MAR AG-1 work that is available for unlimited distribution.

From AG-1's initial investigations a number of hypotheses about tactical NCMW applications were developed to address a variety of tactical level war-fighting scenarios. The hypothesis for MIO was:

> *In coalition force MIO operations, network-enabled collaborative planning/re-planning increases the probability of intercepting a contraband vessel.*

The associated null hypothesis is that network-enabled collaborative planning/re-planning does not increase the probability of intercepting contraband vessels.

MIO operations can form a large part of both peacetime and wartime naval operations, particularly for mid-size and smaller combatants. Since MIO-type operations are so broadly applicable, they provided a good initial area for the study of NCMW effects. In addition, MIO operations are more critically dependent on information and command and control (C2) than on specific weapon systems, which simplifies the problem space and analysis.

In essence, MIO operations consist of a set of naval forces trying to find and apprehend (possibly deter) targets of interest (TOI) carrying contraband (goods or people). The TOI may be mixed in with legitimate vessels. Typically, the TOI must be identified and apprehended in some specific area so that it cannot pass through that zone and evade the blockade. The required criteria for apprehending vessels can vary, but typically determining whether the criteria are met requires close examination by the interdicting force. These identification processes may require several levels of examination by different units, and may be applied to all vessels or just a sample of them. The task of the TOI is to escape the interdicting force through maneuver or deceit.

In MIO, the vessels of interest (or targets) may be regarded as waiting in a queue to be served (or queried, and perhaps inspected and boarded) by warships on patrol. This service also takes time. No two operations are identical, but they are characterized by a sequence of actions starting with a query into the vessel's intent, often followed by a search for contraband by a boarding party, and end in a decision to either apprehend the vessel or allow it to continue.

Collaborative planning and re-planning assumes that dispersed individual commanders, subject to a general commander's intent, can make use of networked communications to develop plans in collaboration as if they were a co-located command. Thus, a MIO force would develop and coordinate their initial plans over the network. The commanders can then make joint decisions on changes to an existing plan as circumstances change. The difference between planning and re-planning is really only one of timing since few plans exist in a vacuum. Planning, however, is often thought of as being an operational level task performed by dedicated command staff, while re-planning in this context is a tactical task.

In both cases, the NCMW application involves doing the normal command staff jobs (for tactical or real-time planning) in a distributed fashion. Thus, while units are dispersed and in the midst of operations their views and inputs can be obtained in planning or adjusting the operations to adapt to unforeseen circumstances. In a coalition operation, there is a further benefit that all nations and their particular requirements can be included in the plans. Coalition operations are

fraught with possibilities for misunderstanding and require that significant effort be put into maintaining relations between the partners. Collaborative planning may provide an additional channel for these efforts, hence the reason for the AG-1 hypothesis.

The expected outputs and results of the use of collaborative planning and re-planning are:

1. Improved synchronization between units since unit commanders understand their partners' parts in the plan and their concerns about the plan;
2. Increased flexibility in operations because the overall force is able to respond in an adaptive manner to new circumstances;
3. Improved use and understanding of sensor and intelligence data;
4. Better matching of force to threat, since units can redeploy to match a threat;
5. Deconfliction of the battle space. Since everyone participates in the re-planning, there will be fewer problems of water space or airspace management;
6. Decreased HQ workload since virtual command teams can be formed outside of the operational level command;
7. Increased ownership of plans by all units or nations involved since everyone has been involved in the plan development; and
8. Increased speed and quality of command.

The focus of this effort was to investigate the usefulness of applying a queuing model to Maritime Interception Operations within the context of the NCMW concept of tactical collaborative planning. Both analytical and simulation-based queuing models were examined, and the theoretical model was applied parametrically to two MIO scenarios.

Using the steady-state probability of target vessel interception (i.e., service) as the primary measure of effectiveness, AG-1 was able to demonstrate the usefulness of queuing theory to relate NCMW application measures to force effectiveness. In addition, the queuing models provided valuable insight into the aspects of the MIO task where NCMW concepts might be applied. Thus, the group demonstrated that queuing theory is directly applicable to the second stage of analysis for operations that can be viewed as a demand for service, and provides direction in the process of refining NCMW concepts into testable applications. The parametric results obtained provided general bounds on expected improvements in effectiveness; specific results, however, will depend upon the particular NCMW applications and how they are used.

A complete report of the MIO TACSIT results is beyond the scope of this paper but is provided in great detail in the report of the MIO TACSIT Group cited above. The analysis by the MAR AG-1 group demonstrated that queuing theory provides a good model for a class of maritime operations that are expected to benefit from Network-Centric Maritime Warfare concepts and applications. Specifically, those operations characterized by a 'demand' for (or avoidance of) service can often be adequately modeled and analyzed by applying queuing theory. This fills one of the necessary stages in a quantitative analysis of NCMW concepts – that of linking application measures of performance (MOPs) to force measures of effectiveness (MOEs).

The examination of engagement level models and the variation of MOE with the parametric study of input MOPs is an important part of the process of refining NCMW concepts to the point where they can be tested. The two applications of the NCMW concept of network-based collaborative planning and re-planning analyzed by AG-1 using a queuing model highlight the capabilities and shortfalls of the methodology. For aggregate steady-state systems, queuing theory provides a rich source of insight. The analyst must keep in mind, however, that, in reality, service time and service accuracy often are not stationary processes and interesting phenomena will occur outside of steady-state situations.

The quantitative results obtained from running the MIO queuing models supported the group's hypothesis – that in coalition-force MIO operations, network-enabled collaboration planning/re-planning could significantly improve the probability of intercepting a contraband vessel in many cases. For example, in a scenario with an overall arrival rate of 25 targets per day, there is a 20% improvement in interception probability simply by providing some mutual coordination within the force, and a 50% increase in capability through dynamic, collaborative re-planning of the force response.[22]

These results confirmed these authors' anecdotal experience from interaction with operators who have participated in MIO operations in the Arabian Gulf, and thus, this study of coalition MIO operations provides general evidence to support the continued development of collaborative planning and re-planning applications. Given that the former commander of the United States Pacific Fleet noted that 'Maritime interception operations is another maritime-centric effort in our contribution to the Global War on Terrorism and forms perhaps our greatest 'growth opportunity' in our fight against global terrorism,' the MIO modeling work conducted by AG-1 should inform coalition partner navies of the substantial benefits of networked operations.[23]

B. Antisubmarine Warfare (ASW) TACSIT

The second tactical situation examined by MAR AG-1 was that of Antisubmarine Warfare. Like MIO, it too represented a tactical scenario familiar to all the member nations and one that all believed they would be involved with in the future. The results of this study reported here were extracted primarily from the report of the ASW TACSIT Group at the 9th International Command and Control Research and Technology Symposium.[24]

---

[22] Hazen et al., 'The Analysis of Network-Centric Maritime Interception Operations (MIO) Using Queuing Theory,' pp. 8-9.

[23] Remarks by Admiral W. Doran, Commander, United States Pacific Fleet, at the 'West 2005' Conference, San Diego, California, February 2, 2005.

[24] R. Klingbeil et al., "Utilizing Network-Enabled Command and Control Concepts to Enhance ASW Effectiveness,' presentation at the 9th International Command and Control Research and Technology Symposium, Copenhagen, Denmark, September 14-16, 2004. The majority of the detailed analysis of the TACSIT contained herein is excerpted directly from this paper, as it is the primary repository of this TTCP MAR AG-1 work that is available for unlimited distribution.

With significant experience in ASW analysis, AG-1 was able to define the operational and tactical issues at hand and approached the complex issues involved in ASW from a multinational and multilateral perspective with a sound understanding of the challenges and opportunities associated with ASW operations in a coalition environment. The AG-1 team members were armed with literally decades of collective experience in ASW operations gleaned from coalition ASW exercises in various venues, including NATO and the United States Pacific Command's Rim of the Pacific (RIMPAC) exercises. Additionally, several of the AG-1 participants were members of the science and engineering staff at the Naval Undersea Warfare Center Division, Newport, Rhode Island, where they had carefully analyzed ASW exercises as part of their ongoing work.

With a far greater background and experience in ASW analysis than with MIO, AG-1 was able to quickly refine the options for this TTCP study and define the way ahead for the study. After weighing a wide range of options regarding *what* to analyze, the group decided to analyze two hypotheses:

1. *In coalition force ASW, network-enabled shared situational awareness (SSA) can reduce false contact loading, by means of data correlation and fusion of the information obtained and provided by individual search elements, and thereby improve search effectiveness.*

2. *Sensor operators in a collaborative information environment (CIE) can reach-back to ASW experts to improve classification performance against both target and non-target contacts.*

AG-1 used two queuing models that incorporate reneging (leaving a queue after entry) and balking (inability to enter a queue) to execute the computations needed to quantitatively analyze these hypotheses.

The rationale for picking these two hypotheses was a desire to move beyond the strong results of the MIO TACSIT and to deal with actions the coalition force might take once it was robustly networked. Thus, while the study did not 'wave away' the issue of robustly linked, networked operations, it attempted to take the analysis to the next level and examine what specific actions would most benefit the force if they were, in fact, robustly networked. After much deliberation, it was determined that SSA and a CIE were two major expected benefits of networking the maritime force. Thus, the ability to support SSA and CIE provided the optimum measures of effectiveness for this analysis. Particular instantiations of these benefits were expected to be important for improving the effectiveness of networked coalition ASW and thus were the focus of this study.

Situational awareness means, in essence, knowing what is going on within a volume of space and time. Then, SSA means that two or more individuals understand a situation in the same way.[25] In this study AG-1 examined the possibility of using network-enabled SSA to reduce false contact loading in ASW to increase ASW effectiveness.

[25] For a careful examination of the definitions and concepts of SA and SSA, see A.A. Nofi, *Defining and Measuring Shared Situational Awareness*, CNA Research Memorandum, CRM D0002895.A1/Final, November 2000.

A CIE is the aggregation of infrastructure, capabilities, people, procedures, and information to create and share the data, information, and knowledge that enables collaboration among a selected group of individuals or organizations.[26] In this study, AG-1 examined the possibility of using a CIE to connect individual forward-deployed ASW sensor operators with an ASW expert, such as an ashore acoustic intelligence (ACINT) expert, in order to augment operator expertise, enhance operator performance, and mitigate the relatively poor target vs. non-target classification performance of some afloat sonar operators.

The AG-1 team found that the aspects of SSA and CIE, as just described, could be analyzed using queuing theory. The team did not suggest that queuing theory was the only effective methodology for examining SSA and CIE, but rather, that for the purposes of this study, queuing theory provided an effective methodology. The group validated the MIO experience that any 'demand-for-service' system, or any system with a waiting line for service that can experience congestion, can be analyzed using queuing theory. Therefore, to the extent that a military task or system fits into a demand-for-service framework, it is analyzable by queuing theory.

The two queuing model tools, called QDET and QSIM that were used to conduct quantitative parametric analyses of the SSA and CIE ASW concepts.[27] A number of general conclusions were drawn from the analysis that provided evidence of the value of networking ASW forces, and also provided some indication of where network-centric applications might be focused.

The SSA and CIE ASW concepts were conceived, in part, through extensive dialog with others in the U.S. Navy ASW community, particularly with representatives of the Naval Warfare Development Command and the Program Executive Office – Integrated Warfare Systems. The latter is developing, among other things, a Common Undersea Picture (CUP) capability for United States and coalition ASW forces.

The Shared Situational Awareness (SSA) Analysis

SSA means that two or more individuals understand a particular circumstance in the same way. First and foremost, connectivity between distributed systems is needed to achieve this. AG-1 examined the possibility of using network-enabled SSA to reduce false contact loading in ASW, and thereby increase ASW effectiveness. The hypothesis was:

In coalition force ASW, network-enabled SSA can reduce false contact loading, by means of data correlation and fusion of the information obtained and provided by individual search elements, and thereby improve search effectiveness.

Submarines, particularly diesel submarines operating on battery in a complex littoral environment, are difficult to detect, in part because both their passive and active signatures are

[26] USJFCOM, Multinational Experiment III, available online at Internet <jfcom.mil/about/experiments/mne3.htm, 2003>.
[27] K.M. Sullivan and I. Grivell, *QSIM: A Queuing Theory Model with Various Probability Distribution Functions*, NUWC-NPT Technical Document 11,418, 14 March 2003 (updated by I. Grivell, December 2003).

low. In addition, if contact is gained, it is often held only intermittently. Further compounding the ASW problem is the fact that littoral regions of interest generally contain many false contacts. Thus, false contacts can substantially interfere with the detection of the target of interest (TOI). More powerful sensors can exacerbate the false contact problem because the number of contacts detected increases approximately as the square of detection range.

There are several 'costs' associated with reacting to false contacts:

1. Reactive forces may be diverted or employed unnecessarily;

2. Fuel, sonobuoys, and weapons may be expended unnecessarily;

3. Reactive forces may not be available when needed; and

4. Prosecution of real TOI may be delayed or missed.

These adverse events are often observed in real-world exercises. One might ask: to what extent can network-enabled SSA mitigate some of these problems? In order to explore the false contact problem and test the above SSA hypothesis, an ASW TACSIT was developed. In the case with limited SSA, a Blue forward barrier submarine detects and misclassifies a surface vessel as a TOI and diverts from its planned search track to investigate. This diversion can cause detection of the TOI to be delayed or missed entirely.

In the case with network-enabled SSA, it is assumed that an air platform can provide surveillance of the region of interest and transmit an accurate surface picture to an assumed 'Contact Refinement Node (CRN).' It is also assumed that the Blue submarine also transmits information about the suspected TOI to the CRN. The network allows the CRN to be forward or on land. The task of the CRN is to assist with or conduct data alignment, correlation, localization, and target motion analysis, and classification across sensor contacts and tracks. The CRN shares this information in near real-time with all Blue ASW forces, including the submarine. The result of these activities is that the Blue submarine stays on its intended search track and does not become diverted by the non-TOI, as is the case without network-enabled SSA.

In the model selected, AG-1 needed a realistic estimate of the number of TOIs and non-TOIs that would produce sensor contacts. This number can be considerably larger than the actual number of objects. For given sensor and contact properties and dynamics, we can then calculate the arrival rate of contacts (customers) to the sensors. The arrival rate (AR) is thus comprised of the sum of TOI and non-TOI arrival rates.

Some of the TOIs and non-TOIs are detected by sonar and must be classified. Most of the arrivals are classified easily and are quickly identified as being non-TOIs. A portion of the arrivals may be difficult and time consuming to classify as a non-TO, however, due to the overlap with selected submarine attributes. As a result, detection and classification queues can form in highly cluttered regions.

Added complexities are balking and reneging. Contacts pass into and out of sensor coverage or have some finite lifetime that is often exponentially distributed. If such a loss happens within a

queue or within service, then the contact is said to have reneged. If it occurs before entry to the detection and classification processing queues, then the contact is said to have balked.

All of these factors are incorporated in AG-1's multi-contact queuing model. The primary output needed is the probability that an arbitrary contact is acquired and completes detection and classification processing. The probabilities of calling a target a target (a hit or correct classification) and calling a non-target a target (a false alarm or incorrect classification), were then multipliers to the probability of acquisition.

AG-1 analysis of the ASW TACSIT showed that the probability of acquiring a target was a function of contact arrival rate (AR). In the model run, contact AR for the combination of TOI and non-TOI varied from 0 to 10 contacts per hour. In this model, mean time to renege (hold contact) was assumed to be 15 minutes. Curves were produced for mean service times of 15, 30, 60, and 120 minutes, providing a parametric sweep of time to classify a contact by whatever process.

For the SSA ASW TACSIT, this led to the result that, as contact AR increases the probability of acquisition decreases. This occurs because as AR increases, balking and reneging increase. As the queue size grows, some of the possible contacts balk because they cannot enter the queue, and some of the contacts in the queue renege because they take too long to be serviced.

One effect of SSA is to decrease the AR of non-TOI to the classification system. There are a number of possible ways this can occur within SSA, for example, by surveillance of a portion of the non-TOI field, as previously described. It can also occur by the use of sophisticated Tactical Decision Aids (TDAs) that can correlate some sensor contacts with non-TOI objects or phenomena (such as reverberation prediction with active sonar).

Thus, the AG-1 modeling showed that the decrease in the AR of non-TOI does result in a higher probability of acquisition against the TOI. This effect of improved SSA, yielding a higher probability of acquisition can be parametrically analyzed. This exemplifies the value-added of SSA on reducing contact AR, and in turn, increasing ASW effectiveness.

The principal findings of this study of SSA on false contact loading in ASW are as follows:

1. Queuing theory can provide a framework for the analysis of the SSA ASW concept, because SSA is a 'demand for service' process;

2. Improving classification performance against both benign contacts and targets of interest can increase ASW effectiveness. In effect, this reduces the arrival rate of benign contacts, thereby increasing the probability of acquiring targets of interest;

3. An accurate surface picture, shared among the ASW units, could improve ASW effectiveness. Networking the force for information transfer is a key enabler of this aspect of SSA. Real-time connectivity is needed;

4. An alternative method for increasing ASW effectiveness is to employ more ASW units, i.e.,

increase the number of servers; and

5. The queuing theory framework can be used to analyze the tradeoff in benefits between shared information and force size (i.e., 'bits' vs. 'bangs').

In this section, we examined the possibility of using network-enabled SSA to reduce false contact loading in ASW to increase ASW effectiveness. The AG-1 hypothesis was: *In coalition force ASW, network-enabled SSA can reduce false contact loading by means of data correlation and fusion of the information obtained and provided by individual search elements and thereby improve search effectiveness.* AG-1's findings provide quantitative evidence that supports this hypothesis.[28]

The Collaborative Information Environment (CIE) Analysis

A collaborative information environment (CIE) was defined above as the aggregation of infrastructure, capabilities, people, procedures, and information to create and share the data, information, and knowledge that enables collaboration among a selected group of individuals or organizations.[29]

AG-1 examined the possibility of using a CIE to connect individual forward-deployed ASW sensor operators with an ASW expert, such as an ashore acoustic intelligence (ACINT) expert, in order to mitigate the relatively poor target vs. non-target classification performance of some sonar operators. The team also examined the possibility of using network-enabled CIE to improve the overall ASW classification performance and effectiveness of forward-deployed force elements. The hypothesis was: Sensor operators who did not have the requisite expertise to succeed at this target classification challenge in a CIE can reach-back to ASW experts to improve classification performance against both target and non-target contacts.

Once sensor contact is made on an object or phenomenon, the detection and classification problem is, in essence, an analysis and decision-making problem. There are many determinants of decision-making behavior, including:

1. Problem complexity;

2. Time available;

3. Number/quality of alternatives;

4. Perceived risks;

5. Information presentation rate;

[28] Klingbeil, et al "Utilizing Network-Enabled Command and Control Concepts to Enhance ASW Effectiveness,' pp. 17-18.

[29] *Department of Defense Joint Net Centric Capabilities* (Washington, D.C., Office of the Assistant Secretary of Defense for Networks and Information Integration, July 2003).

6. Individual differences in cognitive and decision styles; and

7. Level of expertise.

A small percentage of sonar operators have great expertise and are considered experts at what they do, for example, ACINT riders on ASW platforms. Therefore, it might be possible to use the network, with additional infrastructure, to link sensors, operators, experts (not collocated with forward operators), and tactical decision aids (TDAs) to improve ASW performance. This concept is an extension of the reach-back cell (RBC) concept. The RBC normally provides:

1. Environmental assessment;

2. Sensor performance predictions;

3. Red-cell wargaming;

4. Initial ASW battlespace assessment;

5. Initial plans, including unit stationing, tactics, and sensor employment;

6. Submarine contact database management;

7. Submarine contact information fusion;

8. Ongoing analyses and assessments of mission execution; and

9. *Can provide sensor/threat experts to advise forward operators*.

With robustly networked coalition forces, forward sensor operators *can* be linked to an ASW expert. In fact, multiple operators are forward and linked by means of a connectivity infrastructure to an expert threat analyst and sensor operator. The operators and expert can be considered as being embedded in a CIE. The expert would usually respond to requests for assistance by the operators. Due to the nature of ASW, including the problem that holding time may be short; the CIE requires synchronous tools to allow collaboration between simultaneously engaged participants. In addition, the expert will need to be aware of the ASW context and history experienced by each operator. This amount of information can be used to define the network architecture and the characteristics of network infrastructure.

Utilizing some of the same parameters of the SSA case above, AG-1 determined quantitatively that the probability of acquisition of a contact was enhanced when the forward-deployed sonar operators were able to operate in a CIE. The group found that, as might be expected, from the larger number of variables in the ‘equation’ (expertise of the individual sonar operators, expertise of the ACINT expert, type of target submarine, type of shipboard and/or aircraft equipment, etc.) definitive numerical results were not as readily available as in the SSA case. Nevertheless, the available evidence and the analysis showed a strong correlation between the degree of CIE established and ASW success – suggesting that more detailed analysis in this area.

The principal findings of this study of CIE on ASW effectiveness are as follows:

1. Queuing theory can provide a framework for the analysis of the value of the operator-expert CIE because this collaboration is a 'demand for service' process;

2. Networking the force can enable a CIE that, through improved classification performance, might increase ASW effectiveness;

3. Synchronous collaborative tools are needed to enable this collaboration; and

4. Expert workload may need to be controlled to avoid 'missing' requests for assistance.

In this work, AG-1 examined the possibility of using network-enabled CIE to support operator--expert collaboration in order to improve ASW classification performance and effectiveness. The hypothesis was: *Sensor operators in a CIE can reach-back to ASW experts to improve classification performance against both target and non-target contacts.* The findings provide evidence that supports this hypothesis.

Summary of the ASW TACSIT Analysis

In this study, AG-1 showed, through the analysis of two ASW TACSITs, that network-centric concepts can enable shared situational awareness (SSA) and a collaborative information environment (CIE). Both SSA and operator--expert collaboration in a CIE were shown to improve ASW performance and effectiveness. Specific warfighting findings included:

1. ASW effectiveness can be increased by improving classification performance against both benign contacts and targets of interest. In effect, this reduces the arrival rate of benign contacts, which thereby increases the probability of acquiring targets of interest.

2. An accurate surface picture, shared among the ASW units, could improve ASW effectiveness. Networking the force for information transfer is a key enabler of this aspect of SSA. Real-time connectivity is needed.

3. Networking the force can enable a CIE that, through the increase of classification performance, might increase ASW effectiveness. Synchronous collaborative tools are needed to enable this collaboration.

The results from this analytic effort indicated that selected NCMW ASW concepts, if implemented, should have positive effects on ASW effectiveness. For example, NCMW applications that decrease the mean time to service contacts, in general, improve effectiveness. Furthermore, applications that decrease the arrival rate of unwanted contacts can improve the detection and classification of ASW targets of interest.

C. Anti-Surface Warfare/Swarm (ASuW/Swarm)

The third and final TACSIT examined was that of ASuW operations, specifically that of 'Swarm' attack against coalition naval units. In many ways, this TACSIT represented the most interesting (and challenging) case studied by AG-1 for a number of reasons. First, for the MIO and ASW cases, the coalition force would be primarily on the 'offensive' in either ships with contraband or hunting enemy submarines (although there clearly is a strong defensive component to many ASW operations), while in the Swarm case, the coalition naval force would definitely be on the 'defensive.' Second, in the MIO and ASW cases, there was typically a slow-moving tactical problem, while in the Swarm case, the tactical situation was one that moved rapidly. Finally, this Swarm case was one that lent itself to the use of a completely different model than those used in the MIO and ASW TACSITS, thus plowing new ground for analysis.

The results of this study reported in this paper were extracted primarily from the report of the ASuW/Swarm TACSIT Group at the 10th International Command and Control Research and Technology Symposium.[30] Because this 'warfare area' is relatively new, some additional background explanation of the nature of the challenge is in order.

In the ASuW problem in general and Swarm attacks in particular, battlespace control near land is essential to ensure prompt access and freedom of maneuver for coalition forces moving from the sea to objectives in the near shore area. As coalition naval forces operate in littoral areas, potential adversaries are responding with innovative, often asymmetric approaches to coastal naval warfare. A number of coastal nations – several of which border strategically important waterways – are exploiting small boat warfare and integrated coastal defenses to blunt, neutralize, or defeat larger navies operating in the near shore area.

The tactic that appears to have the most traction with these nations is that of 'swarming' attacks by large numbers of fast inshore attack craft (FIAC). There is no simple definition for these craft – they can be as small as recreational vehicles such as a Jet Ski or as large as naval or coastal fast-patrol boats. Also 'swarming' attacks can come from multiple axes and use various attack formations. The navies of coalition nations have conducted numerous studies and analyses in an attempt to come to grips with the threat of swarming small boat attacks. In one study for the U.S. Navy, an industry team found that different types of threat platforms had different effective weapons ranges. The study grouped these into two general categories; small threat platforms (cigarette boats, Boghammars, and others) with a maximum effective weapon range from 0.1 to 0.5 nautical miles and larger naval vessels such as advanced patrol boats carrying short-range guided missiles.

While a number of studies did not discount swarming attacks by larger vessels such as advanced patrol boats, the studies focused heavily on swarming attacks by very small craft as the

[30] D. Galligan et al., 'Net Centric Maritime Warfare – Countering a "Swarm" of Fast Inshore Attack Craft,' presentation at the 10th International Command and Control Research and Technology Symposium, McLean, Virginia, June 13-16, 2005. The majority of the detailed analysis of the TACSIT contained herein is excerpted directly from this paper; as it is the primary repository of this TTCP MAR AG-1 work that is available for unlimited distribution.

predominant scenario likely to be faced by coalition navies operating in littoral waters. The consensus of a number of studies and the opinions of serving naval officers appear to converge and focus on a primary massed, small boat threat consisting of 10 to 20 high-speed maneuvering boats attacking over a 20- to 60-degree azimuth sector. The boats have a simultaneous arrival time with closing speeds of up to 35 knots. Their maneuver is typically in a sinusoidal path. The small boats are considered to be commercial types with no obvious distinguishing feature to support easy classification. Identification of the attack results from the characteristic behavior of a large number of high speed inbound boats.

The threat of swarming small boats is not a new one. For a number of years, work in naval laboratories focused on the small, fast, maneuverable boats as primary threat elements. The operational experience of serving naval officers in AUSCANNZUKUS nations indicated that naval forces must be capable of engaging small coastal naval combatants such as patrol boats and guided-missile corvettes or other smaller boats. Several reports noted that boats could be operated in an unpredictable manner and under unexpected conditions. These reports concluded that these craft may appear as part of the normal friendly or neutral traffic in the area, making them all the more difficult to counter. In addition, industry reports provide numerous examples of observed and reported naval exercises by rogue nations that demonstrate their willingness and ability to surreptitiously get inside the effective maximum range of the surface weapon systems of a larger naval force.

The nature and the magnitude of this threat have riveted the attention of coalition navies who recognize, in general, that a coordinated response from networked coalition naval assets is the optimal way to defeat this threat. In an article in the *U.S. Naval Institute Proceedings*, the current U.S. Chief of Naval Operations opined:[31]

> 'Small, fast enemy surface combatants represent another threat to operations in geographically confined areas, where their size and the surrounding clutter of geography and traffic make long-range detection difficult…A diverse force, networked with distributed sensors, offers promising response capabilities once enemy vessels are under way.'

While this swarming small-boat attack threat has been discussed in professional journals and reviewed in depth in various studies, there has been, to date, little quantitative analysis to determine the extent to which networking coalition naval platforms can help to deal with such a threat. Therefore, it was determined that this was a particularly fruitful area for AG-1 analysis.

The AG-1 ASuW/Swarm study characterized the degree of networking between members of a maritime force, and used the map-aware non-uniform automata (MANA) intelligent-agent-based distillation model to represent the C2 and sensor interactions between allied units, and separately between the units of the attacking force. The study sought to determine what degree of improvement was possible via surveillance and targeting, and indicated the point at which the battle must be moved 'offshore' using either helicopter or unmanned combat air vehicle (UCAV).

[31] Vice Admiral Mike Bucchi and Vice Admiral Mike Mullen, 'Sea Shield: Projecting Global Defensive Assurance,' *U.S. Naval Institute Proceedings*, November 2002, pp. 56-59.

The AG-1 challenge was to investigate possible network-centric measures to overcome the Swarm threat, using operational analysis to quantify the outcome. The problem was defined by very short surveillance (detection) ranges due to the small size of Type 1 FIAC, and even shorter identification (ID)/classification range.[32] These factors are very scenario/environment dependent, and ducting conditions may hamper ship-mounted sensors. Such factors, plus current rules of engagement (RoE), ensure that engagements are now conducted at 'whites of the eyes' ranges well inside potential enemy weapon launch range.

The FIAC/Swarm study was initiated in early 2003 (and completed the following year), and AG-1 took a broad three-level modeling approach using the following tools:

- 'Simple' spreadsheet, plus the Queuing Theory (QT) models
- MANA model
- Threedim model

The platforms likely to be involved in the modeling included some-high value units; their escorts, typically one or two destroyers or frigates (DD/FF); some airborne assets (helicopter or unmanned aerial vehicle (UAV)); the opposing forces; and background or neutral shipping. The 'three-tier' approach was to provide depth and a degree of validation and verification; it was not clear at the outset whether the spreadsheet and QT models might (through meta-modeling) over-simplify the problem. However, there was some confidence in MANA's strengths as an intelligent agent model to represent swarming aspects, while Threedim (as a fully featured battle model) had the ability to model at greater fidelity, including weapon system arcs, but with a simpler (i.e., 'dumb') target set.

A modeling workshop was held in late 2003. The characteristics of FIAC and defensive systems were presented and discussed along with the operational realities of Swarm engagement, using experts from the UK Maritime Warfare Centre at HMS DRYAD. The study hypothesis was reviewed and it was agreed that it captured the essence of the analysis problem:

> *'In an ASuW Swarm attack, Blue shared situational awareness and an associated sensor-to-effector capability reduces the number of leakers against Blue assets.'*

The NCMW options for the FIAC/Swarm study include the following cases, with varying degrees of 'networking:'

1. **Baseline.** No communications or networking between units. This is not realistic, but sets the base case for proper comparison between options, by reducing the force to a collection of 'singleton' ships that cannot act in a coordinated manner.

[32] Three types of FIAC threats were modeled, and these types represented the generally accepted FIAC types described in the naval literature on the subject. Type 1 FIAC are those represented by a Jet ski or Boson Whaler with Rocket Propelled Grenade (RPG) weapons or a large-blast bomb used in a suicide attack. Type 2 FIAC are those represented by larger 'Boghammer' class boats with unguided multiple-launch bombardment rockets or with larger anti-tank guided weapons. Type 3 FIAC are those represented by small Fast Patrol Boats (FPBs) typified by the Super Dvora, with smaller anti-ship missiles or torpedo armament.

2. **Low.** Shared situational awareness but with organic targeting.

3. **Intermediate.** Shared situational awareness and organic targeting (as Low case), plus reach back to intelligence information.

4. **High.** Shared situational awareness, organic targeting, and reach back to intelligence information (as Intermediate case) plus inorganic (i.e., off-board) targeting.

Regarding metrics and presentation of results, it is important to define suitable measures of effectiveness for the purpose of determining the effect NCW has when it is used in the Swarm attack scenarios. The following MoEs were adopted:

1. The fraction of Red threats that come within their weapons range of the high-value unit (HVU).

2. The probability of at least one Red threat reaching its weapons range of the HVU.

3. The number of naval vessels that suffer defense capability-kill while defending the force.

4. The number of neutrals inadvertently destroyed, (only relevant when inorganic weapons targeting is used).

The results were generally presented as graphs of the probability or number of leakers versus the weight of attack. Where available, the standard errors in the average MOE value were used to provide uncertainty estimates for them.

During the initial modeling work, the base case results with point defense and improved target indication (TI) for a single-sector attack (using close-range guns and various permutations of gun range and slew times), showed that:

1. Current point defense systems can be overwhelmed by a relatively small number of FIAC.

2. The key drivers are FIAC speed, rate of Blue weapon fire determining the number of shots before Red fires, and the effective range difference of Red and Blue weapons.

The results of the three models were in substantial agreement and AG-1 decided to use MANA as the principal model to analyze Swarm attacks for the remainder of the study. The full results of this MANA model work is classified due to the sensitivity of the models and the work involved, therefore, this paper will move directly to the general results of the analysis.

The analysis pointed to a number of operational benefits derived from robust networking**.** The broad classes of operational gain from ‘network enabling’ forces, when compared to the baseline ‘singleton’ case are:

1. **Better use of close-range guns.** This is achieved by meeting the RoE criteria for opening

fire at the maximum useful weapon range, rather than a shorter range, once decisions have been made by each weapon crew and ships command team. This applies to manually aimed ('crew served') weapons like the M-60 machine gun or 40-mm grenade launcher, and 20-mm and 30-mm cannon, as well as autonomous weapons like Phalanx Block 1B.

2. **Use of medium-caliber gun to maximum range.** The escorts' medium caliber gun (a US 5"/54 or the UK 4.5" Mk 8) will typically fire 20 to 25 rounds per minute out to about 26-km, with either direct action (DA) fusing (exploding on impact with the sea or a target), or via a variable time (VT) proximity fuse for airburst over the target, which is attacked by the shell fragments.

3. **Move the battle outwards.** This is accomplished by using helicopter or UCAV. This class of benefit applies to all classes of FIAC and provides either ISR/ID information about the target – thus achieving engagement criteria for ship mounted weapons – or the helicopter or UCAV can also be armed and then used to attrite the incoming FIAC raid. The differences are that the crewed helicopter can be autonomous, while the UCAV relies on good networking back to the controlling ship.

The results of the analysis using the MANA model clearly showed the need to 'do something.' Present ships defenses are sensor-limited by short detection and ID ranges, and are sometimes hampered by restrictive RoE. Saturation therefore can occur at relatively low weights of attack by Type 1 FIAC.

An ASuW Swarm could be countered by networking between escorts, helicopters/UAVs/ UCAVs and the merchant ships. Improvements come in three broad bands:

1. Use of existing close-range guns (MG, 20/30-mm, Phalanx 1B) to maximum range, to defeat Type 1 threats.

2. Use of existing medium-range weapons to medium-range bracket to attack Type 2 FIAC, plus use of smart rounds (laser designator in helo/UAV) to maximum range.

3. Maximum use of armed helicopters/UCAV to attrite raids further out. This is the only counter to a longer range Type 3 attack, but the trade-off between helo and UAV/UCAV depends on the scenario.

The results of the AG-1 MANA analysis showed that for the smallest Type 1 FIAC, intermediate and high levels of networking could increase Force survivability substantially. Countering the larger Type 2-3 FIAC could be achieved by the use of networked air ISR.

The trade-off between helicopter and UCAV depends on whether the threat adopts a single sector or widespread (i.e., isotropic) attack. Armed airborne assets will always improve the survivability of the force, but the finite weapon payload and space/time considerations caused by the target spread, drive the number of airframes required.

In summary, the third and final MAR AG-1 TACSIT showed, as its two predecessors did, that robust coalition networking could provide substantial benefits. In this case, it increased the probability of success when a naval force is attacked by a FIAC 'Swarm' attack. The nature of the study organization and the fidelity of the MANA model also informed the study team of specific tactics that could aid the defending force in fighting off such an attack. Accordingly, the ASuW/Swarm TACSIT was an important outcome of AG-1's work and a valued input for the work of AG-6.

D. Transition from AG-1 to AG-6

As indicated earlier, AG-1 was chartered for a defined period of time, October 2001 to September 2004. The TTCP methodology and 'rules of the road' are for an action group to complete its work in two to three years, report out to its governing body (in this case, the MAR leadership), and then dissolve. Based on this remit, AG-1 completed its work on schedule and passed its body of work on to the MAR and TTCP leadership.

When the AG-1 Chairman reported on the group's work to the MAR leadership, that leadership team determined that the issue of coalition networking was so important that it wanted this work to continue. The MAR leadership decided that the best way to leverage the work of AG-1 and to explore new challenges was to charter a new group, AG-6, and direct this group to extend the work of AG-1 to a greater degree of specificity with respect to systems and processes required to implement network-centric maritime warfare. The approach being taken by the U.S. Navy and Marine Corps is known as FORCEnet, and the new action group was tasked to study FORCEnet Implications for Coalitions. A Terms of Reference (TOR) was quickly issued and the work of AG-6 began.

Action Group 6 (AG-6) FORCEnet Implications for Coalitions (Ongoing)

Based on a strong recommendation by the MAR leadership for a 'seamless handoff' from AG-1 to AG-6, the two teams met together in the late 2004. This was a closeout meeting for AG-1 and a start-up meeting for AG-6. Three AG-1 National Leaders transitioned from AG-1 to AG-6, ensuring much of the continuity and leveraging of effort that the MAR leadership sought. Additionally, there were select members of other delegations that continued from AG-1 to AG-6. The result was a team ready to undertake new challenges, but one that had the collective benefit of first person, detailed knowledge of the AG-1 studies, as well as the experience of working in an intense coalition environment.

Based on the knowledge that AG-6 would not take long to 'get up to speed,' the MAR leadership set in place an aggressive time line to complete the work. The MAR TOR directed:

> Building on the results and findings of AG-1, MAR initiated plans for a follow-on 'FORCEnet Implications for Coalition' Study (AG-6) to examine the implications and way ahead for realizing coalition capabilities that are compatible with both the functionality and timeline of the U.S. Navy's FORCEnet initiative. (MAR

> leadership seeks to) define in functional terms various levels of coalition interoperability with FORCEnet; to assess the incremental value of higher levels of interoperability; to make appropriate use of USN FORCEnet and other TTCP nations' systems engineering effort, of TTCP nations' modeling capability, of interactions with Trident Warrior and other exercises, and with other TTCP Group efforts, (e.g. HUM); and provide input to national balance of investment studies.

AG-6 set to work immediately to carry out the mandate of the TOR and to 'bound the problem space' to work through the issues of coalition interoperability in general and the issues of coalition nations 'falling in' on the U.S. Navy's FORCEnet capabilities with the goal of zeroing in on the TOR remit and 'harmonizing national coalition C4I interoperability strategies and development plans.' Since AG-6's work is ongoing, this paper will not attempt to report definitive results of this team's efforts (since those results will take time to reach fruition), but rather will provide a window on the work to be accomplished as an example of what coalition partners can accomplish if a long-term relationship of dedicated naval professionals is supported and nurtured.

Building on the compelling evidence obtained by AG-1 (in one overarching situation and in three tactical scenarios) that networking coalition ships at sea confers substantial benefits to the combined naval force, AG-6 will investigate the extent to which a coalition force built around a FORCEnet-capable U.S. naval battle formation can be more effective if all the ships in the group are able to participate in the U.S. Navy/Marine Corps' FORCEnet and Global Information Grid infrastructure in the conduct of a realistic tactical scenario.

An analogy offered by one of the AG-6 members helps to illustrate the scope of this study. He noted that some years ago Singapore made an enormous investment in 'wiring' the nation with fiber-optic cable. 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. The question for AG-6 is whether FORCEnet can play a similar role in the development of maritime coalition capabilities.

The United States has committed to an enormous investment in the GIG and in FORCEnet. Those systems will connect the U.S. military as no military has ever been connected before. There may be some incremental cost on the part of the U.S. Navy in designing FORCEnet to be completely 'coalition capable' and there may be some attendant cost on the part of coalition nations to 'fall in' on the U.S. Navy's FORCEnet in the same fashion that the international business community 'fell in' on Singapore's excellent infrastructure. AG-6's goal is to quantify – with as much specificity as possible – how much more combat-capable a FORCEnet-centric coalition battle formation will be than one that is not connected. This analysis will then assist the leadership of the five TTCP nations in determining whether the investment brings the concomitant return in warfighting effectiveness.

AG-6 deliberated for some time in order to find a scenario that represented a real-world naval challenge and one that also lent itself to the kind of detailed analysis necessary to address both

the TOR requirements and the overarching goals of the group. AG-6 ultimately determined that a scenario that caused a coalition naval force to conduct not just one – but multiple, cascading missions – would both mimic real-world conditions and present robust possibilities for analysis.

The scenario selected involved coalition naval operations in and around the South China and Philippine Seas. In this notional scenario, a coalition naval force initially is tasked to provide humanitarian support and disaster relief in a Southeast Asian nation. When indigenous separatist groups use the opportunity afforded by this chaos to foment trouble, the humanitarian support and disaster relief mission quickly morphs into peace-making/peace-enforcement. As the scenario evolves, the coalition naval force ultimately faces a challenge from a neighboring nation unhappy that this force is on scene, and the coalition naval force ultimately must deal with surface and submarine threats.

The group determined that selecting the right mix of naval vessels to undertake these missions was as important as picking the right scenario. After extensive dialogue with uniformed naval professionals in all five nations, a decision was made that a naval force built around a U.S. Expeditionary Strike Group (ESG) with supporting ships and aircraft from all five nations, would represent the most realistic coalition battle formation sent to undertake this mission.[33]

AG-6 will analyze the extent that coalition networking built around leveraging the U.S. Navy's FORCEnet (Fn) capability will enhance the chances of mission success. The levels of interoperability selected for analysis are:

Option 0 (do nothing)	Small size (all U.S.) ESG force, fully Fn capable
Option 1 (do minimum)	Added Coalition ships, but not Fn capable (larger overall force)
Option 2	Intermediate Fn capability to the additional coalition ships
Option 3	Full Fn capability to entire force – robust networking

The central question posed by the AG-6 TOR was to determine the 'price of admission' for the other four coalition partners to operate effectively with the U.S. Navy/Marine Corps FORCEnet-capable battle formation. One proposed solution to minimize this 'price of admission' is discussed in the next section of this paper.

The Global Information Grid and FORCEnet Can Provide the Right Infrastructure

When the MAR leadership stood up AG-6 and directed it to leverage the work of AG-1, there was a built-in mandate for continuity and, as mentioned above, some AG-1 members, including three national leaders, transitioned from AG-1 to AG-6. However, on the U.S. team, there was an almost complete turnover of personnel. This was done for a compelling reason, for with the shift in the new group's focus to FORCEnet, there was a concomitant mandate for change in

[33] For this scenario, the United States ESG would include three amphibious assault ships (built around a large-deck command ship), one cruiser, two destroyers, three littoral combat ships, and one attack submarine. Australia would contribute two frigates and one amphibious transport ship. Canada could send up to a task group (including a destroyer, two frigates and a replenishment ship). New Zealand would send one auxiliary ship and one frigate. The United Kingdom would send one aircraft carrier and one frigate.

order to bring sufficient subject-matter expertise to the team. Accordingly, the new U.S. National Leader and several team members were drawn from the Space and Naval Warfare Command (SPAWAR) in San Diego (the U.S. Navy's FORCEnet Chief Engineering entity) and from that command's principal laboratory, SPAWAR Systems Center, San Diego (SSC San Diego).

Some additional background is needed to understand the importance of this transition. The SPAWAR Enterprise has been at the forefront of FORCEnet development since this concept evolved from the work of the U.S. Chief of Naval Operations Strategic Studies Group a number of years ago. Soon after Admiral Vern Clark took over as the U.S. Navy's Chief of Naval Operations, he articulated the U.S. Navy's vision as 'Sea Power 21' based on the four pillars of Sea Strike, Sea Shield, Sea Basing, and FORCEnet.[34] While some critics dubbed the first three pillars 'old wine in new bottles,' most seasoned naval observers recognized that FORCEnet was indeed something new and exciting that could fundamentally alter the way naval warfare was conducted.

The detailed vision for FORCEnet was set forth in a 2005 publication of the Naval Network Warfare Command, *FORCEnet: A Functional Concept for the 21st Century*. Signed by the Chief of Naval Operations *and* the Commandant of the Marine Corps, this short document defines the importance and essence of FORCEnet and explains where FORCEnet will fit in the overarching context of military command and control. Importantly, this publication provides the U.S. Navy's working definition of FORCEnet:[35]

> FORCEnet is the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force.

In straightforward terms, FORCEnet refers to the systems and processes for providing fully networked naval command and control in 2015 to 2020. The objective of FORCEnet is to provide commanders the means to make better, timelier decisions than they currently can and to allow the effective execution of those decisions. This concept envisions extensive connectivity among network elements – greater by orders of magnitude than previously achieved. Since most headquarters are already well connected, the real power of FORCEnet is in connecting the extremities of the force – people, weapons, sensors, platforms and other entities, ultimately extending visibility and empowerment to the extremities.[36] The development of FORCEnet, like the development of the Global Information Grid itself, follows the precepts of the Command and

[34] See Admiral Vern Clark, 'Sea Power 12: 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, for two of the earliest articles in the open literature regarding Sea Power 21 and FORCEnet. The capitalization of 'FORCE' while 'net' remained in small letters was done purposefully by the CNO. This was done to emphasize that FORCEnet was about providing a warfighting capability to the naval *force*, and was not about 'the net.'

[35] Admiral V. Clark and General M. E. Hagee, *FORCEnet: A Functional Concept for the 21st Century*, February 8, 2005. This publication can be found on the Naval Network Warfare Command website at Internet <enterprise.spawar.navy.mil/getfile.cfm?contentId=816&type=R>.

[36] D. Alberts and R. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, D.C.: DoD Command and Control Research Program, 2003).

Control Research Program, making FORCEnet the *naval* portion of the Global Information Grid.[37]

This document goes on to describe 15 required FORCEnet capabilities, capabilities that will guide the technical community to design FORCEnet in a way that will enable warfighters to achieve the maximum utility from this system. While a listing of these 15 attributes is beyond the scope of this paper, they are available for ready reference in this Naval Network Warfare Command publication.[38] Importantly, AG-6 examined this publication and determined that these attributes were consistent with the kind of naval command and control that all nations desired.

Within SSC San Diego, scientists and engineers had been working on FORCEnet since its inception, and they soon discovered the FORCEnet design parameters enabled them to do some interesting things. They learned that the totality of the U.S. Navy's 'higher level guidance' on FORCEnet, ranging from the initial concept documents produced by the Chief of Naval Operations Strategic Studies Group to SPAWAR Headquarters' FORCEnet Architecture and Standards document,[39] allowed them a wide range of ways to actually *design* FORCEnet as it would be instantiated in the U.S. Navy fleet.[40]

Based on its extensive background in navy networking at sea, command and control, knowledge management, human systems integration, and other disciplines, this SPAWAR Headquarters and SSC San Diego team devised an approach to the design of FORCEnet that SSC San Diego has dubbed 'Composeable FORCEnet.'[41]

It would be a nice story to say that these SSC San Diego scientists and engineers designed Composeable FORCEnet with naval coalition operations in the forefront of their design process. It would be a nice story – but it would be untrue. What these subject-matter experts *did* do was design Composeable FORCEnet in a way that would enable it to be used by the widest range of users. They set out to build a working model of Composeable FORCEnet based on open architecture and open standards, a system that would be the antithesis of current closed systems

---

[37] The body of work produced by the U.S. DoD Command and Control Research Program (CCRP) provides much of the theoretical, conceptual and analytical basis for network-centric operations as it is generally understood and practiced by military units. For more on the CCRP, see Internet <dodccrp.org>.

[38] *FORCEnet: A Functional Concept for the 21st Century,* Naval Network Warfare Command, pp. 12-19.

[39] Office of the Chief Engineer, Space and Naval Warfare Command, *FORCEnet Architecture and Standards, Volume I (Operational and Systems View) and Volume II (Technical View)* (San Diego, CA: SPAWAR, 2005).

[40] *FORCEnet Architecture and Standards Volume II (Technical View)* clearly defines the objective that the technical community must achieve in designing FORCEnet: 'develop a naval networking infrastructure and integrated applications suite with full interoperability among the service components, joint task force elements, and allied/coalition partners. The FORCEnet Architecture will ensure that design decisions made by component programs are consistent with the FORCEnet blueprint and incorporate common engineering, information, protocols, computing, and interface standards across various computing environments and platforms. This blueprint will be based on joint and commercial standards, with development and implementation coordinated with transformational initiatives, the Army, Air Force, and Coast Guard, as well as Joint commands and allies.'

[41] SSC San Diego scientists and engineers have briefed the Composeable FORCEnet concept to literally hundreds of military, industry, and academic professionals over the past several years. See, for example, George Galdorisi et al., 'Composeable 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 Internet <dodccrp.org>.

or systems of systems. The fact that coalition forces could be some of these users was a beneficial byproduct of this unique design.

The purpose of this paper is not to 'tout' Composeable FORCEnet as the be-all and end-all engineering design or the only possible implementation of FORCEnet, but merely to show how AG-6 has adopted it as one networking model to use in its scenario as they explore how coalition *forces will actually work together and interact.* SSC San Diego hosted the first full-fledged meeting of AG-6 and the group was able to see an extensive demonstration of Composeable FORCEnet and 'look under the hood' to determine if it was, in fact, a suitable framework for its study. As a result, AG-6 adapted the Composeable FORCEnet methodology for its purposes, and, for that reason, a short description of this FORCEnet prototype is in order here.

The intent of Composeable FORCEnet is to fundamentally alter the way in which military decision makers view, manage, and understand the information environment. Composeable FORCEnet supports shared situational awareness across strategic, operational and tactical levels to enable superior decision-making. Composeable FORCEnet tools enable the warfighter to compose C4ISR constructs 'on the fly' to build the right bundle of capabilities to deal with the current tactical and operational situation.

Technically, rather than building turn-key systems that require large investments in integration, Composeable FORCEnet represents a transformation toward providing seamless, open, object-based architectures that permit '*composeable*' information services, hardware, and applications. Composeable FORCEnet provides a new conceptual framework for distributing and sharing information, and eliminating information stovepipes. Research to date has shown that Composeable FORCEnet has the potential to dramatically change C4ISR operations by providing the means to achieve shared situational awareness through a tailorable and intuitive human-computer interface. Composeable FORCEnet supports shared situational awareness across strategic, operational, and tactical levels to enable decision-making that *vastly exceeds* that of any potential adversary.

Composeable FORCEnet has two primary goals. The first goal is to deliver a 'composeable' framework that enables the discovery and utilization of Web-based services and sources of Web-enabled data (or information) as well as to 'plug-and-play' new hardware and software. By composing various data sources, hardware, software, and services, including sensors and weapons, communications, computing, applications, collaboration, and human-computer interaction components, new functional capabilities can be created that meet emergent warfighting requirements. The framework for Composeable FORCEnet is based on open, public, distributed Web services, specifications, and standards. Thus, these new functional capabilities lead to the inherent ability to create new organizational structures and even permit the development of new and innovative tactics and doctrine without re-engineering supporting systems.

The second Composeable FORCEnet goal is to provide mechanisms to transform fused data of known pedigree into information and then into knowledge in a manner that directly supports decision making at all levels of command. This is accomplished through customizable (composeable) geo-spatial, functional, and temporal views of an operational situation, where the

full spectrum of warfighting plans, issues, concerns, and status can be tailored, assimilated, and understood by commanders and their battle staffs.

SSC San Diego developed a demonstration of the Composeable FORCEnet concept based on a straightforward, intuitive framework. The framework is based on a three-tiered architecture and uses the process of publication and subscription services. AG-6 observed the Composeable FORCEnet demonstration operating on an IP network, which meant that the demo could be run from any location with an Internet connection. Data is published from Web sources, which is straightforward, as well as from legacy sources, simply by tagging the data with XML.

Data is published into a translation server that objectifies it and geo-references it using publicly available Open GRS Consortium standards. The information in this layer can be subscribed to by any visualization client that is compliant with these standards. The demonstration AG-6 observed employed several of these visualization applications to represent the complex information that FORCEnet will make available. The Composeable FORCEnet concept for managing this complex data is based on the use of three interface metaphors. One metaphor is based on the recognition that warfighters think primarily in terms of geo-space (where am I, where is the enemy, etc.), so the map metaphor is used to represent the world, but it has been expanded greatly compared to what electronic maps can do. The second metaphor is the interface to functional information such as documents and images. For this information, the browser metaphor applies. The third metaphor is the interface to temporal information, such as schedules and plans. For that, a VCR or DVR metaphor is used, where historical information can be re-played, and the future, especially simulations and predictive modeling, can be fast-forwarded. These metaphors are seamless so that information in one domain can be dragged into another. For example, an image found through the browser could be dragged onto the map and ortho-rectified if it has latitude-longitude information within it. Finally, there is a robust collaboration capability so everything can be seen as a shared workspace. All of this functionality is the result of selecting applications, services, and tools that are compliant with open standards. No specific tools, or applications, or services, or data are mandatory in this system. Rather, the best technologies can be *composed* to deliver the final product.

Analogies to this approach are common in the commercial sector. One consumer-based example of composeability, as it applies to a capability, might be an individual who wishes to produce a home movie. Today, he/she might visit a local computer store and shop for a computer. There will probably be shelves of computers to choose from producers such as Sony, Fujitsu, Compaq, Toshiba, Mac, or a custom built PC. The selection depends on factors such as cost, memory, speed, and included peripherals. A movie-editing application would be selected from among several available from different software developers based on cost and features, and that software would be installed, usually via an installation wizard, into the computer. Then, a digital camera would be selected, again based on cost, resolution, size, zoom, and other features important to the user. As the scenes are shot, they can be loaded into the editing program using Firewire or USB connections, or perhaps via a disk. When a draft video has been completed, the producer might want to get some assistance from colleagues, so he/she can select an Internet provider based on cost and availability, and, using a browser of choice, the movie can be sent to them for their input using their own systems, which may include quite different components. What was accomplished in this process was to compose a capability by buying the components that met

each of the user's requirements. Moreover, as newer products with improved features become available, the users can replace one component at a time to achieve improved capability, leaving the other components in place to operate as before. This process was possible because commercial standards now permit these components to work together seamlessly.

Providing these kinds of capabilities to the warfighter has been the domain of the Composeable FORCEnet effort since its inception. Composeable FORCEnet provides the capability to demonstrate and evaluate the operational meaning of FORCEnet to the warfighter. In the conventional military sense, the operational construct of Composeable FORCEnet provides the ability to conduct and coordinate naval FORCE operations efficiently and effectively. This means:

1) A warfighter, or organization, can collaborate with anyone, anywhere, anytime.

2) Warfighters can allocate bandwidth and priorities for applications and individuals.

3) Warfighters define their own quality of service standard.

4) Warfighters can get sensor coverage when and where they need it.

5) Warfighters can tailor their information requirements to support their missions.

6) Warfighters can put the right weapon on the right target with speed and precision.

The Composeable FORCEnet technical concept is based on a fundamental departure from the legacy notion of system-centric application development and deployment. Decades of naval operational and technical experience have shown that interoperability cannot be achieved through the development of stovepipe applications and systems. Yet neither can interoperability be achieved solely through systems integration, or even a system-of-systems concept – a set of systems that has been integrated via a layer of blanketing middleware code (another, larger stovepipe). Interoperability is likely to require the adoption of a service-oriented approach rather than a system-oriented one. Composeable FORCEnet adopts such an approach. A service-oriented architecture delineates the roles of service provider and service consumer in network-centric operations, and emphasizes the benefits of this modular approach. Focusing component definition on providing or consuming a defined service simplifies design and greatly eases the burden of integration, deployment, and maintenance.

Composeable FORCEnet rests solidly on the foundations of open industry standards for interoperability and the ideas of modular Web services. Composeable FORCEnet combines a unified objectified view of all relevant data with a new geo-spatial metaphor for information understanding to bring shared situational awareness across the battlespace. To this end, Composeable FORCEnet couples a powerful information representation, management, and domain engineering methodology with emerging industry standards for information exchange and understanding.

As defined at the outset of this section, composeability in the sense that it is used in the context of FORCEnet has a broader definition than merely the Web services, the data sources, and the applications. Composeable FORCEnet is meant to convey the idea that, by virtue of the ability to compose these components, it should become possible to compose organizations because they are inherently interoperable through composeable services. This is the essence of what makes Composeable FORCEnet attractive as a coalition command and control tool and why AG-6 has adopted it to inform its work.

Summary and Conclusions

The combination of determining the parameters of coalition interoperability and particularly understanding how much is enough and how to quantify it is a large subject and has taken a 'long paper' to properly address the issue. A long paper might imply there will be an extensive summary and conclusions – but this is not the case.

What this paper has demonstrated can adequately be summed up in just six points, and these 'bullets' represent the major takeaways of this paper:

- The importance of coalition operations is strong, and growing, and coalition operations already represent the norm for any significant operation.
- One of the most important pillars of coalition interoperability – and arguably the most critical one – is C4ISR.
- The technical details of enabling coalition partners to achieve C4ISR interoperability are not trivial and must be worked by all coalition partners.
- TTCP offers an extant vehicle to continue to analyze the value-added of enhanced coalition C4ISR interoperability.
- The TTCP MAR AG-1 and AG-6 groups have done – and continue to do – significant work to examine the effectiveness of coalition interoperability.
- Composeable FORCEnet offers one methodology to ensure FORCEnet is coalition capable and provides seamless interoperability at sea.

While these are only interim results, since AG-6 has two years of dedicated work ahead, the prospects for demonstrating the manifest benefits of robust coalition interoperability through ongoing, focused analysis appear to be excellent.