The Ninth International

Command & Control Research and Technology Symposium

Paper Title:

# Developing and Populating the Global Information Grid for Joint and Coalition Operations: Challenges and Opportunities

Topical Area:

Network Centric Operations Transformation

Mr. George Galdorisi (point of contact)
Mr. Dan Thigpen
Mr. Frank White

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
Dan.Thigpen@navy.mil

# Abstract

Network Centric Operations are transforming the nature of warfare. While literally countless definitions have been offered to explain Network Centric Operations and Network Centric Warfare, recent directives by the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) have served to bound the problem and define the elements of the Global Information Grid (GIG) – the foundation for Network Centric Warfare. This paper addresses a critical element of this GIG construct – how will the GIG be populated and developed to ensure success in Joint and coalition operations. We assert that a GIG designed to be utilized by U.S. *and* coalition forces and a GIG populated by a wide array of U.S. *and* coalition sensors and other dynamic sources of information will be a much more powerful tool than a GIG that is designed, developed, resourced and used nearly exclusively by U.S. forces. We base this assertion on the operational realities of warfighting and the lessons learned from Operational Enduring Freedom and Operation Iraqi Freedom. For example, in the naval context, in the spring of 2002, during Operation Enduring Freedom, 91 coalition ships were concentrated in the Central Command Area of Responsibility. While 31 of these ships were U.S. Navy ships, 60 of these ships belonged to U.S. coalition partners. Clearly, the success of this U.S.-led operation – as well as others – was tremendously enhanced by the warfighting capabilities provided by a robust array of coalition assets. As the United States' military builds and populates the Global Information Grid as the foundation for Network Centric Warfare the value-added of building the GIG in such a way that it both supports coalition partners and accommodates sensors and systems that these partners bring to the table is clear. While the construct of the GIG as it is currently envisioned does not exclude coalition partners, this paper suggests that insufficient effort has yet been applied by each of the United States' military services to constructing their portions of the GIG to easily and seamlessly accommodate coalition partners. Thus, our paper's thesis boils down to this: While our coalition partners ask what the *price of admission is* to work with United States military forces, in a GIG-enabled environment we ask *what the price of omission* is if the United States fails to include these coalition platforms - as well as the sensor suites they bring to the fight – into our Global Information Grid and other warfighting networks. We assert that the price of omission is too high and robust efforts must be undertaken immediately to accommodate potential coalition partners into the GIG at the earliest stages of its development.

# Developing and Populating the Global Information Grid for Joint and Coalition Operations: Challenges and Opportunities

*In today's world, it is inconceivable that anything could be accomplished outside of coalition operations.*

Dr. David Alberts
Director, Research and Strategic Planning
Office of the Assistant Secretary of Defense NII
Seventh ICCRTS – September 16, 2002[1]

*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.*

Professor Paul Mitchell
Director of Academics – Canadian Forces College
Naval War College Review – Spring 2003[2]

*The United States has long been a strong proponent of naval coalition operations and has led such coalitions in a wide variety of wartime and peacetime operations over the past several decades. As United States Navy and Marine Corps units field increasingly robust C4ISR capabilities, U.S. allies – who rarely can afford the IT-21 capabilities of U.S. Navy ships – continue to ask what the "price of admission" is to work with U.S. carrier strike groups and expeditionary strike groups. But as the United States Navy slips below 300 ships the question U.S. Navy planners must ask is what is the "price of omission" if it is unable to find a way to seamlessly fold coalition ships into a U.S. Navy network. As the Navy designs FORCEnet – the "glue" that holds together the elements of Sea Power 21 – it must design it in a way that readily enables our allies to participate in the net or we will lose them as vital contributors to naval warfighting – perhaps forever.*

## Introduction

Network Centric Operations are transforming the nature of warfare. While literally countless definitions have been offered to explain what Network Centric Operations and Network Centric Warfare, recent directives by the Assistant Secretary of Defense for Networks and Information

Integration (ASD/NII) have served to bound the problem and define the elements of the Global Information Grid (GIG) – the foundation for Network Centric Warfare.[3] ASD/NII's three goals; 1) make information available on a network that people depend on and trust, 2) populate the network with new, dynamic sources of information to defeat the enemy, and 3) deny the enemy comparable advantages and exploit weaknesses, provide the key parameters for the Navy as it has designed its component of the GIG.[4]

That Navy component is FORCEnet – the "glue" that holds together the three key components of Sea Power 21; Sea Strike, Sea Shield, and Sea Basing. FORCEnet was conceptualized by the Chief of Naval Operations Strategic Studies Group and formally unveiled by the CNO at the Naval War College's Current Strategy Forum in June 2002.[5] In the relatively short time since then, the FORCEnet concept has morphed rapidly into a well-defined program under the stewardship of the Deputy Chief of Naval Operations for Warfare Requirements and Programs and the Commander of the Navy Network Warfare Command. The Department of the Navy's FORCEnet Campaign Plan offers a working definition of FORCEnet.[6]

> FORCEnet is the architectural framework for naval warfare that aligns and integrates warriors, networks, sensors, command & control, platforms and weapons into a globally networked, distributed combat force, scalable across the spectrum of conflict from seabed to space and from sea to land.

The FORCEnet Campaign Plan notes further that FORCEnet "will be developed and delivered to function in a Joint/Allied/Coalition/Interagency environment and that associated architectures, systems and doctrine must focus on interoperability.[7] While the Campaign Plan provides this general assurance that FORCEnet will be compatible with coalition forces, few details are provided regarding how this will be accomplished. Much is left to the imagination regarding how FORCEnet will be populated and developed to ensure success in naval coalition operations. Intuitively, a FORCEnet designed to be utilized by U.S. *and* coalition forces and a FORCEnet populated by a wide array of U.S. *and* coalition sensors and other dynamic sources of information will be a much more powerful tool than a FORCEnet that is designed, developed, resourced and used nearly exclusively by U.S. forces.

## FORCEnet as an Enabler for Warfighting at Sea

The importance of building a FORCEnet grid that is compatible with coalition partners is not based solely on the need to conduct coalition operations for "political cover" – although this is an important consideration – but on the operational realities of warfighting and the lessons learned from Operation Enduring Freedom and Operation Iraqi Freedom. For example, in the spring of 2002, during Operation Enduring Freedom, 91 coalition ships were concentrated in the Central Command Area of Responsibility. While 31 of these ships were U.S. Navy ships, 60 of these ships belonged to U.S. coalition partners (see Figure 1).[8] Clearly, the success of this U.S.-led operation – as well as others – was tremendously enhanced by the warfighting capabilities provided by a robust array of coalition assets and sensors. But will our coalition partners be able to work effectively in the future with a FORCEnet-enabled United States Navy?

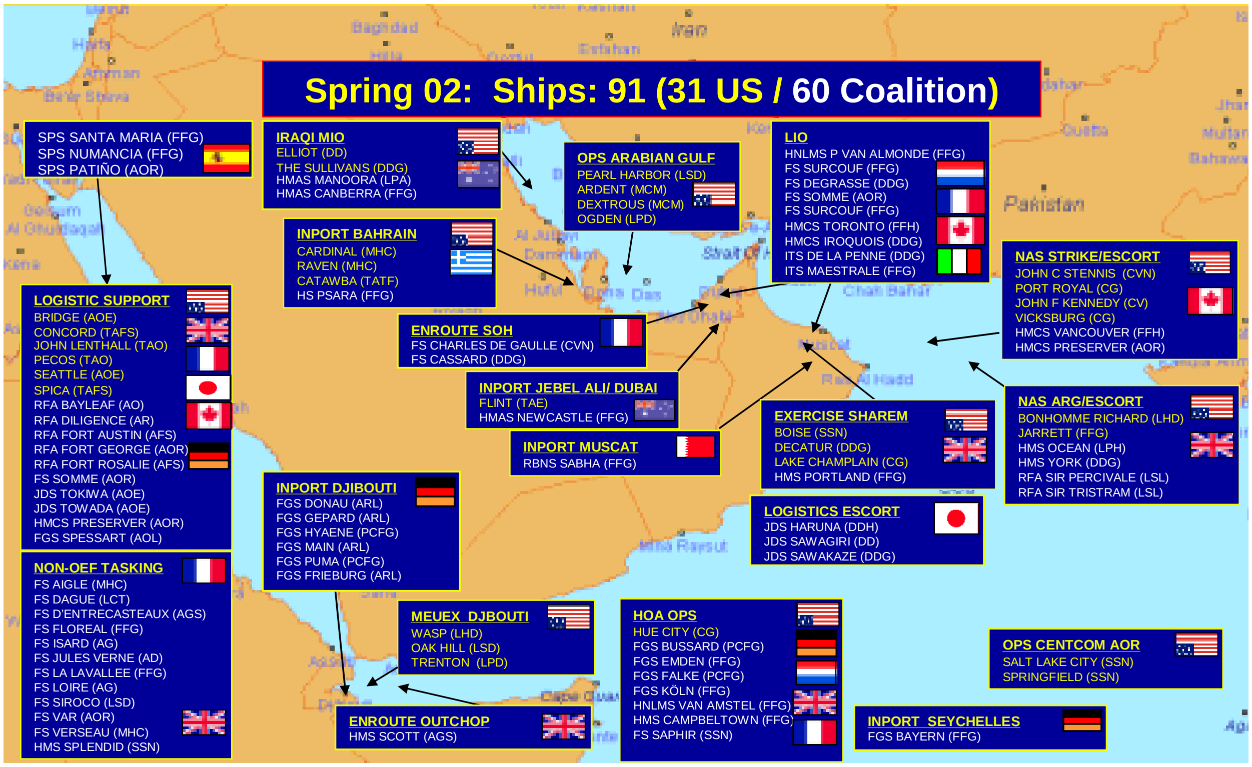

Figure 1. Maritime Coalition

This is not a trivial question, as the trend towards naval coalition operations is not an artifact of these two short, discrete conflicts but a fact of life engendered by the worldwide war against terrorism. In a widely-publicized speech at the Naval War College's 16th International Seapower Symposium in October 2003, the Chief of Naval Operations called for enhanced international naval cooperation – a "maritime NORAD" – as a critical element in a coalition strategy against terrorism.[9] Given the United States Navy's worldwide global commitments it appears likely that the CNO's call for coalition partners to work together with the United States at sea is an idea that has traction.

As the United States' Navy builds and populates the FORCEnet grid as the foundation for the maritime component of Network Centric Warfare, the value-added of designing and building FORCEnet in such a way that it both supports coalition partners and accommodates sensors and systems that these partners bring to the table is clear. A FORCEnet grid populated exclusively by U.S. sensors and systems may, in fact, be unaffordable and ineffective. A major naval operation conducted solely by United States Navy forces may have severely proscribed operational effectiveness compared to what could be accomplished with a coalition force fully embedded in the net.

The importance of including U.S. coalition partners "in the net" was put most succinctly by the Director of the U.S. Department of Defense Office of Force Transformation, Vice Admiral Art Cebrowski, who opined; "The United States wants its partners to be as interoperable as possible. Not being interoperable means you are not on the net, so you are not in a position to derive power from the information age."[10] While the construct of FORCEnet as it is currently envisioned does not exclude coalition partners, the United States Navy may be in danger of inadvertently excluding coalition partners from the net – and effectively marginalizing their contributions to warfighting effectiveness if including coalition partners in FORCEnet does not become primary criteria in its design.

### FORCEnet as an Enabler for Networking United States and Coalition Partners

How important is coalition participation in FORCEnet? The exigencies of modern naval warfare – demonstrated in Operation Enduring Freedom and Operation Iraqi Freedom - suggest that rather than long-standing naval alliances, where coalition had ample time to absorb doctrine, operating precepts and tactics, tomorrow's coalition operations will feature pick up games with coalition ships, aircraft and other units arriving on scene ready to fight – if they are able to check into the net. This strongly suggests that FORCEnet be designed from the keel up to have the ability to seamlessly include coalition partners in the net.

Not all observers are sanguine that the United States Navy can overcome policy and security issues and design FORCEnet in a manner that enables dynamic coalitions of naval forces to work together seamlessly. Thomas Barnett of the Naval War College has noted, "Not only will our allies have little to contribute to a come-as-you-are party, they won't be able to track the course of the conversation."[11] Others, such as Paul Mitchell of the Canadian Forces College – citing the experience of Canadian ships assigned to United States Navy Carrier Battle Groups – are even more pessimistic. Professor Mitchell opined in a recent *Naval War College Review* article that: "The United States is unlikely to hamstring its own military forces or to slow its implementation of network-centric warfare given its obvious benefits. It may decide simply to "pass" entirely on alliance participation."[12]

These observers, and others, have correctly pointed out that while coalition operations in the previous century has worked adequately based on voice transmissions and limited data exchanges, with the advent of network centric warfare future coalition operations will only be effective if coalition partners have *real-time* access to the same information that U.S. forces have access to. They point out that this "need for speed" in network-centric operations places the notion of multinational operations at risk especially when coalition partners must operate on separate networks with different security levels and when interoperability barriers may exclude even close allies.

The state of the art in maritime network-centric warfare today features inefficient work around solutions to coalition interoperability. For example, during Operation Allied Force, due to the inadequacy of the NATO information grid, the United States was unable to pass along high-fidelity data to alliance partners. This led to difficulties attacking time-sensitive targets where continuous data exchange and precision updates between sensor and shooter were needed until the target was destroyed.[13] This allied connectivity problems were so severe during Operation Sharp Guard that one observer likened the situation to "the equivalent of changing to a different railway gauge at each national boarder."[14] Thus, in maritime coalition operations over the past decade, the "need for speed" engendered by attempting to operate in a network-centric fashion has bumped up squarely against a patch-work of networks that were not inherently interoperable.

For the United States, it would appear that there is little likelihood that coalition interoperability can be achieved by continuing to make incremental changes to existing communications and data exchange systems and that a new system must be designed from the ground up that will enable the seamless exchange of information between and among coalition partners. In the maritime domain this means that coalition partners must have access to the FORCEnet and this cannot be a U.S.-only system. The best way to accomplish this is to build FORCEnet at the outset to readily accommodate coalition partners. Experience with other acquisition programs – most notably the Joint Strike Fighter - indicates that designing coalition interoperability into FORCEnet at its early design stages is far more effective than attempting to modify FORCEnet to accommodate coalition sensors and systems after it is built.

None of this is to suggest that the success of United States and coalition force naval operations will be ensured if only the right "technical attributes" are built into FORCEnet. There are significant policy, security, and, in particular, releasability issues, that must be worked through. However, these are issues that can be dealt with relatively swiftly when policymakers elect to do so – while redesigning FORCEnet after it is built to accommodate coalition partners in the net is something that cannot be accomplished overnight.

This may be a "chicken and egg" issue that has impeded more rapid resolution of naval coalition interoperability issues. On the one hand, some members of the technical community have opined that releasability issues so impede coalition interoperability efforts that it is futile to attempt to design technical systems with a high degree of coalition interoperability only to have releasability issues preclude any interoperability at all. On the other hand, some members of policy and security community have opined that robust technical pathways to effective coalition interoperability are not available, making arguments about information releasability moot.

There is compelling evidence that there is sufficient progress on both sides of this issue to overcome the concerns of even the most hardened skeptics. The initial instantiations of the FORCEnet architecture documents allow sufficient flexibility to design FORCEnet *from the outset* in a manner that will accommodate coalition platforms, systems and sensors.[15] With respect to releasibility – long the Achilles heel of effective coalition interoperability - the Office of the Secretary of Defense for Intelligence has indicated that government officials are nearing an agreement that will allow coalition partners to gain access to data posted on the Secret Internet Protocol Router Network (SIPRNET), the primary communications and planning network utilized by the United States Navy.[16]

Taken together, these changes to the technical and policy issues impacting FORCEnet bode well for those designing and building FORCEnet to engineer it at the outset for robust coalition interoperability. At the highest levels of the Department of the Navy, there is recognition that coalition interoperability is crucial to the ability of the Navy and Marine Corps to carry out their missions. The Secretary of the Navy's *Report to the Congress on FORCEnet* indicates, "FORCEnet planning is being coordinated with allies and coalition partners."[17] However, this document provides little indication of how this is to be done, nor does it establish a review process that ensures that there are checks and balances that require program managers responsible for the multiple systems and sensors supporting FORCEnet.

## Conclusions and the Way Ahead

If FORCEnet is to function as the key to netting together U.S. navy *and* coalition partner there must be both a top-down and a bottoms-up approach to achieving this. At the highest levels, policy makers and acquisition professionals must provide the explicit guidance and direction regarding coalition interoperability and provide the requisite funding to achieve this.

Concurrently, at the operational level, warfighters must continue to articulate the importance of coalition interoperability in much the same way as Admiral Robert Natter, then-Commander of U. S. Fleet Forces Command put it in the aftermath of Operation Enduring Freedom:[18]

> The significant involvement of coalition forces in Operation Enduring Freedom – including over 100 ships deployed in Central Asia for an extended period – has re-emphasized the requirement for improved IP (internet protocol) data systems interoperability with allied and coalition forces.

Additionally, the good work that is currently ongoing between and among both formalized and more ad hoc coalition partnerships, ranging from AZCANZUKUS, to The Technical Cooperation Program (TTCP), to various Defense Exchange Agreements, needs to be enabled beyond merely serving as contact and information exchanges. These groups – and others – if empowered by their national authorities, are ideally suited to identify, experiment with, and implement concepts and technologies that can contribute to integrated coalition warfare in a FORCEnet environment. Not only would this early cooperation transform FORCEnet from a U.S.-centric capability that the United States is trying to "force" upon its partners in maritime coalition operations to a system with extensive coalition buy-in, but it would also make available to the FORCEnet engineering community a wide array of cutting-edge research that our most likely coalition partners are currently conducting – especially in the areas of information fusion and situational awareness.

The good news for the United States Navy and for the wide array of its potential coalition partners is that there now appear to be no systemic impediments to design FORCEnet in a way that *enables*, rather than *proscribes*, robust coalition participation in naval network centric warfare. What the Navy must do as it begins the journey to build and deliver FORCEnet is to keep the operational need to include coalition partners in the net at the forefront in designing FORCEnet. If the Navy fails to do that, it may inadvertently create a warfighting environment at sea where the United States can only act unilaterally – a situation that would almost certainly ensure that we would not prevail at sea in the new millennium.

# Notes

1. *Proceedings, Seventh International Command and Control Research and Technology Symposium (ICCRTS)*, Quebec City, Quebec, September 16-17, 2002. Accessed at Command and Control Research Project website: www.dodccrp.org

2. Paul T. Mitchell, "Small Navies and Network-Centric Warfare: Is There a Role?" Naval War College Review, Spring 2003, pp. 83-99.

3. Department of Defense Instruction 8100.1 *Global Information Grid Overarching Policy*, September 19, 2002.

4. Memorandum from Department of Defense Chief Information Officer, *DoD Net-Centric Data Strategy*, May 9, 2003.

5. *Sea Power 21: Operational Concepts for a New Era* (Washington, D.C., Department of the Navy, June 2002).

6. Office of the Chief of Naval Operations/Commanding General Marine Corps Combat Development Command Memorandum for Distribution *FORCEnet Campaign Plan* Ser N61FP/3U606721 (Washington, D.C., Department of the Navy, 3 June 2003), p. 3.

7. FORCEnet Campaign Plan, p. 4.

8. Briefing, Commander, U.S. Naval Forces Central Command, May 13, 2002.

9. Lawrence Modisett, "Joint Efforts of World's Navies Could Lead to Smooth Sailing," *Boston Herald*, November 16, 2003.

10. Office of the Secretary of Defense, Office of Force Transformation, Military Transformation: A Strategic Approach, Fall 2003, accessed at: www.oft.osd.mil

11. Thomas Barnett, "The Seven Deadly Sins of Network Centric Warfare," U.S. Naval Institute Proceedings, January 1999, p. 37.

12. Mitchell, "Small Navies and Network-Centric Warfare: Is There a Role?" p. 91.

13. Joseph M. Ladymon, "Network Centric Warfare and its Function the Realm of Interoperability," Acquisition Review Quarterly, Summer 2001, p. 115.

14. "General Warns over Digitisation Split," International Defence Review, January 1, 2002.

15. Office of the Chief Engineer, Space and Naval Warfare Systems Command, FORCEnet Architecture Vision, Preliminary Draft, Version 1.1, May 23, 2003.

16. Amy Butler, “U.S. Nearing Agreement to Allow Coalition Partners Access to Classified Data,” *Defense Daily*, November 19, 2003.

17. Office of the Secretary of the Navy, *Report to Congress on FORCEnet*, May 16, 2003.

18. Space and Naval Warfare Systems Center Charleston, *Chips*, Summer 2002, p. 4.