15th ICCRTS
The Evolution of C2

Paper entitled:
Coalition Networking in a Service Oriented Architecture Environment

Topic:
Topic 3: Information Sharing and Collaborative Processes and Behaviors

Mr. George Galdorisi (Point of Contact)
Space and Naval Warfare Systems Center Pacific
Dr. Stephanie Hszieh
Space and Naval Warfare Systems Center Pacific
Mr. Martin Jordan
Space and Naval Warfare Systems Command
Dr. Stephan Lapic
Space and Naval Warfare Systems Center Pacific

Space and Naval Warfare Systems Center Pacific
53560 Hull Street
San Diego, California 92152-5001
(619) 553-2104
george.galdorisi@navy.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Coalition Networking in a Service Oriented Architecture Environment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Space and Naval Warfare Systems Center Pacific,53560 Hull Street,San Diego,CA,92152-5001**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

Proceedings of the 15th International Command and Control Research and Technology Symposium (ICCRTS '10), Santa Monica, CA, June 22-24, 2010

14. ABSTRACT

The need for U.S. forces to operate effectively with coalition partners is recognized at the highest levels of the United States national and defense policies and doctrines. For the U.S. Navy, enhanced coalition operations is now a key part of its maritime strategy and is best articulated in the Global Maritime Partnership initiative. As maritime networks have emerged as the primary means of communications within forces of advanced navies, rapid technological change ? as well as the cost of new networking systems ? has often led to an uneven technical infusion of new systems. The U.S. Navy has embarked on an ambitious program to develop a fully networked force and to operate in a Service Oriented Architecture (SOA) environment known as FORCEnet. The Navy has been exploring how to best leverage FORCEnet to enhance effective coalition networking and make the Global Maritime Partnership a reality. For SOA to fully exploit the capabilities of a networked force, a shift in the architecture and configuration of application services is required. AUSCANNZUKUS C4 experimentation in Trident Warrior has validated the requirement for distributed applications and network services and the need for SOA to push the data out to the warfighter as far forward as possible. We will present the results of experimentation and analysis efforts conducted under the auspices of AUSCANNZUKUS and The Technical Cooperation Program (TTCP) ? a five-nation defense science collaboration effort ? to demonstrate the enormous potential of effectively networking coalition navies.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**12**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

ABSTRACT

The need for U.S. forces to operate effectively with coalition partners is recognized at the highest levels of the United States national and defense policies and doctrines. For the U.S. Navy, enhanced coalition operations is now a key part of its maritime strategy and is best articulated in the Global Maritime Partnership initiative. As maritime networks have emerged as the primary means of communications within forces of advanced navies, rapid technological change – as well as the cost of new networking systems – has often led to an uneven technical infusion of new systems. The U.S. Navy has embarked on an ambitious program to develop a fully networked force and to operate in a Service Oriented Architecture (SOA) environment known as FORCEnet. The Navy has been exploring how to best leverage FORCEnet to enhance effective coalition networking and make the Global Maritime Partnership a reality. For SOA to fully exploit the capabilities of a networked force, a shift in the architecture and configuration of application services is required. AUSCANNZUKUS C4 experimentation in Trident Warrior has validated the requirement for distributed applications and network services and the need for SOA to push the data out to the warfighter as far forward as possible. We will present the results of experimentation and analysis efforts conducted under the auspices of AUSCANNZUKUS and The Technical Cooperation Program (TTCP) – a five-nation defense science collaboration effort – to demonstrate the enormous potential of effectively networking coalition navies.

PERSPECTIVE

"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

"What underpins that view of a 1,000-ship Navy is essentially the relationships, the capabilities of 1,000 connections, whatever they might be, from whatever service, and that doing that together gives us the opportunity to really achieve greatness, and to the degree we don't, the opposite happens."[2]

Admiral Michael Mullen
Chairman, Joint Chiefs of Staff
Australian Defence College
February 22, 2008

"Partnerships are an integral part of our Maritime Strategy today. From the highest level of warfare to the humanitarian assistance missions, Global Maritime Partnerships are playing a decisive role in keeping the peace."[3]

Admiral Gary Roughead
Chief of Naval Operations
Rhumb Lines
September 3, 2008

"Global Maritime Partnerships are setting the standard for international cooperation, in our globalized world and they are an important element to achieving stability in the global commons upon which we all rely."[4]

Admiral Gary Roughead
Chief of Naval Operations
22nd Surface Navy Association National Symposium
January 2010

Much has been written and spoken about coalition interoperability, but the quotations above capture the essence of its importance and the challenges facing today's naval forces. 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 at sea is to court disaster. The need for U.S. forces to operate effectively with coalition partners is recognized at the highest levels of the United States National Security, Intelligence, and Defense policy and doctrine. From the President's *National Security Strategy*, to the Director of National Intelligence's *Global Trends 2025*, to the Secretary of Defense's *National Defense Strategy*, this need to ensure seamless interoperability with coalition partners is articulated as an urgent requirement.

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."[5] This theme is well understood within the U.S. military as it increasingly recognizes the importance of coalition operations.

Nowhere is this requirement more urgent than for U.S. naval forces. Naval forces are traditionally first on scene in a crisis and when forces of other services arrive, they typically "fall in" on top of the networks that these naval forces have established. For the U.S. Navy, enhanced coalition operations are now a key part of its maritime strategy—*A Cooperative Strategy for 21st Century Seapower*.[6] Known as the Global Maritime Partnership, the U.S. Navy's initiative to work closely with coalition partners evolved from then-CNO Admiral Mullen's concept of creating a thousand ship navy of coalition partners and allies to respond to international natural disasters and fight the war against violent extremism.

From the perspective of the U.S. 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 U.S. 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.[7] 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.

It is this operational necessity that dictates the importance of coalition operations, and it is the operators who are saying that the price 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 U.S. 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 the requirement for improved internet protocol data systems' interoperability with allied and coalition forces."[8] More recently, U.S. Marine Corps General Michael Mattis, then-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."[9]

The leadership of other major navies also recognizes the importance of coalition interoperability. For example, The Royal Australian Navy's Chief of Navy, Vice Admiral Russ Shalders, has indicated that Australia has adopted a doctrine of naval co-operation that will lead to "a maritime neighbourhood watch scheme" involving joint exercises with old foes such as Russia and China.[10] The Royal Navy's Chief of Naval Staff and First Sea Lord Admiral Sir Jonathon Band has argued that the Royal Navy should accept sacrificing quality for quantity if it is to maintain a surface fleet of sufficient size to contribute to maritime security operations on a global scale.[11] This interest spreads beyond traditional naval allies to include emerging regional and global naval powers such as India who are exploring the potential benefits of sharing information about maritime threats and situations. [12]

THE TECHNICAL CHALLENGE

While senior naval officers and operators in navies united in the Global Maritime Partnership have expressed the *desire* to effectively network their navies together, the details of *how* this is to be achieved

has been left to the technical communities of these navies. Moreover, the rapid advance of technology over the past few decades has made naval coalition communications more, not less, challenging. Why is this so? As naval networks have emerged as the primary means of communications within forces of advanced navies, rapid technological change – as well as the cost of new networking systems – has often led to uneven technical infusion of new systems. Thus, the very technology that has helped each navy communicate *within* its national force has at times *impeded* effective communications with the forces of other navies.

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?"[13] Some would say that it is not yet where it should be. Writing in the authoritative *Naval War College Review*, Professor Paul Mitchell, the former 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."[14]

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 is important work yet to be done. Additionally, this is consistent with what proponents of network-centric operations have been exposing for some time. The late Vice Admiral Arthur Cebrowski, considered by some to be the "father of network-centric warfare," states: "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."[15]

The U.S. Navy has taken a proactive role in working to solve coalition networking challenges through international fora and partnership-building activities with likely coalition partners – particularly with "five eyes" nations (Australia, Canada, New Zealand, United Kingdom and United States) – under the auspices of the AUSCANNZUKUS partnership and The Technical Cooperation Program (TTCP). These navies have worked together to identify the requirements for coalition operations, the technical capabilities needed to operate in concert, and the technology gaps where they exist. The most effective technical solutions are those that are developed collaboratively by all partner nations, demonstrated in laboratory environments, and then rigorously assessed in operational settings such as Trident Warrior.

ACHIEVING BREAKTHROUGH TECHNICAL SOLUTIONS

To serve Navy and Joint needs – and also to enable effective coalition networking at sea – the U.S. Navy has embarked on an ambitious program to develop a fully networked force and to operate in a Service Oriented Architecture (SOA) environment. Within the Navy, the evolution towards SOA is driven by three major initiatives: the Consolidated Afloat Network Enterprise System (CANES) – which will enhance C4 delivery by leveraging SOA, the Consolidated Net-Centric Data Environment (CNDE) – which will provide over-arching data management, fusion, and governance for the Fleet, and Navy involvement in the Joint Multi-service SOA Consortium. The latter organization strives to rationalize SOA efforts between the US services. The Navy has also been proactively engaging its coalition partners in exploring how to best leverage its enormous investment in net-centricity and SOA to enhance coalition effectiveness and to make the Global Maritime Partnership a reality. We will present a broad spectrum of this work in this section.

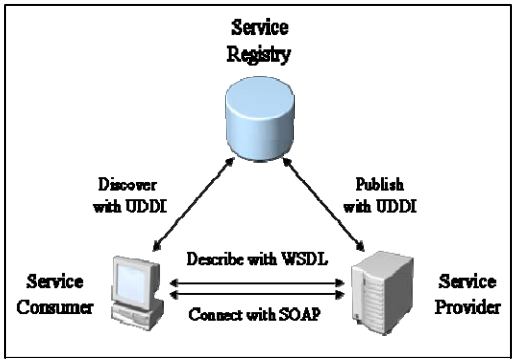

Figure 1: Three Principal Components in SOA

SOA is a distributed computing paradigm in which end-user functionality is created by coupling autonomous software services using well-defined interfaces.[16] There are three principal components in SOA: the service consumer, the service provider, and a service registry where the provider publishes its capabilities for the consumer to discover. A consumer of one service may of course provide another service in turn. The promise of SOA is that the dynamic composition of these services can provide an end-to-end user capability. While the service interfaces must be well-defined, the specifics of service execution need not be. Implementation and inter-operability is achieved by adhering to standards and implemented via a service contract which stipulates how service consumers bind to providers.

While the SOA concept is not tied to a particular technology, web services are the preferred framework for its delivery.[17] In a SOA implementation based on web services, the contract between consumers and providers is described by Web-Services Description Language (WSDL) and implemented using Simple Object Access Protocol (SOAP). Services are published and discovered using Universal Description, Discovery, and Integration (UDDI). These transactions are all based on well-known and platform-independent Extensible Markup Language (XML). It is the combination of these protocols that make web services so attractive and why web services are used in nearly all SOA implementations. Most registry services typically organize services based on criteria and categorize them. Embedding a registry within SOA provides for scalability of services and allows services to be added incrementally. It decouples consumers from providers and provides a look-up service for consumers. Consumers can now choose between providers at runtime rather than hard-coding a single provider. Of course, SOA in general and web-based SOA in particular has been developed in the business context, and we are required to move it into the Defense arena and in a multi-national setting besides.

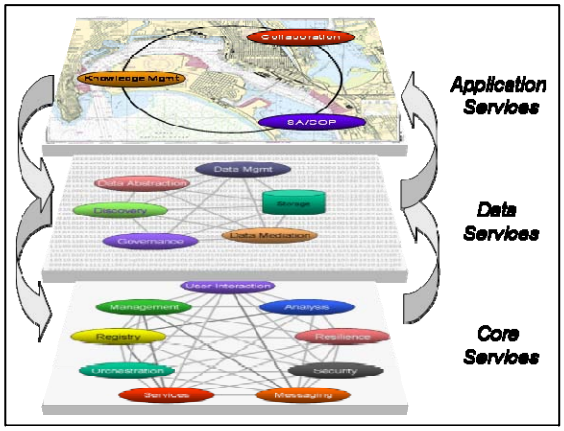

Figure 2: Coalition C4 SOA

In our vision, a coalition C4 SOA consists of three layers: Application services such as Situational Awareness (SA) and shared Common Operational Picture (COP) are implemented for communities of interest on top of a data services layer. The data services layer is much more than a database, but also includes support for data discovery, understanding formatting (via XML metadata for example), fusion, and other features. The data services are in turn supported by a SOA core services layer which provides discovery, messaging, mediation, identity management, security, and other basic services required for the SOA.

For SOA to fully exploit the capabilities of a networked force, including ship-ship networking systems such as EHF TIP or Subnet Relay, a shift in the architecture and configuration of application services is required. Today, with rare exceptions, applications and network services are homed at the Network Operations Center (NOC) or data center, requiring the operator to reach back to shore for all services. Even with direct ship-to-ship network connectivity, these services still require reach-back to shore facilities. Efficient use of the network means using all available network connections and resources. Likewise, today's applications are relatively rigid, lacking the flexibility to be easily reconfigured in response to operational exigencies. The increased robustness and agility required for coalition network-centric operations requires a significant shift in C4

architectures. Single points of failure (such as satellite connections) must be removed. Centralized and monolithic services must be transformed into distributed service modules that can be rapidly recomposed as required. These emerging operational requirements are addressed in part by Service Oriented Architectures and explain the appeal of SOA to U.S. Navy and coalition forces. Within the five AUSCANNZUKUS navies, C4 experimentation in Trident Warrior has validated the requirement for distributed applications and network services and the need for SOA to push the data out to the warfighter as far forward as possible.

Commercially, Universal Description, Discovery and Integration (UDDI) is a platform-independent, XML-based registry for businesses worldwide to list themselves. As an open industry initiative, UDDI enables businesses to publish service listings and discover each other and define how the services or software applications interact over the Internet. A UDDI business registration consists of three components: White Pages, Yellow Pages and Green Pages. White Pages contain the address, contact, and known identifiers. Yellow Pages include industrial categorizations based on standard taxonomies. Green Pages contain the technical information about services exposed by the business**.** There is a critical need to translate this into the Defense context at the Strategic, Operational and Tactical levels on CENTRIXS[18] and other Defense networks.

Service providers and consumers communicate via messages. Services expose an interface contract, which defines the behavior of the service and the messages they accept and return. Because the interface contract is independent of platform and language, the technology used to define messages must also be agnostic to any specific platform or language. For web-based SOA, messages are typically constructed using XML documents that conform to XML schemas. Because consumers and providers communicate via these messages, the structure and design of messages require careful consideration. Messages need to be implemented using a technology that supports the scalability requirements of services. Having to redesign messages will break the interface to providers, which can prove to be costly.

Service orchestration is an extension of the service composition model where a parent service layer performs an orchestration of many business and utility services by controlling workflow logic and invocation sequences. Complex service and business process interactions require a service orchestration platform such as a Business Process Execution Language (BPEL) engine. BPEL has limited capabilities in terms of modeling real-world complex workflows. The focus on BPEL should be as a service orchestration vehicle rather than a full-blown workflow modeling tool. Some BPEL implementations come packaged with commercial Enterprise Service Bus (ESB) products. The impacts on interoperability in a heterogeneous SOA that implements different BPEL engines or different ESB products has not been widely explored or quantified, particularly in the Allied/Coalition space.

SOA is driven by metadata, which is crucial to the development lifecycle of web services.[19] Without metadata, the long term maintainability of a SOA is at risk, because the business logic expressed in services is not visible to software engineers at a higher level than in the code itself. A metadata repository is now required. Spreadsheets and web page listings no longer suffice. Metadata can be used to provide a complete description of the service, including its policies, security requirements, business metrics, service level agreements, and so on, and includes XML schemas, SOAP messages and WSDL interface definitions.

In a SOA, the business logic is expressed in message payloads that are constrained by XML schemas. These schemas define the metadata governing how messages are handled. They are externalized, standardized, and federated, thus providing many advantages to the end-user. Advantages include enforceable contracts for processing behavior, visible specifications for developers, public interfaces for new partners in the architecture, schema-based access to standard infrastructure such as parsers,

transformation engines, etc., insulation for services from changes to schemas, and support for business analysts when planning changes.

The disadvantages of XML schemas are due entirely to the limitations of metadata in general and XML schemas in particular. As a rule, we expect XML schemas to change. XML schemas describing web services message payloads are application-specific, bespoke metadata, which requires human involvement when it changes. Unfortunately, developers modify schema-driven applications by editing the schemas. There is currently no robust, scientific mechanism for identifying where every object in a schema has been defined and referenced. Changing an XML schema is therefore an intensely manual activity. For multiple schema families and multiple developers (or worse, multiple teams of developers), one runs the very serious risk of developing inconsistencies as a result of modifications. In an orchestrated set of web services used and maintained by multiple development teams, the externalized schemas and transformations describe or reference the same data objects over and over again. Schema families and their associated assets present us with horrific redundancy and duplication when we try to evolve them by editing them. Modification of objects presents the kind of maintenance nightmare that should be avoided if at all possible.

Managing the lifecycle of a web services development, particularly from the perspective of the evolution of metadata, is not simply a schema-versioning problem. Versioning schemas are about technical constructs and development processes, not about the management of metadata evolution. Metadata evolution management is one of the biggest problems facing the long term lifecycle management of web services development projects. Metadata evolution management is not scalable with most current technology. To support active metadata, we need a new mix of technologies. An enterprise data dictionary platform is necessary to make all service-related metadata centrally visible to developers, wrapped in a development environment that conforms to a model-driven architecture. Changes to metadata must be powerfully implemented in one central place (within a single-source model contained in the dictionary) and deployed out to the system via automated processes and generators, as one would expect of a model-driven development environment. The visible metadata for the community of consumers should appear as a strongly version-aware and variation-aware Enterprise metadata registry.

Several functionality and technology tools are necessary for SOA life cycle support. Importers to load existing metadata are required. Management tools that can assimilate metadata into an integrated data model and deal with redundancy and duplication are critical. Also needed are tools for design and development, impact analysis, change management, fine-grained version control and release management. A model-driven architecture, central repository and a collaborative development across multiple teams are also very important. A technically sound, robust metadata evolution management strategy is the enabling differentiator for any modern SOA. Without such a radical new approach to managing metadata in a SOA, it is unlikely that the long term promise of flexibility and cost savings will be realized.

The use of Web Services presents many unique security challenges. The typical transport protocol is HTTP(S) which is open on most firewalls. Both users and services are distributed – often times over the Internet. Abstracting legacy systems as Web Services can introduce multiple underlying messaging protocols and security mechanisms, such as data exchange via XML within a SOAP envelope, which introduces new vulnerabilities. Satisfying the complex security requirements of a web-based SOA will require a new set of security standards. We already have a number of tools at our disposal. SAML, Security Assertion Markup Language, is an XML framework for exchanging authentication and authorization information. WS-Federation is a Web Services Federation Language specification that defines mechanisms to allow different security realms to federate by allowing and brokering trust of identities, attributes, authentication between participating web services. WS-Security, WS-Secure Conversations, WS-Security Policy, WS-Trust are enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication.

They provide mechanisms for establishing and sharing security contexts, and deriving session keys from security contexts, can indicate the policy assertions which apply to WS-Security, and define extensions to request/issue security tokens & manage trust relationships. XML-Encryption specifies a process for encrypting data and representing the result in XML. XML-Signature specifies XML digital signature processing rules and syntax. These security standards are at varying degrees of completion and commercialization; in some cases competing standards have been proposed. There are also proprietary solutions for such security problems regarding workflows to provision and terminate users, Single Sign-on and synchronization of disparate directories. The lack of maturity of these security mechanisms and the use of proprietary solutions requires addressing by the coalition technical community.

Even less mature than these security mechanisms is the process of certification and accreditation of SOA for use on Defense networks. Certification and accreditation authorities are accustomed to dealing with integrated systems. While certification of a single software module may appear on its face to be quite straightforward, the combinatorics associated with the ad hoc orchestration of multiple modules will require an entirely new approach. This will prove challenging enough in the setting of a single nation. If multiple vendors provide individual components but the aggregate fails to function as expected, who will be held responsible? In the multi-national settings, the challenges are multiplied. How can we be assured a security vulnerability will not arise when individual components, each secure by itself, are composed in an unanticipated way? What about strictures against foreign code?

Despite the seeming lack of maturity of several key SOA components, there is a great deal of SOA activity going on in the private sector and within our respective Defense organizations which we can and should leverage.[20] There are, however, several areas that require attention and focus for coalition interoperability in a SOA from the operational and technical communities. Of critical importance from the operational community are the identification, scope and description of Defense "business practices" that need to be implemented in a SOA. Knowledge of these key warfighter requirements is critical in directing the efforts of the technical community. Without this guidance, we run the risk of developing technology for technology's sake.

There are several areas that require engagement by the technical community. The development of a technically sound, robust and interoperable metadata and evolution management strategy is critical for the successful implementation and sustainment of a SOA environment. Also important is the definition and standardization of a common and interoperable suite of web services. SOA messages need to be implemented using a technology that supports the scalability requirements of services, particularly in low-bandwidth, tactical environments. Efficient XML may be such an enabler. Like bandwidth, SOA "chattiness" must be carefully controlled in the tactical environment. Tactical networks have high latency and high error rates relative to the Enterprise core networks for which SOA has been developed in the business world. High turn counts result in unsatisfactory application performance. A tactical SOA for the coalition must necessarily be coarse-grained, having limited depth to the service composition and geographic distribution.[21]

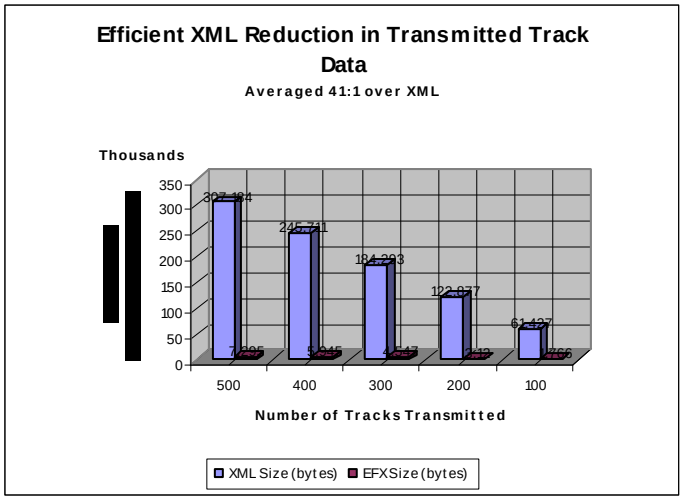

Table 1: Efficient XML Reduction

A proper SOA environment for the coalition must include discovery and directory Services shared between nations; this includes robust Directory Services, not just "White Pages." Also required, and not trivial to implement, is a UDDI registry for National and Coalition networks and the need to map out Content Providers and expected products. Service Orchestration and Mediation requires standardization of work flows and business practices, which will require interaction with the operational community. As noted above, virtually all aspects of SOA Security need to be addressed.

To support distributed operations over ship-ship networks, several distributed services have been demonstrated in Trident Warrior and in operational deployments.[22] Domain Name Service (DNS), email, text chat, COP, and JPEG 2000 Interactive Protocol imagery transfer services have all been successfully configured and exercised disconnected from any NOC. Distributed DNS makes use of conditional forwarding. Conditional forwarding implies that a set of forwarders can be listed separately in each zone. Each specific zone on a ship is configured to forward queries to their respective Network Operation Center DNS server first. If the NOC is unavailable, then the next forwarder becomes the actual ship's DNS server that hosts the zone. Ship's DNS servers are not required to hold any other zone, but their own.

The Microsoft Exchange servers on the platforms with ship-ship network connectivity are configured to use connectors and DNS mail exchanger (MX) records to find the Simple Mail Transfer Protocol (SMTP) e-mail server of the intended recipient, and therefore letting the network find the best path to that server. The standard main connector to the NOC is left intact. The added connector will include all the remote domains with lower costs than the original NOC connector. The added connector will point to DNS for resolution. Since each node advertises its local SMTP e-mail server in DNS to the rest of the network, ship-to-ship e-mails end up being routed directly over any available path.

Sametime Chat and Persistent Chat on CENTRIXS has been demonstrated in NOC-centric, fully distributed and partially distributed architectures in Trident Warrior experimentation venues. A partially distributed architecture, with Sametime servers located on Force-level and Command ships was found to be the most suitable compromise between performance and maintainability. Ships without SATCOM reachback can point their clients to the Sametime server located aboard the big deck and continue operations without NOC reachback.

Distributed COP services have also been demonstrated with multiple applications: GCCS-M, C2PC and the C2PC Controlled Gateway. In the event of a loss of reachback to shore command centers, where the current CENTRIXS COP is maintained, units can point their servers and gateways to local COP sources as designated by the on-scene commander. Similarly, JPEG 2000 clients can be pointed to JPEG 2000 servers within the Strike or Task Group to exchange imagery ship-ship, without the need for shore reachback.

Distributed SOA must be able to extend these basic services to all applications and include the ability to situate the appropriate information and knowledge on the appropriate platforms prior to any loss of reachback. Not all data needs to be replicated out to all ships all the time.

A "BETA TEST" FOR EFFECTIVE INTERNATIONAL LABORATORY COORDINATION

As the United States and its coalition partners continue to evolve to a SOA approach and work together to solve common networking challenges, the importance of international laboratory-to-laboratory work will gain increasing importance. We have found that working within the AUSCANNZUKUS/TTCP nations effectively pools the expertise of a diverse and talented group of scientists and engineers. We anticipate

that the gains made within this group of close allies will then deploy to the larger Global Maritime Partnership, and ensure that navies from around the globe can interoperate at sea.

The Technical Cooperation Program Maritime Systems working group, has fielded two action groups – AG-1 Maritime Network Centric Warfare and AG-6 FORCEnet Implications for Coalitions – that have generated a body of work including data that quantifies the enhanced ability of a fully-networked international naval force to achieve enhanced effectiveness over a wide spectrum of missions ranging from humanitarian assistance, to fighting a local insurgency, to force-on-force conflict at sea. The TTCP Command, Control, Communications, and Intelligence (C3I) working group is composed of technical panels and action group that are addressing the full spectrum of network-centric technical challenges from a Joint, Combined, and Coalition perspective. Within the five navies, the AUSCANNZUKUS organization provides a venue to put interoperability to the test in maritime operations. AUSCANNZUKUS has been extremely active in the series of Trident Warrior sea trials. It is here that we expect to first demonstrate the advantages of SOA for the coalition environment.

While a full description of these working group's results is outside the scope of this paper, the results have been briefed at a wide array of conferences and symposia: from the U.S.-sponsored International Command and Control Research and Technology Symposia series, to the United Kingdom-sponsored Royal United Services Institute Symposia series, to the Royal Australian Navy Sea Power Conference biannual conference and the Royal Australian Navy King Hall Naval History biannual conference.[23]

The development and design processes engaged in by the TTCP and AUSCANNZUKUS that will be employed to enable the SOA vision for the maritime coalition begin in the laboratory. We have offered three examples, TTCP MAR AG-1/AG-6, TTCP C3I and AUSCANNZUKUS participation in Trident Warrior, of a methodology that enables nations – at the laboratory level – to begin the design process to ensure that their navies are able to effectively network at sea. These models of technical corporation are readily exportable to other groups of nations and navies. The prospects for demonstrating the manifest benefits of robust coalition interoperability through ongoing, focused analysis appear to be excellent. The comments of one U.S. Navy admiral, Admiral James Stavridis, currently the Commander of U.S. European Command and NATO Supreme Allied Commander Europe, that, "We will win – or lose – the next series of wars in our nation's laboratories,"[24] can be extrapolated to the laboratories of *all* nations seeking to work together to deal with the maritime threat to the global commons.

---

[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] Speech by Admiral Michael Mullen at the Australian Defence College, accessed at: http://www.jcs.mil/chairman/speeches/080222remarks_AustralianWarCollege.html.
[3] *Rhumb Lines*, September 3, 2008, accessed at: www.navy.mil. *Rhumb Lines* is carried on the official website of the U.S. Navy Chief of Information (CHINFO) and contains weekly information of importance to the U.S. Navy.
[4] Admiral Gary Roughead, remarks as delivered at the Surface Navy Association Symposium Banquet, January 14, 2010, Chrystal City, VA. Accessed at Internet http://www.navy.mil/navydata/people/cno/Roughead/Speech/100115%20CNO%20remarks%20at%20SNA%20Symposium.doc.
[5] 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 www.dodccrp.org.
[6] *A Cooperative Strategy for 21st Century Seapower* (Washington, D.C.: Department of the Navy, 2007). Accessed on the Department of the Navy website at www.navy.mil.
[7] George Galdorisi and Darren Sutton, "Achieving the Global Maritime Partnership: Operational Needs and Tactical Realities," *RUSI Defence Systems*, 15 June 2007, p.69. See also, George Galdorisi and Stephanie Hszieh, "Speaking the Same Language," *United States Naval Institute Proceedings*, March 2008.
[8] Admiral R. Natter, Interview, *Combat Systems Clips*, Summer 2002.
[9] 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.

[10] Vice Admiral Russ Shalders, Royal Australian Navy, Chief of Navy, remarks at the 10th Western Pacific Naval Symposium, October 29 - November 2, 2006, Honolulu, Hawaii.
[11] Royal Navy's Chief of Naval Staff and First Sea Lord Admiral Sir Jonathon Band, remarks at the Royal United Services Institute Future Maritime Operations Conference, November 22-23, 2006, London.
[12] CMDR Gurupreet Khurana, Institute for Defence Studies and Analyses (IDSA), *Defence News* 6 JAN 07. See also, Donald Berlin, "India and the Indian Ocean," *Naval War College Review*, Spring 2006, pp. 58-89 for a more expansive treatment regarding India's maritime interests.
[13] U.S. 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.
[14] P. Mitchell, "Small Navies and Network-centric Warfare: Is There a Role?" *Naval War College Review*, Spring 2003, pp. 83-99.
[15] *Military Transformation: A Strategic Approach* (Washington, D.C.: Department of Defense, 2003), pp. 1-36, accessed at: Internet www.oft.osd.mil. This publication is the capstone publication of the Office of Force Transformation, U.S. Department of Defense.
[16] OASIS Reference Architecture for Service Oriented Architecture Version 1.0, Public Review Draft 1, April 23, 2008; T. Erl, *Service Oriented Architecture: Concepts, Technology, and Design*, Prentice-Hall, 2005.
[17] D. Ortega, E. Uzcategui, and M. Guevera, "Enterprise Architecture and Web Services," *Proceedings of the 4th International Conference on Internet and Web Applications and Services*, ICIW09, May 2009, pp. 24-29.
[18] The Combined Enterprise Regional Information Exchange System (CENTRIXS) networks provide support for a number of coalition enclaves. Nations that participate include Australia, Canada, New Zealand, United Kingdom, Japan, South Korea, Germany, France, Italy, Spain, the Netherlands, and others, in addition to the U.S., which provides centralized management.
[19] J. Gabriel, "Be sure to manage your metadata," February 18, 2005, accessed at www.looselycoupled.com/opinions/2005/
[20] T. Sterkel, "Interoperability on the Pointy End of the GIG: Web Services for Tactical Battlespace NETOPS," *Proceedings of Military Communications Conference (MILCOM) 2005*, pp. 2917-2923; D. Kidston and I. Labbe, "A Service Oriented Framework for Policy-Based Management of Maritime Mobile Networks," *Proceedings of Military Communications Conference (MILCOM) 2006*, pp. 1-7.
[21] For more on SOA granularity, see J. Kral and M. Zemlicka, "Coarse-Grained Commands SOA," *Proceedings of the 3rd International Conference on Digital Communications*, 2008, pp. 76-81.
[22] J. Chan, S. Lapic, and M. Jordan and R. Sibbald, "Naval Tactical Networking for Coalition Forces," *Proceedings of Military Communications Conference (MILCOM) 2008.*
[23] See, for example, George Galdorisi, Stephanie Hszieh, and Darren Sutton, "Naval Cooperation for the Future Force," *Headmark: Journal of the Australian Naval Institute* 134 (2009): 45-53; George Galdorisi, Stephanie Hszieh and Terry McKearney, "Networking the Global Maritime Partnership," *Proceedings of the 13th International Command and Control Research and Technology Symposium*, Bellevue, Washington, June 2008; George Galdorisi and Darren Sutton, "A Technical Approach to Coalition Interoperability," *Proceedings of the 11th International Command and Control Research and Technology Symposium*, Cambridge, United Kingdom, September 2006; George Galdorisi and Darren Sutton, "Coalition Interoperability: How Much Is Enough and How to Quantify It," *Proceedings of the 2006 Royal United Services Institute C4ISTAR Conference*; *Sea Power: Challenges Old and New* (Sydney, Australia: Halstead Press, 2007) – George Galdorisi and Darren Sutton, *Coalition Interoperability: How Much is Enough and How to Quantify It*; and Don Endicott, George Galdorisi and Stephanie Hszieh, "Communications for the Global Maritime Partnership," *Proceedings of the Royal Australian Navy Sea Power Centre 2007 King-Hall Naval History Conference*.
[24] Admiral James Stavridis, "Deconstructing War," *United States Naval Institute Proceedings*, December 2005, pp. 42-45.