12TH ICCRTS
"Adapting C2 to the 21st Century"
Final Paper   4-2-07

Title of Paper: **"Integrating Military and Civilian C2" -- (Student Paper)**

Topics: Military and Civilian C2
                                       C2 Technologies and Systems

Name of Author: John A. Sturm
Point of Contact: same
University: PhD Candidate - Indiana State University
Name of Organization: NuParadigm Government Systems, Inc.
Complete Address: 12977 North Forty Drive, Suite 200
                                       St. Louis, MO 63141
Telephone: (314) 401-6850
E-mail Address: jsturm@nuparadigm.com

Abstract

NuParadigm recently received a Navy SPAWAR contract for "*Secure Legacy Application Integration with NCES*" (SLAIN). As a result, we are developing prototype system models to integrate civilian and military Command & Control (C2) across a Service Oriented Architecture (SOA) network using the internet protocol (IP). Web Services and standards provide the promise of reliable, secure interoperability among disparate applications and technologies. However, integration of Command across Civilian and Military structures is as much about creating interoperability among cultures. Atkinson & Moffat (2005, pg 161) describe the nature of Command as "a function of trusts, fidelity and agility", whereas, Control is a function of rules, time and bandwidth".

Civilian Commands all work under and among state & local governments who have worked out complex trust relationships to get things done such as new roads, disaster relief, criminal pursuit across jurisdictions, etc. In this paper we will explore some of the hopes, challenges and examples of using an SOA environment to extend civilian relationships with the military. The emerging SOA approach is surprisingly adaptive and capable of supporting both communication bandwidth as well as adapting the message between sender and receiver to be understood in the local context (culture) of each other.

Introduction

To begin, it is important to observe the role of communication networks and particularly the internet in supporting the creation, self-organization and maintenance of Command & Control structures. Atkinson & Moffat (2005, pg 161) also stated, "Organizations have a choice: if they wish to exert control over the battlespace, as opposed to command, they need to provide the rules and quantitative technological bandwidth necessary. If they wish to command, as opposed to control the battlespace, they need to provide the more qualitative trusts of fidelity and agility in their people. Taken one step further, command is more associated with culture, and control with technology; and it is the effect of one upon the other that is key." The task of integrating

1

Civilian and Military Commands is as much about respecting and communicating within the context of each participant's culture as it is about having the bandwidth and network access to assign and manage the rules of a battle.

   One of the most exciting areas of synergy between the requirements for C2 and SOA internet technology is the ability to rapidly standup, support and link evolving networks across all types of organizations and cultures. Just as social networks and roads supported the expansion and maintenance of Roman rule (C2) over disparate regions for many centuries, the internet provides the virtual roads and social gathering points to support C2 across the world today. In particular, the evolution of "Random Networks" to become "Small World Networks" and then "Self-Organized Scale-Free Networks" are critical to C2 across military and civilian organizations.

   The internet is surprisingly capable in supporting both types of communication exchange; however, discovering, adapting (i.e. transforming/mediating message contents) takes additional time to understand & communicate the situational awareness (and cultural awareness) of our partners as well as foes.

Network Evolution to Support C2 Environments

   As mentioned, the evolution of "Random Networks" to become "Small World Networks" and then "Self-Organized Scale-Free Networks" are critical to C2 across military and civilian organizations. Random Networks usually form thru chance meetings among people that discover common interests, such as local residents that live near a harbor in the US. Providing a small amount of communications support to random networks (possibly through email access/links) can cause them to have high situational awareness of their particular area. Stephen Flynn, former Navy Commander and author of *America: The Vulnerable* (2006) points out that small groups of individuals in neighborhoods near valuable resources such as shipping ports can have a valuable contribution to Port Security through situational awareness. Terrorists must plan and conduct surveillance on a target for a considerable period of time before attacking the target and they are susceptible to discovery during this time by an informed group of observers.

   Building on this example of Self-Organization of neighbors to assist with Port Security, C2 Operations Centers such as the Joint Harbor Operations Centers (JHOC) would benefit from knowledge gained by a large number of these neighborhood cells. "Self-Organized Scale-Free Networks" consist of a few nodes that have lots of links to many cells and act like "hubs". In fact Atkinson & Moffat (2005, pg 101, 111) "anticipate that Internet or Web-links between individuals will tend to lead to (Self-Organizing) Scale Free Networks." Hubs tend "to become more formal if they are to manage their connections to concentrate and dispense their power effectively." The C2 system becomes "a network of formally defined, locally clustered cells with longer range links (shortcuts over the internet) between them: a Small World" network. In summary, "both Informal Networks and the Formal Organizational Structure are required to work well together in order to deliver the Agile Organization" for effective C2. Ultimately, the arrangement of social relationships and networks should evolve to become Complex Adaptive Systems (CAS) that are "able to dynamically co-evolve and change within, or as part of, a changing (C2) environment" (Atkinson & Moffat, 2005 pg 42).

   As illustrated in the diagram below from the Trident Warrior'07 (TW07) Experiment, the "SLAIN Network" acted as a "Self-Organized Scale-Free Network" to support the C2 System for the Maritime Domain Awareness Community of Interest (COI). The "SLAIN Network"

consisted of a few nodes that have lots of links to many cells and act like "hubs". SLAIN linked the state & local Emergency Operation Centers (EOCs for Virginia Beach & Virginia (Vigilys), and Seattle & Washington (MyState)) with the Navy's command and control systems, shown as the TRITON COP and the MIDAS**tm**, Maritime Integrated Domain Awareness Solution:
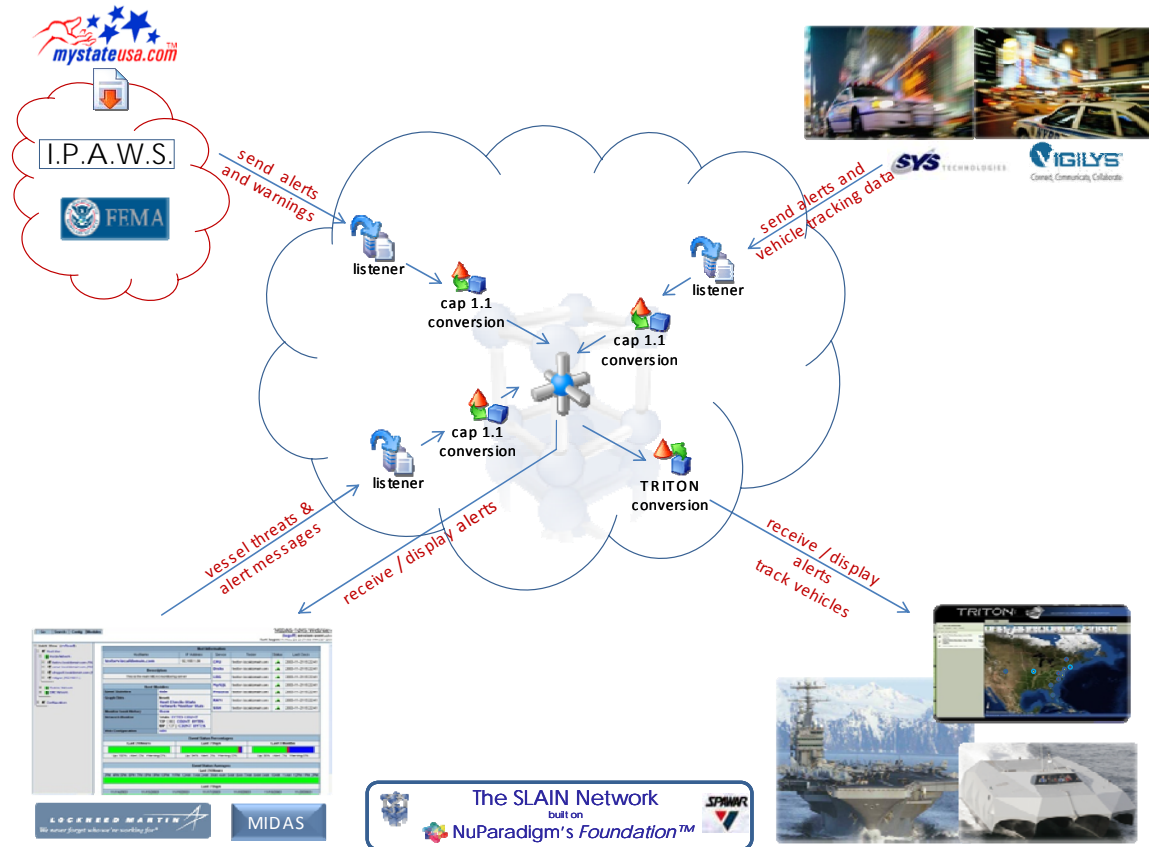
Figure One – High Level view of the Maritime Domain Awareness (MDA) COI experiment in the Trident Warrior'07 Experiment.

Each EOC would properly be considered a "Small Network" with many links across their local community areas and also be representative of the Integrated Public Alert & Warning System (IPAWS) network that is under design. It would not be inappropriate to speculate that neighbors around the Virginia Beach and Seattle harbor areas would probably contact their EOC through the local police if they were suspicious about strangers in their neighborhood observing ship traffic at all hours. Though TW07 was only an experiment, it is likely that we did extend the C2 System down to individual citizens by treating the EOCs as "Small World" networks. In fact one of the terrorist alerts from local authorities in Seattle (shown later in the data message traffic) served to "kick-off" one of the day-long experiment scenarios in TW07.

As stated earlier, "both Informal Networks and the Formal Organizational Structure are required to work well together in order to deliver the Agile Organization" for effective C2. Ultimately, the arrangement of social relationships and networks should evolve to become Complex Adaptive Systems (CAS) that are "able to dynamically co-evolve and change within, or as part of, a changing (C2) environment" (Atkinson & Moffat, 2005 pg 42). Thus SLAIN enables the adhoc "shortcuts" and linkages to create an Agile Organization. If the C2 Mission Plan

changed to hurricane relief & assistance, then the EOCs for the Gulf Coast states would be immediately added and linked with the Navy's C2 Systems.

SLAIN also proved valuable in translating the context of one C2 hub into the context of the other C2 hub and vice versa. In other words, the Navy was able to see the actions & reactions of state/local response teams by watching emergency vehicle movements ("tracks") on shore, while the state/local EOC teams could also see the Navy's ship movements/tracks. Chat Messaging also served as a key socializing and C2 environment during TW07 to bridge the differences between the military and civilian cultures. After TW07, during the "Hotwash" discussion of what happened, the local/first responders described what they saw in their version of the TRITON Common Operational Picture (COP) and then the Navy Commanders described their perspective. Chat was a valuable method for the two groups to stay "synchronized" in order to understand vehicle movements and responses to the scenario being followed. In the paper, *An Architecture and Model For Multi-Level Secure Chat Services* (Sturm, 2007), Sturm described how multi-level chat services could be incorporated into confidential C2 situations to provide clarification and secure discussion for understanding across different individuals & groups.

In addition, it was discussed that SOA technology could have extended this cross-cultural understanding by tagging the embedded data in the message traffic and making it visible on the COP Display. As a simple example, we added the universally understood icon of a "fire truck" as one of the vehicles to distinguish it from a police cruiser during the exercise. Before getting into the details of the TW07 data message handling, routing, mediation, etc. it is valuable to step back and review the state of SOA technology and the technical issues we all face.

SOA Technology Challenges and Issues

As networks evolve, XML messages bear the burden of larger overhead data requirements, especially for the message state recognition that is necessary for conveying data/information context and maintaining security. This overhead includes:
- Transmission and receipt data
- Message validation data
- Tagging of meta-data content and Keywords
- Authentication and authorization data
- Activity monitoring and auditing data
- Encryption & associated De-encryption processing and related Key Management

These overhead burdens become rapidly amplified as the number of concurrent instances grows to even moderate levels. Service areas that are affected by this model include:
- Performance – memory requirements grow exponentially, placing drag on the system.
- Scalability – growth in this model imposes costly infrastructure requirements.
- Resiliency – offering seamless service plus audit reporting imposes greater restrictions on the granularity of security roles and data definitions supported due to the associated cost in processing and storage requirements.
- Federation – all overhead issues are magnified when the requirements for Policy management and communication over disparate systems and technologies are introduced. Policy must in accord with the Memo of Understanding (MOU) of how organizations wish to cooperate and network.

- Situational Awareness of Content & Context – The ability to embrace and instantiate appropriate knowledge into Policy & Rules that have situational (Cultural) awareness is an essential technology partner to Combatant Commanders (COCOMS).
- Content-Aware Object Routing – Monitoring and providing content & context-based distribution/routing of information based on Enterprise-wide Policy management is critical to promote rapid understanding. In the TW07 exercise it was critical to expedite a message about suspicious activity in the Seattle area that exposed a threat to Virginia Beach.

Solution Approach & Direction

The SLAIN secure object framework introduces a next-generation solution by offering security, system continuity, and reliability in a unique way: The framework routes objects through a Secure Context Object Routing Engine (SCORE) rather than routing messages through traditional transport channels. Object state data is maintained within the service object itself instead of as system overhead associated with processing the messages related to a service. It is critical to understand that IP networks are non-deterministic and subject to packet losses at any time. Realized benefits include:

- Reliability – achieved through context specific object message constructs. Just as the DOD promotes "defense-in-depth" for network security, it is equally important to promote "reliability-in-depth" by adding "application layer" technology for reliable data transfer. Message objects can be tracked for confirmation of delivery just as TCP/IP traffic is acknowledged and resent if necessary at the "transport layer". Router congestion can disrupt TCP/IP's ability to guarantee delivery, so an application layer delivery confirmation process is essential for C2 communications.
- Security - validation, authentication, and authorization are directly managed within the object
- Object monitoring – object activity is directly captured within the object as it goes through the service cycle for audit and reporting purposes
- Efficient handling - unnecessary repetitive object handling and parsing is eliminated since the full context of the data object is maintained in one place

As a result, system performance is positively impacted as transaction overhead is dramatically reduced. Realized service improvements include:

- Performance - Service management overhead grows in direct proportion to volume rather than exponentially.
- Scalability - SCORE hubs are easily distributed. The inherent independence of service objects due to internal state maintenance makes this possible.
- Effectiveness – Finer security and data granularity with detailed activity tracking are readily achieved since the objects are not constrained in their ability to store the information required to achieve this.
- Synchronization - The independence of objects also allows for ease of implementation in asynchronous access models such as publish & subscribe.
- Resiliency - Object routing also increases attack prevention capability since all objects are easily validated or rejected within the secure object framework.
- Federation - SCORE hubs are able to retain necessary context translation definitions and transparently facilitate object transfer between domains.

- Object Routing - Most importantly for network evolution to support the development of "Small World Networks" and thus the concept of "Self-Organizing Networks for efficient C2", Object routing provides necessary "shortcuts" to facilitate the growth & maintenance of relationships among remote and culturally diverse partners. The internet enables global access to distant data, while the "intelligent" embedded tagging within objects permits cultural awareness about the semantics and meaning of the data contained.

Example for Presentation: Integrated Public Alert & Warning System (IPAWS)

In addition to the "SLAIN" Navy SPAWAR research effort, NuParadigm is working on development of the IPAWS (Integrated Public Alert & Warning System) functionality for the thirteen-state hurricane risk area of the US. The IPAWS model shown below was part of the Maritime Domain Awareness (MDA) COI experiment in the Trident Warrior'07 Exercise in March, 2007 (see Figure One).
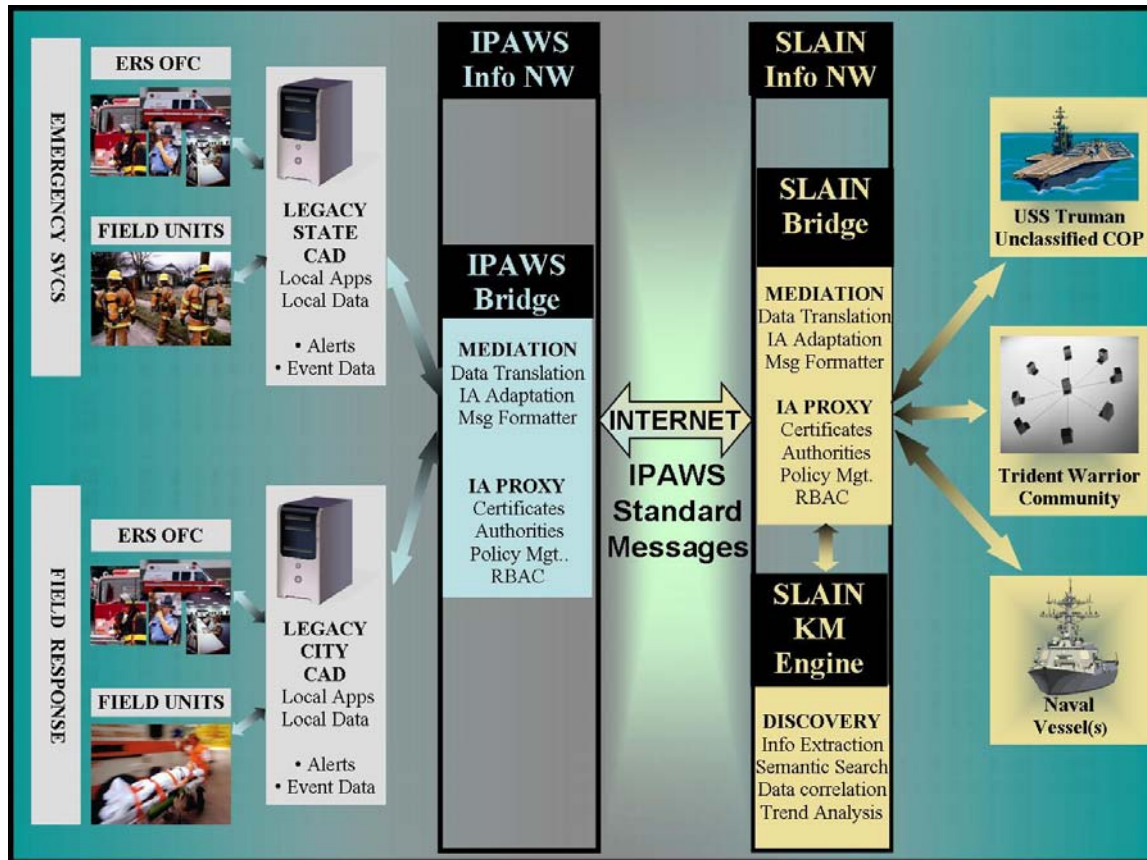
Figure Two – Part of the Maritime Domain Awareness (MDA) COI experiment in the Trident Warrior'07 Exercise using the IPAWS (Integrated Public Alert & Warning System) functionality for the thirteen-state hurricane risk area of the US.

The legacy state Computer-Aided Dispatch (CAD) and the legacy city Computer-Aided Dispatch (CAD) systems shown in Figure One are examples of potential "Small World Networks" which were linked through the SLAIN technology of Object Routing to form the Military-Civilian Command Authority. The overall C2 network then "evolved" to become a "Self-Organized Scale-Free Network".
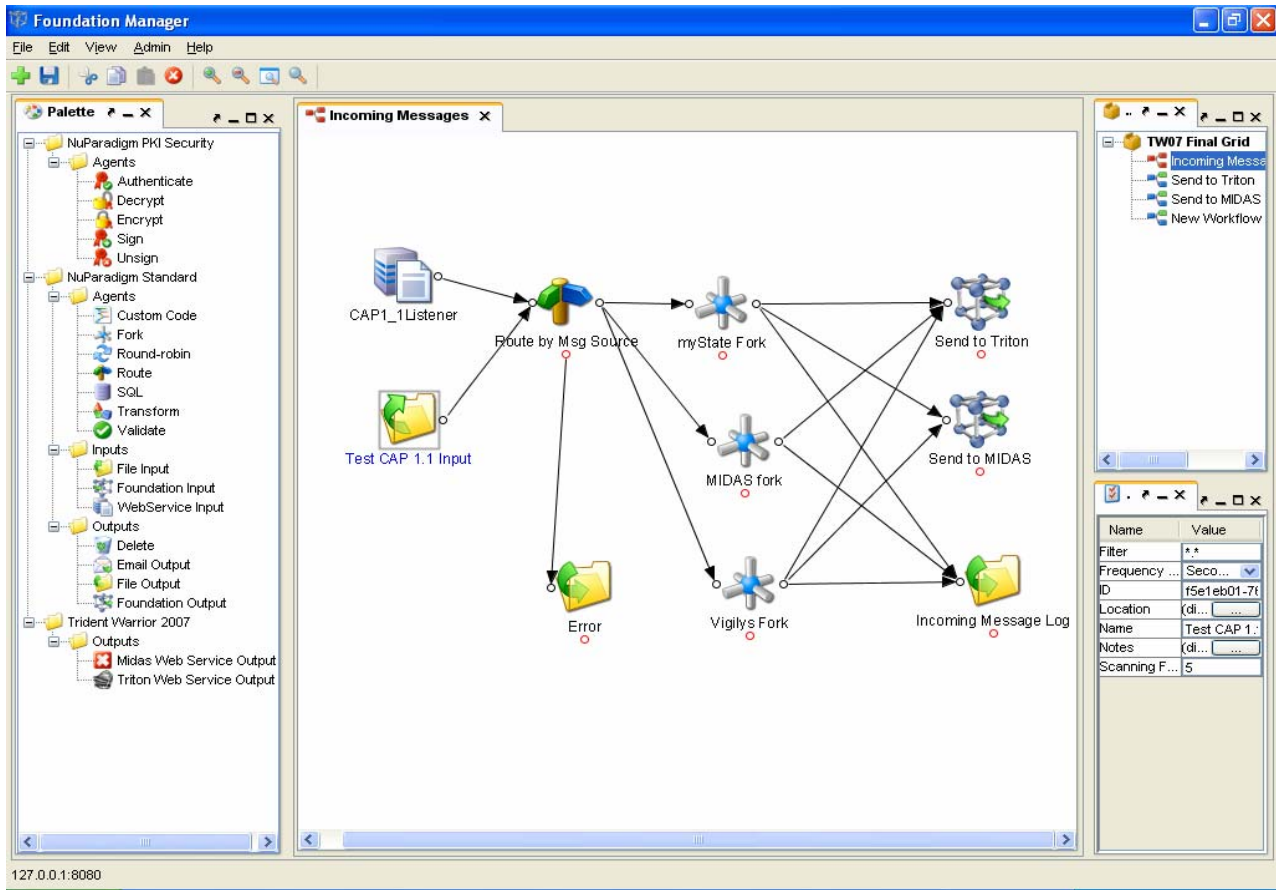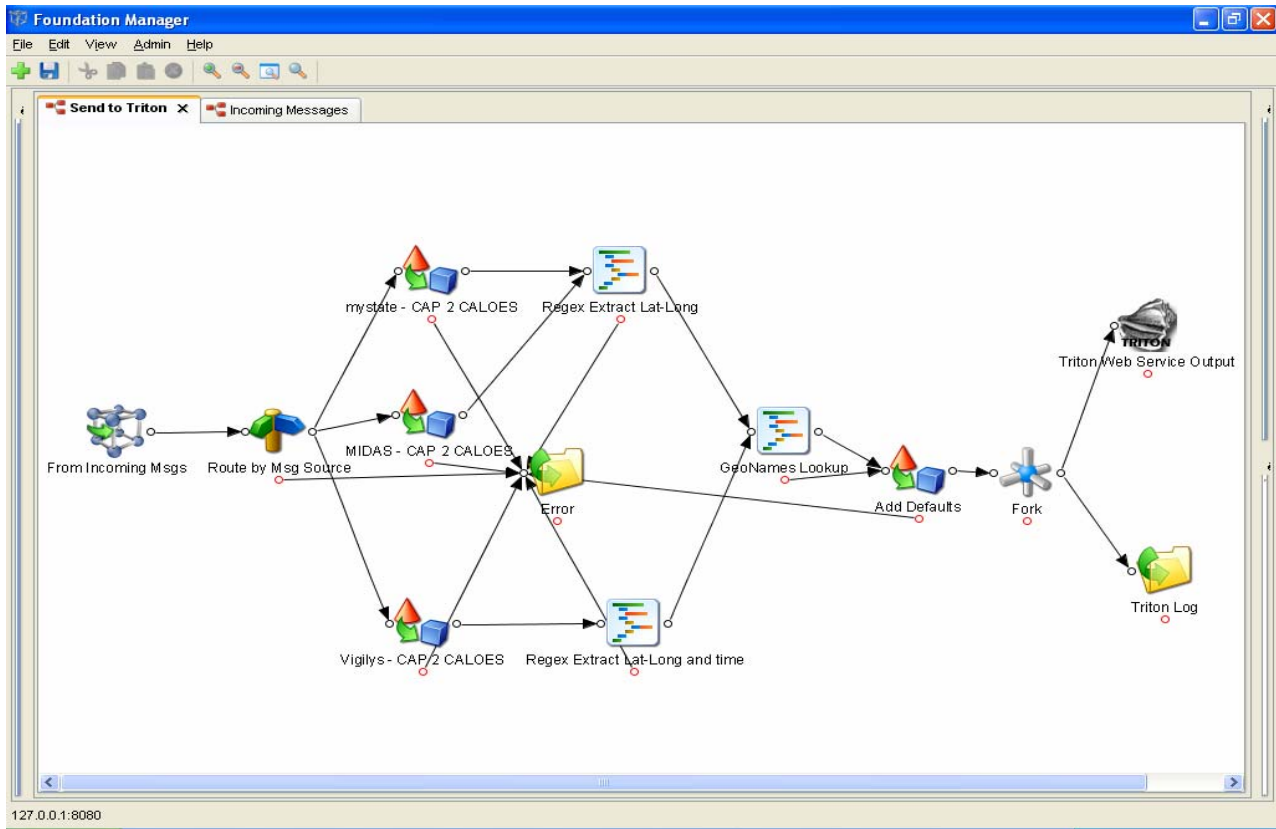
Figure Three – View of the IPAWS & SLAIN object routing environment for linking multiple data sources into the Maritime Domain Awareness (MDA) COI for TW07

Figure Three above illustrates the use of intelligent agents to capture, route, convert and mediate data contained in the message objects to create the infrastructure for the IPAWS and MDA COI. In addition to intelligently routing the objects based on specific content, the concept enables end-to-end conversion and mediation as necessary to convey a common understanding about events to the C2 Commanders.

In the next diagram below, Figure Four, we are extracting and converting geospatial coordinates for vehicle movement in order to provide a common format across the Common Operational Pictures for the various C2 Systems. Then in Figure Five, the various C2 Systems are able to see a Common Operational Display (COP) of the alerts and the response by state/local vehicles.

Figure Six is a sample of the data objects that were exchanged among the MDA COI participants. The objects actually tell a story about a fictitious incident that was staged and then show the emergency response and vehicle movements ("tracks"). Any data contained within the messages could be extracted for analysis and refinement of the picture displayed. In fact, the C2 Commanders suggested afterwards that additional on-line tagging in the display would be beneficial for understanding the situation being acted out in the scenario.

Figure Four – View of the IPAWS & SLAIN object routing environment for extraction, conversion and transmission of geospatial coordinates across Military & Civilian C2
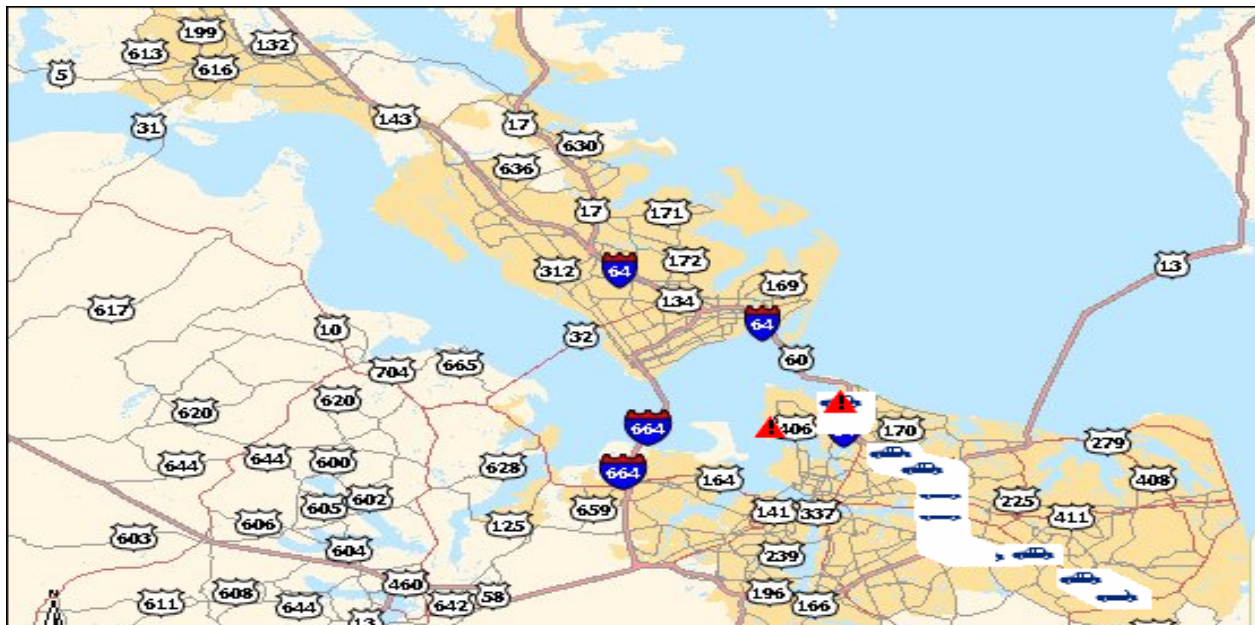
Figure Five – High Level view of TW07 MDA COI Common Operational Display for tracking alerts and state/local emergency responders.

OBJECTID	LOCATION	LATITUDE	LONGITUDE	CITY	ZIP_CODE	OWNER	SUBJECT	MODIFIED	TIME_	INCIDENT_NAME	INCIDENT_SITE_NAME
2	36.94503007 929109,- 76.27229332 923889 10	36.94503007	-76.27229332	Norfolk	23503	inbound@vig ilys.com	Incident	Mar 16 2007 10:04AM	2007-03-16T09:04:56-05:00	GROUP GATHERING IN PKG LOT; 45 PEOPLE TW070031	California at [36.9450300 7929109,-76.27229332 92388
3	36.94503007 929109,- 76.27229332 923889 10	36.94503007	-76.27229332	Norfolk	23503	inbound@vig ilys.com	Incident	Mar 16 2007 10:04AM	2007-03-16T09:04:58-05:00	GROUP GATHERING IN PKG LOT; 45 PEOPLE TW070031	California at [36.9450300 7929109,-76.27229332 92388
4	36.94503007 929109,- 76.27229332 923889 10	36.94503007	-76.27229332	Norfolk	23503	inbound@vig ilys.com	Incident	Mar 16 2007 10:05AM	2007-03-16T09:05:00-05:00	GROUP GATHERING IN PKG LOT; 45 PEOPLE TW070031	California at [36.9450300 7929109,-76.27229332 92388
5	36.9083989,- 76.1805081 10	36.9083989	-76.1805081	Virginia Beach	23455	inbound@vig ilys.com	Incident	Mar 16 2007 10:05AM	2007-03-16T09:05:01-05:00	SUSP ACTIVITY; LITTLE CREEK INLET RAIL DEPOT; DIVE	California at [36.9083989,-76.1805081]
6	36.9083989,- 76.1805081 10	36.9083989	-76.1805081	Virginia Beach	23455	inbound@vig ilys.com	Incident	Mar 16 2007 10:05AM	2007-03-16T09:05:03-05:00	SUSP ACTIVITY; LITTLE CREEK INLET RAIL DEPOT; DIVE	California at [36.9083989,-76.1805081]
7	36.94450166 666667,- 76.27049 10	36.94450166 666667	-76.27049	Norfolk	23503	inbound@vig ilys.com	Vehicle	Mar 16 2007 10:05AM	2007-03-16T09:05:06-05:00	C11	California at [36.9445016 6666667,-76.27049]
8	36.90997666 6666665,- 76.179595 10	36.90997666	-76.179595	Virginia Beach	23455	inbound@vig ilys.com	Vehicle	Mar 16 2007 10:05AM	2007-03-16T09:05:08-05:00	C1	California at [36.9099766 66666665,-76.179595]
9	36.90925166 666667,- 76.17995833 333333 10	36.90925166	-76.17995833	Virginia Beach	23455	inbound@vig ilys.com	Vehicle	Mar 16 2007 10:05AM	2007-03-16T09:05:09-05:00	E11	California at [36.9092516 6666667,-76.17995833 33333
10	36.910555,- 76.17938166 666667 10	36.910555	-76.17938166	Virginia Beach	23455	inbound@vig ilys.com	Vehicle	Mar 16 2007 10:05AM	2007-03-16T09:05:16-05:00	C1	California at [36.910555,-76.17938166 666667]
11	36.9083989,- 76.1805081 10	36.9083989	-76.1805081	Virginia Beach	23455	inbound@vig ilys.com	Incident	Mar 16 2007 10:05AM	2007-03-16T09:05:16-05:00	SUSP ACTIVITY; LITTLE CREEK INLET RAIL DEPOT; DIVE	California at [36.9083989,-76.1805081]
12	36.910555,- 76.17938166 666667 10	36.910555	-76.17938166	Virginia Beach	23455	inbound@vig ilys.com	Vehicle	Mar 16 2007 10:05AM	2007-03-16T09:05:19-05:00	C1	California at [36.910555,-76.17938166 666667]
13	36.908815,- 76.18016166 666666 10	36.908815	-76.18016166	Virginia Beach	23455	inbound@vig ilys.com	Vehicle	Mar 16 2007 10:05AM	2007-03-16T09:05:20-05:00	E1	California at [36.908815,-76.18016166 666666]
14	36.91110000 0000005,- 76.17919833 333333 10	36.9111	-76.17919833	Virginia Beach	23455	inbound@vig ilys.com	Vehicle	Mar 16 2007 10:05AM	2007-03-16T09:05:22-05:00	C1	California at [36.9111000 00000005,-76.17919833 3333
15	36.90933666 666667,- 76.17993 10	36.90933666	-76.17993	Virginia Beach	23455	inbound@vig ilys.com	Vehicle	Mar 16 2007 10:05AM	2007-03-16T09:05:24-05:00	E1	California at [36.9093366 6666667,-76.17993]
16	36.9083989,- 76.1805081 10	36.9083989	-76.1805081	Virginia Beach	23455	inbound@vig ilys.com	Incident	Mar 16 2007 10:05AM	2007-03-16T09:05:26-05:00	SUSP ACTIVITY; LITTLE CREEK INLET RAIL DEPOT; DIVE	California at [36.9083989,-76.1805081]
17	36.90933666 666667,- 76.17993 10	36.90933666	-76.17993	Virginia Beach	23455	inbound@vig ilys.com	Vehicle	Mar 16 2007 10:05AM	2007-03-16T09:05:28-05:00	E1	California at [36.9093366 6666667,-76.17993]

Figure Six – Data Sample showing messaging incident alerts and vehicle movements ("tracks") for the TW07 MDA COI Common Operational Display.

Summary

The SOA network environment can act as a strong catalyst for development of effective and agile C2 structures. The vision of an effective C2 system becomes a network of formally defined, locally clustered cells with longer range links (shortcuts over the internet) between them: a Small World network. In summary, "both Informal Networks and the Formal Organizational Structure are required to work well together in order to deliver the Agile Organization" for effective C2. The secure object routing framework described earlier promises to provide the "shortcuts" essential to C2 network evolution.

However, significant challenges remain to develop the SOA networks required. The overhead associated with maintaining the message stream and the higher levels of abstraction required in web service communication make this promise difficult in systems of even moderate complexity. This is particularly pronounced when using an integration architecture that follows traditional, centralized orchestration patterns. The challenge is maintaining security, performance, and reliability across disparate systems while minimizing the impact on service levels and the need for significant additional infrastructure investment. As a result of our Navy work, we will be addressing several fundamental issues that need to be solved for full deployment of C2 Systems over the GIG with complete situational (and cultural) awareness to support integrated Military and Civilian operations.

References

S. R. Atkinson & J. Moffat (2005) - The Agile Organization: From Informal Networks to Complex Effects and Agility.
Publisher: DoD Command and Control Research Program, Washington, D.C.

H. Haury (2005) - Resolving the Problem of Aligning Communities of Interest, Data Format Differences, Orthogonal Sensor Views, Intermittency, and Security – DoD Homeland Security Command and Control Advanced Concept Technology Demonstration.
Whitepaper presented by J. A. Sturm at 10th CCRTS in June, 2005.
Publisher: NuParadigm Government Systems, St. Louis, MO

S. Flynn – America: The Vulnerable
Publisher: Harper Collins, 2006

J. A. Sturm (2007) - An Architecture and Model For Multi-Level Secure Chat Services.
Accepted for Presentation at the IEEE Sarnoff Symposium, May 2007 at Princeton University