NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

METHODOLOGY FOR EVALUATING THE EFFECTIVENESS OF COLLABORATIVE TOOLS FOR COORDINATING MDA EMERGENCY RESPONSE

by

Richard J. Wagreich

September 2006

Thesis Advisor: Alex Bordetsky
Second Reader: Sue Higgins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Methodology for Evaluating the Effectiveness of Collaborative Tools for Coordinating MDA Emergency Response		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Richard J. Wagreich, LTJG, USNR			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** **DISTRIBUTION STATEMENT A**	

13. ABSTRACT (maximum 200 words)

The Federal Government recognizes that collaboration between the various departments and local, federal, and private sector can best support maritime security. Of course the question is how to get these entities to collaborate? Collaborative technology can provide an answer to Maritime Domain Awareness (MDA) and Emergency Response collaboration, but the right tool for this mission must be selected. In order for the right tool to be selected, then the right criteria must be used to evaluate the tool for this particular mission. The criteria must not only look at the tool or the network, but the whole picture: cognitive processes, organizational structure, and the doctrine and procedures of the players involved.

This thesis will focus on establishing criteria for evaluating collaborative tools in the tactical environment of MDA and Emergency Response collaboration. In this environment, an Incident Commander will need to coordinate military, coalition, federal, state, local entities, as well as non-governmental organizations. A methodology does exist that meets these criteria, the North Atlantic Treaty Organization Code of Best Practice for assessing Command and Control Systems.

14. SUBJECT TERMS NATO COBP, C4ISR Evaluation, Collaborative Technology, MDA, Emergency Response, Disaster Relief			**15. NUMBER OF PAGES** 71
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

METHODOLOGY FOR EVALUATING THE EFFECTIVENESS OF COLLABORATIVE TOOLS FOR COORDINATING MDA EMERGENCY RESPONSE

Richard J. Wagreich
Lieutenant Junior Grade, United States Naval Reserve
B.A., George Washington University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: Richard J. Wagreich

Approved by: Alex Bordetsky,Ph.D.
Thesis Advisor

Susan Higgins
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Federal Government recognizes that collaboration between the various departments and local, federal, and private sector can best support maritime security. Of course the question is how to get these entities to collaborate? Collaborative technology can provide an answer to Maritime Domain Awareness (MDA) and Emergency Response collaboration, but the right tool for this mission must be selected. In order for the right tool to be selected, then the right criteria must be used to evaluate the tool for this particular mission. The criteria must not only look at the tool or the network, but the whole picture: cognitive processes, organizational structure, and the doctrine and procedures of the players involved.

This thesis will focus on establishing criteria for evaluating collaborative tools in the tactical environment of MDA and Emergency Response collaboration. In this environment, an Incident Commander will need to coordinate military, coalition, federal, state, local entities, as well as non-governmental organizations. A methodology does exist that meets these criteria, the North Atlantic Treaty Organization Code of Best Practice for assessing Command and Control Systems.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr. Alex Bordetsky and Professor Sue Higgins for their mentoring and support. Their knowledge has allowed me to see collaboration both from a technical and social aspect. I would also like to thank Alex for his guidance throughout the last two years. In addition, I would also like to thank Mr. Phil Wiliker, NORTHCOM, for providing time and guidance to a young junior officer to assist him in the right direction on Collaborative Technology requirements, and LTCOL Karl Pfeiffer, USAF, for always taking the time to provide necessary guidance to a lost naval Junior Officer.

On a personal note, I want to thank Mr. Mike Homen, and his wife, Barbra for their continued guidance over the past two years, and Ms. Alena Neighbors for her love, support, and keeping me on the straight and narrow while writing this thesis. Finally, I want to thank my father and mother, Ira and Honora Wagreich, for their insistence that I continue to persevere until this task was complete.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Imagine a routine cargo vessel entering San Francisco Bay carrying a routine container with a routine crew, or so the ship's manifest says. In reality, two members of the crew support a terrorist network and have shipped a nuclear agent capable of disrupting the city of San Francisco. How can we quickly interdict and capture the terrorist cell? How do our emergency response units (fire, medical, and police) respond with military assistance? It seems like the plot of a movie, but since September 11, 2001, this scenario has become an event that federal, state, and local agencies have sought strategies to address. Of course, the current National Strategy for Maritime Security (September 2005) concedes that various departments, federal, state, and local, have carried out their own strategies and solutions for the above questions. In December 2004, the President directed the Secretaries of the Department of Defense and Homeland Security to lead the Federal effort to develop a comprehensive National Strategy for Maritime Security, to better integrate and synchronize the existing Department-level strategies and ensure their effective and efficient implementation.

In his speech to the Cleveland City Press Club, Commandant of the Coast Guard Thomas Collins said, "Well, the plan, stated in its simplest terms, is to identify and intercept threats well before they reach our shores. Realization of this goal depends on timely information-sharing, protecting our vital maritime infrastructure, partnering with others at home and abroad, building on

current international cooperative security efforts, and preparing to respond quickly to future events."[1] His speech entitled "Collaboration: The Pathway to Maritime Domain Awareness (MDA) Success" indeed shows the necessity of collaboration between various agencies to achieve unity of effort in maritime security and emergency response to an MDA threat. The Maritime Domain is defined as all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime related activities, infrastructure, people, cargo, and vessels and other conveyances.[2] Maritime Domain Awareness is defined as the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States.[3]

The National Strategy for Maritime Security states that maritime security is best achieved by blending public and private maritime security activities on a global scale into an integrated effort that addresses all maritime threats. The Strategy aligns all Federal government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private sector entities.[4]

---

[1] Admiral Thomas Collins, USCG, "Collaboration: The Path to Maritime Domain Awareness Success," June 2005.

[2] National Security Presidential Directive NSPD-41, 21 December 2004, p. 5.

[3] Ibid.

[4] National Strategy for Maritime Security, Department of Homeland Security, September 2005, p. ii.

B. COLLABORATIVE TECHNOLOGIES

"Collaboration is the key to improving maritime security," Admiral Collins, Commandant of the Coast Guard, June 2005.

The Federal Government recognizes that collaboration between the various departments and local, federal, and private sector can best support maritime security. Of course the question is how to get these entities to collaborate? The private sector and the federal government have often provided technological solutions aimed at facilitating collaboration.[5]

What capabilities are necessary in the collaborative tools that will be employed? For federal agencies, the following capabilities are required as outlined in the December 9, 2005 Statement of Objectives for the new DoD Standard Collaborative Tool, the Net-Centric Enterprise Services (NCES):

1. Web Conferencing

For the Department of Defense, web conferencing is the most important standard capability for a collaborative tool.[6] It must provide the capability for users to meet virtually to conduct meetings, hold training, host conferences, etc.[7] Web conferencing must be available in two variations.[8] The first variation is ad hoc web conferencing sessions in which a virtual room is created when the meeting starts and dissolved when the last user departs. The second type of web conferencing is persistent

[5] OSD-C4I, DOD Standard Collaborative Tool Implementation Overview, GENADMIN, 101431ZAUG2001, p. 1.

[6] Net-Centric Enterprise Services Statement of Objectives, Defense Information Systems Agency, 9 December 2005, p. 2.

[7] Defense Information Systems Agency. Net-Centric Enterprise Services Statement of Objectives, 9 December 2005, p. 1.

[8] Ibid.

sessions in which the virtual rooms remain in existence regardless if any user is in attendance.

2. Virtual Spaces

The second capability requested for the Department of Defense is virtual spaces.[9] This capability permits users to collaborate asynchronously. With this capability, users would be able to indefinitely store files online and share them with some, all, or no other users.[10]

C. PROBLEM STATEMENT

There are many tools that are available that meet these capabilities stated in the Department of Defense (DoD) requirements. Table 1 is the current list, compiled by MITRE, of the collaborative tools that are available for local, state, and federal entities to choose from.

AUDIO/VIDEO CONFERENCING	
Camfrog Video Chat	Speak Freely
eyeballchat	Sun Microsystems ShowMe
MASH multicast-based collaborative apps.	TelNetZ, Inc.
MBONE Lawrence Berkeley National Lab Vat	TeraGlobal - Session
MBONE Lawrence Berkelely National Lab Vic	VocalTec Internet Phone
Microsoft NetMeeting	VTEL Video Conferencing System
Teleconferencing Central (online resource)	White Pines Cu-SeeMe Conferencing

CONFERENCE SERVERS	
Lotus - neT.120 Conference Server	PictureTel NetConference Multipoint Server

[9] Defense Information Systems Agency. Net-Centric Enterprise Services Statement of Objectives, 9 December 2005, p. 1.

[10] Ibid.

Persystant's Conferport	VocalTec Conference Server
Cisco ICS Collaboration Server	White Pines MeetingPoint Conference Server

TEXT CHAT AND INSTANT MESSAGING	
AOL Instant Messenger	MSN Messenger 1.0 ICQ
Abbot Chat	Mercury Prime
Bantu	Netlert
Express Communicator	NodScan
eRoom	Odigo
Gale Messaging System	Omniprise
DigiChat	Quicksilver
Jabber	SIMP
General Dynamics InfoWorkSpace LaunchPad	Trillian
Mirabilis ICQ	Volano Chat
Microsoft Chat	2 Way Interactive Messaging
MindAlign	Worlds 3D Chat
	Yahoo Messenger
	Zircon IRC Chat

DATA CONFERENCING	
Databeam FarSite	Netopia Timbuktu
Facilitate.com	Netscape Conference
Intel Proshare	Sun Microsystems SunForum
Glance	Placebased LiveMeeting
Microsoft NetMeeting	White Pines Cu-SeeMe Conferencing
Meetingworks	WebEx
Latutude - MeetingPlace	

PLACE-BASED COLLABORATION ENVIRONMENTS	
Centra	Lotus SameTime
ComanyWay	MShow
DSTC/DARPA WORLDS Project	MindAlign
eRoom	MITRE CVW Open Source Project
Extranet Secure Portals	Microsoft Netmeeting
General Dynamics InfoWorkSpace	Paragon Dynamics Virtual Environment Solutions
Groove	Collabraspace
iOra	SPAWAR Odyssey Collaboration System
GroupServe	SiteScape
GroupSystems	TeamWave Workplace
Presence-AR	TelNetZ, Inc.
WorkZone Extranet	**Web 4M**

COLLABORATIVE SOFTWARE DEVELOPMENT	
CollabNet	Rational
Embarcadero Technologies	CanyonBlue
TogetherSoft	Collaboration Technologies Inc.

DOCUMENT MANAGEMENT	
chrome – Nextpage	

Table 1. Current Collaborative Technologies on the Market as Compiled by MITRE

As this table shows, there are many tools that federal, state, and local entities can employ. As the private sector continues to provide tools that facilitate

collaboration, there must be criteria in place that enable the users to evaluate the selection of the tool. The criteria that are being used for source selection provides a broad view and focuses more on how the tool effects the computer network or the capabilities of the tool itself.[11]

Collaborative technology can provide an answer to MDA and Emergency Response collaboration, but the right tool for this mission must be selected. In order for the right tool to be selected, then the right criteria must be used to evaluate the tool for this particular mission. The criteria must not only look at the tool or the network, but the whole picture: cognitive processes, organizational structure, and the doctrine and procedures of the players involved. We must also realize that the collaborative environment shifts depending on which level of planning and execution the tool will be used: strategic, operational, or tactical. Of course as one moves from the tactical to the strategic level of planning and execution of Maritime Domain Awareness and Emergency Response, the environment increases in complexity and dynamics.

This thesis focuses on establishing criteria for evaluating collaborative tools in the tactical environment of MDA and Emergency Response collaboration. In this environment, first responders are from military entities, law enforcement, and federal, state, and local emergency entities. The on-scene commander (OSC) must coordinate these entities. In addition, international organizations may also provide assets for support. This means that the criteria must utilize a methodology that focuses on Joint-interagency collaboration with the possibility of working

[11] NCES Critical Comments, 9 December 2005.

with a coalition and civilian agencies. A methodology does exist that meets these criteria, the North Atlantic Treaty Organization Code of Best Practice (NATO COBP) for assessing Command and Control (C2 Systems).

II. THE NATO COBP FOR C2 ASSESSMENT

A. BACKGROUND

Since the end of the Cold War, NATO has been involved in missions that are not military in nature, or Operations Other Than War (OOTW). We have seen NATO used for peacekeeping operations, humanitarian assistance, and has also been deployed to areas outside the European continent. These missions have ensured that collaboration between NATO military commanders and civilian agencies, nongovernmental organizations (NGOs), and state entities has a necessity for successful operations.

Table 2 taken from the NATO COBP below demonstrates the differences between conventional and OOTW.

Factor	Symmetric, Conventional	OOTW
Mission/Operation		
Stability	Relatively stable	May be more dynamic
Focus	Enemy	No traditional opponent
Commitment	Common (military)	Uncertain (political/military)
Principles		
Unity	Of command	Of purpose
Decision making	Hierarchical	Consensus
Operations	Surprise, secrecy	Transparency
Information		
Nature of the problem	Knowns and knowns	Unknowns and knowns
Key question	How to get information	What information to get
Focus	Enemy military	Military/political/economic/ social factors
Situation awareness	Common air-land-sea	Limited dissemination, more complex
Database	Very large, well structured	Larger, less structured
Analysis		
Unit	Battalion level entity	More behavioural
Ease in integration	Relatively easy	Very difficult
Focus	Military (systems, organizations)	Political/Military and societal
Approach	Traditional operations analysis	"Softer" analysis

Table 2. Differences Between MOOTW and Conventional Warfare

Advances in *technology*, particularly information related technologies, offer military organizations unprecedented opportunities to significantly reduce the fog and friction traditionally associated with conflict.[12] At the same time, they may prove to be challenges in themselves across a wide variety of realms: technical, organizational, and cultural.[13] Therefore, in order for analysts to properly evaluate technology, one must look at these dimensions and see how organizational and processes influence the tools that need to be looked at. The NATO COBP provides a generic methodology that can help an analyst take all these aspects into consideration when developing the criteria to analyze tools.

B. WHY NATO COBP IS A GOOD METHODOLOGY FOR EVALUATING COLLABORATIVE TOOLS FOR EMERGENCY RESPONSE

If the NATO COBP is a top-down approach that depends on user requirements and Measures of Merit (MoM) that may not fully address the dynamics in coordinating emergency response for an MDA threat, why use it? First of all, the NATO COBP provides a generic methodology to looking at C2 assessment. It is up to the analyst to use the process to define a specific problem. Secondly, the Operational environment which MDA Threat Response falls into is an area the Department of Defense refers to as: Military Operations Other Than War (MOOTW). Joint Publication 3-07, delineates Six Principles for MOOTW: objective, unity of effort, security, restraint, perseverance, and legitimacy.[14]

[12] SAS-026. The NATO CODE OF BEST PRACTICE for C2 Assessment. CCRP, 2002, p. 2.

[13] Ibid.

[14] JP3-07, Joint Doctrine for Military Operations Other Than War, DoD, 16 June 1995, p. II-1.

Compare these principles that guide MOOTW with the principles outlined in the National Plan to Achieve MDA and one can make a few comparisons: unity of effort, information sharing and integration, safe and efficient flow of commerce.[15] One can see the principles of unity of effort, security, and perseverance in the MDA principles. The statement that opens the principles, "The first step towards meeting these principles is to ensure GMCOI stakeholders, at all levels, know what they can do to help, how they can do it and, most importantly why Maritime Domain Awareness is in their collective best interest,[16]" shows that MDA is attempting to obtain the legitimacy principle of MOOTW as well. The focus of the NATO COBP is to provide a methodology to assess Command and Control (C2) technology within a MOOTW environment given the complexity of civilian-military-coalition operations. This environment coincides with the environment that the collaborative technology would be used for in a tactical MDA emergency response.

C. WHAT IS THE NATO COBP PROCESS?

The NATO COBP offers broad guidance on the assessment of C2 for the purposes of supporting a wide variety of decision makers.[17] It should be noted that the COBP is focused upon the assessment challenges associated with the nature of C2, and does not provide a specific solution to a C2-related problem.

[15] Department of Homeland Security, National Plan to Achieve Maritime Domain Awareness, October 2005, p. 4.

[16] Ibid, p. 3.

[17] Ibid, p. 11.

1. Steps Applied to the Process

All steps of assessing C2 systems are interrelated and hence interdependent. Figure 1 taken from the NATO COBP outlines these phases and interrelationships.

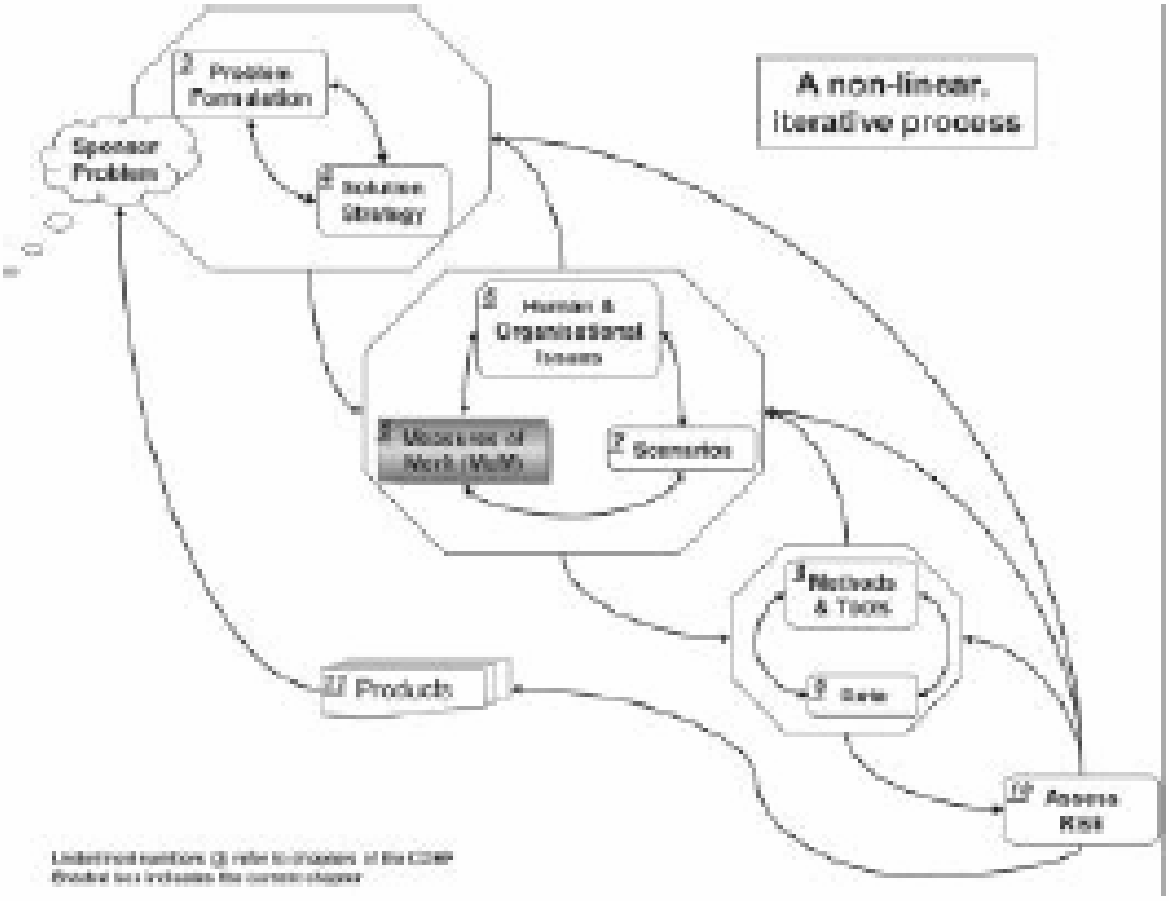

Figure 1. C2 Assessment Process

The phases are Problem Formulation and Solution Strategy; Measures of Merit, Scenarios, and Human and Organizational Factors Analysis; Methods and Data

Requirements; and finally Risk Assessment and products finalization.

a. Problem Formulation & Solution Strategy

According to the NATO COBP, problem formulation involves decomposition of the analytic problem into appropriate dimensions such as structures, functions, mission areas, command echelons, and C2 systems[18]. The NATO COBP states that this is an ongoing process, as outlined in Figure 2.

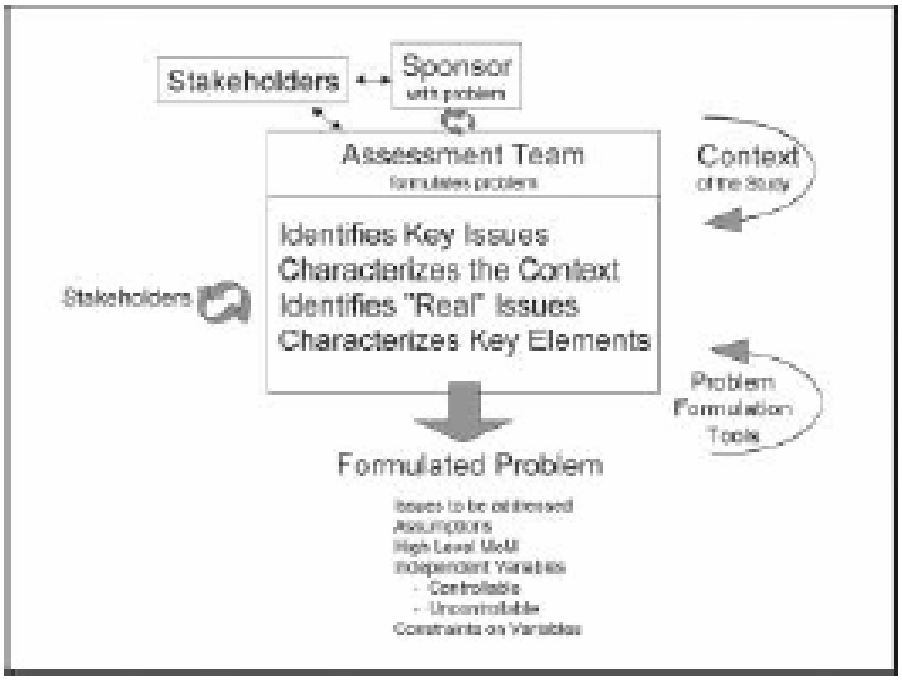

Figure 2. Problem Formulation Process (NATO COBP)

Chapter III will provide a discussion of the key issues.

A solution strategy is “How” the assessment of the technologies will take place. It includes the statement of work outlined by the sponsor, experimentation campaign

[18] SAS-026. NATO COBP for C2 Assessment, CCRP, 2002, p. 54.

plan, and study management plan.[19] Figure 3 outlines the process of the solution strategy. The solution strategy is discussed in Chapter IV in the form of scenarios integrated into the Tactical Network Topology Experiments and the Strong Angel Disaster Relief Series.

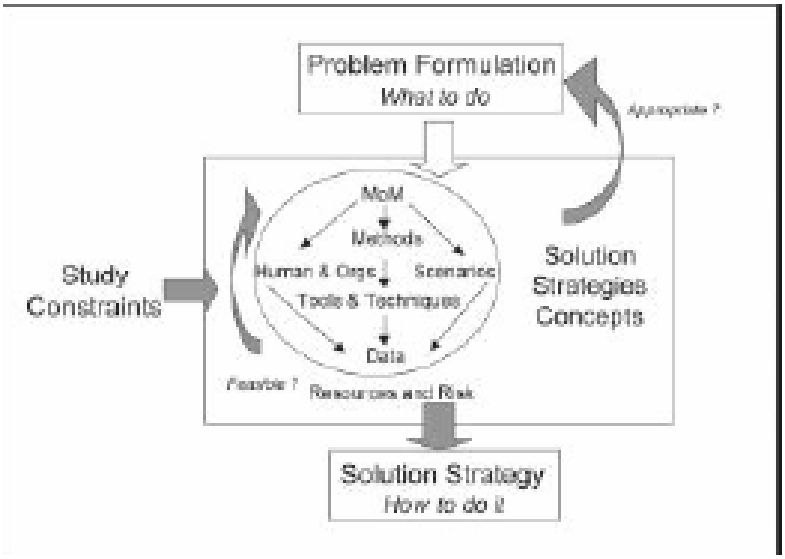

Figure 3. Solution Strategy Process (NATO COBP)

b. Measures of Merit

The reason the NATO COBP is a good process for evaluating collaborative tools is that the Measures of Merit (MoM), the evaluation criteria, looks at not only the technology, but also its impact on the decision makers, the cognitive processes, organizational structure, and policy or doctrine. The NATO COBP utilizes a hierarchy of MoM, arranged into five categories. Dimensional Parameters are the most basic and focus on the properties or characteristics inherent in the physical C2 systems.[20] Next are Measures of Performance (MoP), which focus on internal

[19] SAS-026. NATO COBP for C2 Assessment, CCRP, 2002, p. 38.

[20] Ibid., p. 92.

system structure, characteristics and behavior.[21] Next are Measures of C2 Effectiveness (MoCE), which focus on the impact of C2 systems within the operational context.[22] Next are Measures of Force Effectiveness (MoFE), which focus on how a force performs its mission or the degree to which it meets its objectives.[23] The highest levels of MoM are Measures of Policy Effectiveness (MoPE), which focus on policy and societal outcomes.[24] The relationships of these five relationships are shown in Figure 4 as taken from the COBP.

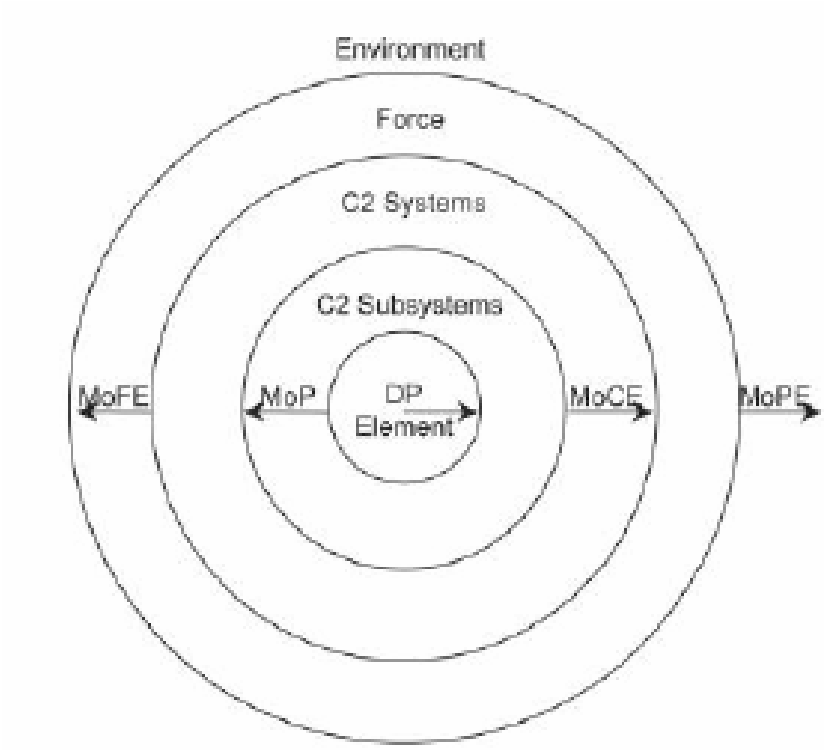

Figure 4. Relationships between the Measures of Merit

[21] SAS-026. NATO COBP for C2 Assessment, CCRP, 2002, p. 92.

[22] Ibid.

[23] Ibid.

[24] Ibid.

c. Scenarios/Human and Organizational Factors

The NATO COBP defines scenario as a description of the area, the environment, means, objectives, and events related to a conflict or a crisis during a specified time frame suited for satisfactory study objectives and the problem analysis directives.[25] Scenarios consists of four elements—a context (i.e. geopolitical situation), the participants (e.g., intentions, capabilities of blue, red, others), the environment, and the evolution of events in time.[26] In C2 assessments, the purpose of scenarios is to ensure that the analysis is informed by the appropriate range of opportunities to observe the relevant variables and their interrelationships.[27]

The human dimension is one of the distinguishing characteristics of C2. The NATO COBP addresses these characteristics into three categories. The first category is human behavior related to performance degradation, such as stress and fatigue, and as a consequence of social interactions among individuals and members of groups.[28] The second is decision-making behavior (cognitive questions) including the cognitive complexity of the issues and the capacities of the commanders or other decisionmakers of interest.[29] The last is command style.[30] These issues and factors are discussed in Chapter III of the thesis.

---

[25] SAS-026. NATO COBP for C2 Assessment, CCRP, 2002, p. 164.

[26] Ibid., p. 165.

[27] Ibid.

[28] Ibid, p. 128.

[29] Ibid.

[30] Ibid.

2. Challenges of the Top-Down Approach to C2 Analysis

The NATO COBP utilizes a top-down approach to analyzing the C2 system. With a top down approach, higher level echelons determine the user requirements and the MoM that needs to be considered in the problem formulation. The challenge with a top down approach is that the requirements may fit the strategic and operational dimensions that the various services or agencies need. The user requirements for example in the Net-Centric Enterprise Service (NCES), the new collaborative tool for the Department of Defense, the Selection process came from the Combatant Commanders and the Service Chiefs.[31] These individuals, however, operate on the strategic and operational levels of warfare. However, these requirements may not fully address the dynamics in coordinating emergency response for an MDA threat on a tactical level.

[31] Phil Wiliker, C2 Division, NORTHCOM, Phone Conversation, 2 February 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TACTICAL USER REQUIREMENTS

A. HIGH LEVEL REQUIREMENTS COMPARED

On February 28, 2003, the President issued Homeland Security Presidential Directive (HSPD)-5, which directs the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS). According to HSPD-5: *This system will provide a consistent nationwide approach for Federal, State,[2] and local[3] governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system; multiagency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources.*[32] Beginning in FY 2006, federal funding for state, local and tribal preparedness grants will be tied to compliance with the NIMS.[33] With funding on the line, any collaborative tool will need to ensure it complies with the procedures, organizational structure outlined in the NIMS.

The NIMS outlines both the organizational structure and the technology requirements that need to be in place so

[32] George Bush. Homeland Security Presidential Directive-5, Department of Homeland Security, 28 February 2003, p. 1.

[33] Alex Bordetsky, et. al. Progress Report on the NJ Emergency Response Network, May 2006, p. 7.

that a collaborative tool needs to be tied into or measured against.

In addition, for a joint collaborative tool between the military and the first responders in responding to an MDA threat, a comparative study must be made that looks at both the traditional Maritime Component Command Structure and the NIMS.

1. Organizational Structure

When various agencies arrive on the scene in a disaster most organizations find themselves in a chaotic environment. There are “social and technical blinders” established where people are focused on their own agendas. The challenge, therefore, with emergency response is how to get the people to go past their own agendas and see each other as allies rather than adversaries in support of a mission. An organizational structure does provide that capability on a human side.

The NIMS provides a dynamic bottom-up command and control structure. An incident commander is generally a local policeman, fireman, or emergency technician. As the incident increases in complexity, so does the seniority of the incident commander: going from local, to city, to county, to state, and final federal agencies. All agencies are supporting the incident commander, which could be a local/city/or state agency. The NIMS also provides the ability of an agency to emerge within the command and control structure quickly and easily.

This differs from the military traditional command and control structure in which command is given to the senior person present. Nevertheless, the goals of the incident commander are the same in emergency response as they are in

maritime domain awareness: achieve Unity of Effort from all participants and make decisions as timely and accurate as possible.

2. Technology

One of the main elements of maintaining unity of effort is the establishment of shared situational awareness or a common operational picture. The NIMS training online states: "Effective communications, information management, and information and intelligence sharing are critical aspects of domestic incident management. Establishing and maintaining a common operating picture and ensuring accessibility and interoperability are principal goals of communications and information management."[34] If we look at the priorities needed for Information Sharing from the National Plan for Achieving Maritime Domain Awareness outlined in Table 3 below, we see two comparative requirements for the sharing of information: establish a Common Operational Picture (COP) for all entities and technology must be interoperable with all players.

[34] http://www.nimsonline.com, Official NIMS training website, Communications and Information Management Session.

Information and Standards			
Actions and Tasks	**Near Term**	**Long Term**	**Agency Lead**
Share Information			
Eliminate regulatory barriers to information sharing and interoperability through the establishment of operating protocols, Memorandums of Understanding and Memorandums of Agreement necessary for joint, interagency and industry relationships.		X	DOD DHS
Restrict access privileges to ensure data are only use for specific purpose, for finite time, and by those with necessary permissions.	X		DOD DHS
In accordance with Executive Order 13356 (Sharing of Terrorism Information) and the Intelligence Reform Act of 2004, establish legal authorities, interagency agreements, and policies to allow the processing and fusion and of foreign intelligence, domestic law-enforcement information, and commercial maritime data, with appropriate safeguards.	X		DOD DHS
Enhance automated database, sensor, information extraction and fusion through a common distributed virtual database.	X		DOD DHS
In compliance with national statutes, law, policy, and Presidential Directives, develop and implement information handling procedures to identify data requiring special protection. Leverage current Intelligence Community efforts to develop secure, authenticated access and user controls for classified, sensitive, or restricted information.	X		DOD DHS
Develop an open architecture for data sharing, with governance standards for web-based information storage access.	X		DOD
Establish and implement interoperable communication standards, to include mandating, as appropriate, DOD's Global Information Grid (GIG) across Federal, state and local partners to enable information sharing.		X	DOD
Mandate a "write-to-release" standard be applied across all collection regimes.	X		DOD
Establish a network-centric, near-real time virtual information grid that can be shared, at appropriate security levels, by Federal, state, local, and international agencies with maritime responsibilities. This national maritime common operating picture will be the primary means of dissemination for MDA information.	X		DOD DHS
Establish information assurance capabilities that allow the sharing of information through all levels of classification in both directions between highly classified and law enforcement sensitive.	X		DOD

Table 3. Information Sharing Priorities Outlined in National Plan for Achieving MDA

3. Conclusions from Analysis

Based on the analysis of the priorities and the way emergency response and the military will be operating, we see similar issues and requirements being generated. We see organizational structures that will be hierarchical and static where the players are known: a boarding team reaching to databases for information or a law enforcement squad responding to a boat in the harbor. However, both the National Plan for MDA and the NIMS argue that traditional structures may not adequately address the terrorist threat.

An ad hoc organizational structure can provide the dynamic organizational need to address both emergency response and MDA. A Joint Interagency Task Force (JIATF) for the military or a Unified Command (UC) Structure for the civilian first responders can provide this ad hoc structure. Within these structures various agencies can come together under a JIATF or Unified Commander. By collaboration, these entities provide the necessary unity of effort needed to obtain a successful operation. In both cases, the goal is to share information and maintain a Common Operational Picture. The selected technology must support both the military and the civilian side in order to ensure collaboration between civilian first responders and military support for domestic MDA threats. At the same time, the technology must also provide the decision makers the ability to make decisions as quickly and as accurately as possible. The technology must not only allow humans to collaborate and achieve unity of effort, but also be interoperable with each other in order to facilitate human

collaboration. How will a collaborative tool fit into this picture?

B. THE ROLE OF COLLABORATIVE TOOLS

Microsoft Groove was the main collaborative technology used by disaster relief teams during Hurricane Katrina. MS Groove is a collaborative tool that offers a standard workspace that includes whiteboard, file sharing, chat, VOIP, project management, and instant messaging capability. A study of how Groove was used in a traditional organizational structure provides a glimpse at how the technology was used. As a response, to Hurricane Katrina, Naval Postgraduate School (NPS) sent two detachments to the Gulf Coast. If one looks at the Task Force Katrina Workspace for NPS Detachment 2 in Groove, we see the following data:

1. Chat was limited to determining who was who inside the network during the early phases when the network was in the process of being established.
2. The functions that were used the most were the file sharing and discussion capabilities.

In contrast, we can look at the MS Groove Workspace for the cooperative NPS-Special Forces Command (SOCOM) Maritime Interdiction Operations (MIO) Field Experiments. These experiments are covered in greater detail in the next chapter. By looking at the Katrina Workspace, MS Groove's file sharing capability was extensively used. This information was used by the Joint Forces Maritime Component Commander (JFMCC) for making decisions. Likewise, MS Groove's file sharing capability and discussion board were used extensively in support of a boarding party during the

MIO Field Experiments for helping participants make a decision with regard to the MDA Threat. However, unlike, the Katrina situation, the chat capability was extensively used, allowing peer-to-peer relationships to exist between the participants in communicating. A collaborative technology that provides or an organizational structure that uses chat, instant messaging, and other peer-to-peer services, has the potential of transforming a traditional C2 structure into an ad hoc structure. Likewise, an ad hoc structure would rely heavily not only on the file sharing and discussion board features, but also chat, instant messaging, and other peer-to-peer services. Figure 5 shows the two roles that a collaborative tool can provide to an organization, either as a collaborative mechanism for transformation or as a decision support tool.

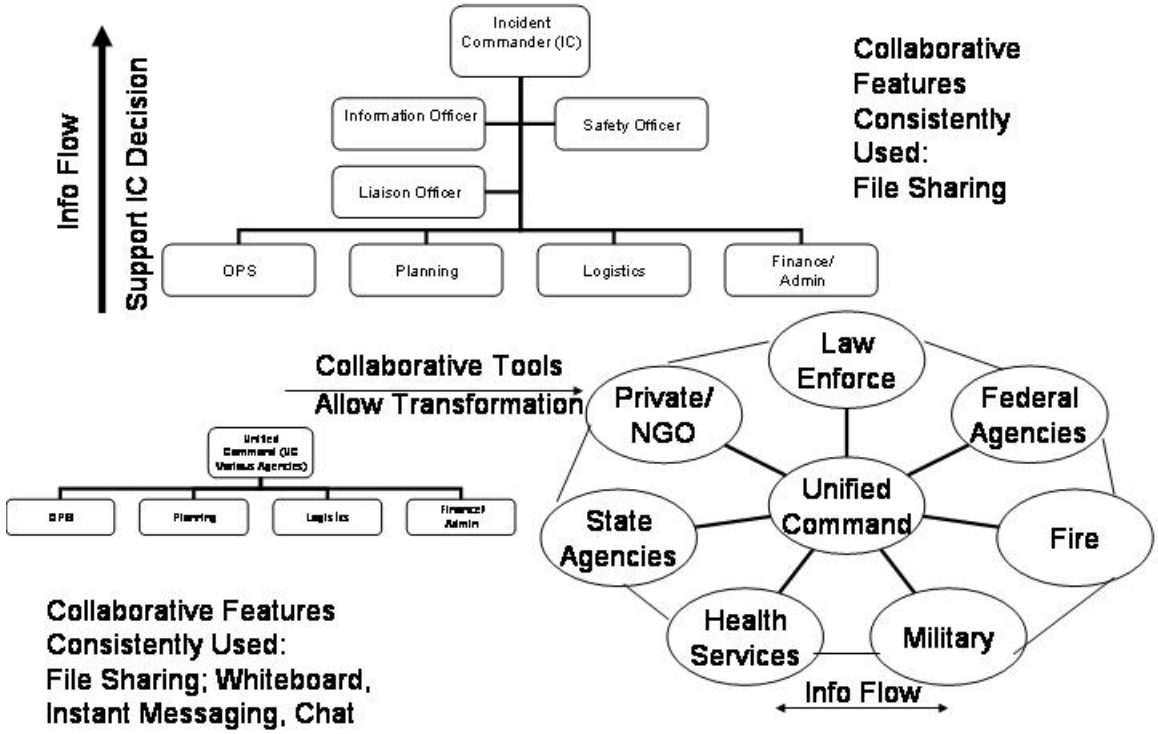

Figure 5. Collaborative Tool Role and Organizational Structure

IV. METRICS AND EXPERIMENTATION

A. METRICS TO BE USED FOR EVALUATION

From the previous chapter, there are several areas that an analyst evaluating the tool needs to look at. The first area is the interoperability of the tool. In terms of the NATO COBP Measures of Merit, interoperability can be an area for evaluation as a Measure of Performance (MOP), Measure of Effectiveness (MOE), Measure of Force Effectiveness (MOFE), and Measure of Policy Effectiveness (MOPE). As a MOP, interoperability can be determined in two ways. In accordance with the NIMS, all entities participating in an emergency response check-in with a Liaison Officer, assigned to the Command Staff of the Incident Commander. For a collaborative tool to really be interoperable, it should be able to interact with most of the tools that are at the disposal of the Incident Commander. The second phase of interoperability is how quickly the tool can be accessed once interfacing with another tool. In terms of the other Measures of Merit associated with interoperability, surveys given to the decision makers who would be using the tool, could provide data. Unfortunately, the data collected from these surveys are "fuzzy information," since they are based on the subjective view of the users. In order to provide more objective data, sampling a greater audience of users would generate a normal distribution of the answers.

Situational Awareness (SA) and the ability to provide a Common Operational Picture (COP) is another area for evaluation. In order to evaluate the SA, the scenario must provide major events that participants must respond. All

users of the collaborative tool should be asked about their understanding of the situation after the event is planned. Again, each user will write about their experience and their piece of the situation, so the information may be "fuzzy." By providing a broad range of users and a large sample audience, the information should unfold into a normal distribution of the data.

However, there must be other issues that need to be considered. During the Strong Angel III Disaster Relief Demonstration, many collaborative tools were brought into the field. There, feasibility and ease of use were definitely factors in the success of the operations that were unfolding during the exercise. Based on the After Action Report and Lesson Learned from Hurricane Katrina and my observations from Strong Angel (more detailed in Chapter V), Table 4 provides general questions an analyst should consider when evaluating a tool to be used for emergency response and civilian-military MDA response for a selection authority (FEMA, federal, state, local, military, DHS, etc.) Prior to selection of the tool for general distribution, the answers to these questions should be used in the report to the selection authority.

Dimensional Parameters		
Tool Evaluated		Date:
Capabilities	What services does this tool offer? (i.e. chat, file sharing)	
System Requirements	Is the tool peer-to-peer or client server? How much memory is required to run the program? How many users can be supported by this tool?	
Security of Information	How does the tool protect confidentiality of information? How does the tool protect authenticity of information? How does the tool protect integrity of information?	

Table 4. Overarching Questions for an Analyst Regarding Dimensional Parameters

Measures of Performance		
Tool Evaluated		Date:
Scalability	How fast does a user get access to the tool as the number of users increase? How fast do clients retrieve information as the number of clients on the network increases? How much memory is required as each user enters the workspace?	
Network effects	How much of the Available band-width is used to support users? As client usage increases, what is the network latency time?	

Table 5. Overarching Questions for an Analyst Regarding Measures of Performance

Availability of Information	How soon is data available for use? How many users are able to get access to documents? How often is the data accessible to users?	
Security of Information	How much of the data is viewed by “non-trusted agents”? How much of the data used is created by “non-trusted” agents? How much of the information is unnecessary information?	
Interoperability	Of the systems available for use, how many can the collaborative tool interface with? How fast can the tool be set up and made operational with the other systems?	
Feasibility	Can the tool be used on FCC unlicensed bands? Can the tool be easily deployed?	

Table 6. Overarching Questions for an Analyst Regarding Measures of Performance (continued)

Measures of Effectiveness		
Tool Evaluated		Date:
Information Sharing	How many files are posted in the file sharing area? How many files posted are needed by the user? How many Requests for Information are submitted by the users? Which users did not need the information shared? What collaborative features were used by the participants? What collaborative features were not used? Why not?	

Table 7. Overarching Questions for an Analyst Regarding Measures of Effectiveness

Decision Support	How fast was the DM process made with the tool? How fast is the DM process without the tool? Once information was posted in the tool, how quickly did the DM get that information? Did the tool provide a clear understanding to the DM of where the information was located? Did the tool provide a capability to alert decision maker that new data is available? What collaborative features did the DM like and use in the DM process? How did the tool help the process? How does the process change with this collaborative tool?	

Table 8. Overarching Questions for an Analyst Regarding Measures of Effectiveness (continued)

Commander's Intent	What were the objectives of the Response Team? How did the tool help accomplish those objectives? How did the tool affect the organizational structure? Is the tool a burden or a help in accomplishing the mission?	
Situational Awareness	Did the tool make both the IC and EOC Commander aware of what tasks still need to be complete to fulfill mission objectives? Did the tool enable the IC and EOC Commander to come to an agreement as to what still needs to occur to complete mission objectives? Did the tool alert the ICP and EOC of major situations that were occurring during the course of the incident?	

Table 9. Overarching Questions for an Analyst Regarding Measures of Effectiveness (continued)

Interoperability	On the application level, how many applications cannot interface with the tool? On the network level, how many information networks available to the IC and staff, can the tool operate on? Of the users that the IC needs for decisions, how many cannot use the tool?	

Table 10. Overarching Questions for an Analyst Regarding Measures of Effectiveness (continued)

A survey is the best method of getting answers to these questions. Below is an example of survey questions that provide more specific answers to the questions in Table 6. The tool that will be evaluated is MS Groove during the MIO Experiments between 29 August and 1 September 1, 2006 in Alameda Bay. Keep in mind that the answers are subjective to the view of the users. Therefore, the more users that take the survey, the better the distribution of answers, and hopefully, the more objective the analysis will provide.

TNT 06-4 Survey

Name:_____ Position: _____
Date: _____ Tool Evaluated: _MS GROOVE__

Part I: Experience with MS Groove

A. Prior to exercise

1. On average how often did I use MS Groove prior to the exercise?

1	2	3	4	5
Never	1/month	1/2 weeks	1 week	Every day

2. The training I received on MS Groove was beneficial?

1	2	3	4	5	6
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	N/A

Why?_____
_____
_____
_____

Part II: Interaction with the tool

1. It was easy for me to find the information I needed from MS Groove discussion and file sharing.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

2. MS Groove alerts helped me realize when new information was available.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

3. MS Groove made it easier to get data from the boarding party.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

4. MS Groove made it easier to get data from advisory entities like Biometrics Fusion Center and Lawrence Livermore Laboratory.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

Part III. Situational Awareness

1. What is your understanding of the situation as of Date: _____ Time: _____

_____
_____
_____
_____
_____
_____
_____
_____
_____

2. MS Groove's features (chat, discussion board, etc.) made it easier to come to an understanding of the situation.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

3. MS Groove made it easier for me to maintain control of the situation.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

4. MS Groove improved my ability to coordinate assets.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

5. MS Groove improved my ability to track assets.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

Part IV. Decision Support

1. MS Groove allowed me to make faster decisions.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

2. MS Groove was the primary means of sharing my thoughts with necessary participants.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

3. MS Groove was the primary means of getting feedback from boarding party, fusion centers, and the Tactical Operational Command Center.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

4. MS Groove allowed me to quickly identify which problems I could address and which ones I need to pass on.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

Part V. The process

1. MS Groove improved my ability to meet the Tactical Operational Commander's Objectives

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

2. MS Groove improved my ability to respond to the threat.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

3. How did the tool change my Standard Operating Procedures?

_____
_____
_____
_____

4. Changes to my Standard Operating Procedure were worth using MS Groove.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Why?_____
_____
_____
_____

B. EXPERIMENTS THAT CAN PROVIDE TESTING

Currently, there are two experiments that helped provide the grounds for testing the metrics above and resolving the overarching questions outlined in Table 6: the Strong Angel III Disaster Relief Integration Demonstration and the Tactical Network Topology (TNT) MDA Experiment. In both cases, MS Groove is the primary means of collaboration between entities.

1. Strong Angel III Disaster Relief Demonstration Overview

Strong Angel III is a low-key demonstration of globally relevant methods for improving resilience within any community under pressure. Strong Angel III is particularly designed to explore techniques and technologies that support the principle of resilience within a community that finds itself isolated and vulnerable.[35]

a. Scenario

In the demonstration the citizens of a community are deprived of power, cell phones, and Internet access, and are beyond the immediate reach of federal assistance. One key objective of this project is to effectively tap the expertise and creativity within an affected community, including through public-private partnerships. A second overarching objective is the development of social tools and techniques that encourage collaborative cooperation

[35] www.strongangel3.net/about

between responders and the population they serve during post-disaster reconstruction."[36]

2. TNT MDA Experiment Overview

The TNT MDA Experiment is a joint venture between the Naval Postgraduate School, US Special Operations Command (USSOCOM), and the Lawrence Livermore National Laboratory (LLNL). The objective of this experiment is to continue to evaluate the use of networks, advanced sensors, and collaborative technology for rapid Maritime Interdiction Operations (MIO); specifically, the ability for a Boarding Party to rapidly set-up ship-to-ship communications that permit them to search for radiation and explosive sources while maintaining contact with the mother ship, C2 organizations, and collaborating with remotely located sensor experts.[37]

The MDA Experiment has increased in complexity over the last few years. The initial experiment began with a coast guard cutter and a small diving vessel, the Cypress Sea as the target and mother ships for the boarding. Today, the TNT MIO experiment includes cargo vessels, a coast guard cutter, local and state law enforcement, LLNL, Biometrics Fusion Center, Maritime Intelligence Fusion Center West, and Coast Guard District Eleven as participants. In addition, several federal agencies and foreign nations (Austria, Sweden, and Singapore) are observing remotely.

a. Scenario

The Scenario for TNT 06-4 was that the port of Hong Kong communicated to the Maritime Security Office

[36] www.strongangel3.net/about

[37] Bordetsky, Alex. TNT 06-3 MIO Plan, June 2006, p. 1.

(MSO) in the port of Oakland that they detected radiation on a container that was bound for the port of Oakland, but guards had their radiation sensors to high for local detection and arrest. By coordinating with the US Coast Guard (USCG) and the United States Navy (USN) for assistance, the MSO, the USCG, and the USN detect the radiation source and the USCG District 11 orders the interdiction of the vessel.[38] A network diagram of the TNT 06-4 diagram as compiled by Georgios Stavroulakis is shown in Figure 6.

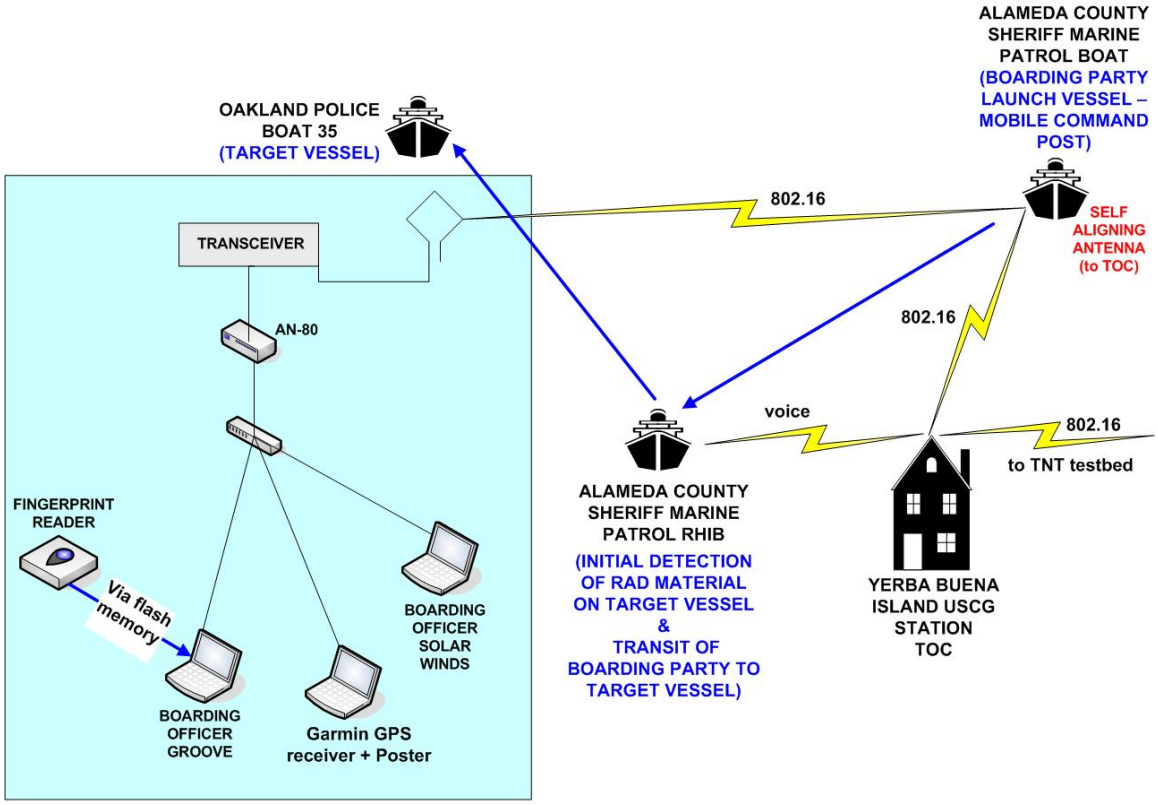

Figure 6. TNT 06-4 MIO Network Diagram

[38] Brian Rideout, et. al. TNT 06-4 MIO Plan, Scenario, p. 3.

V. RESULTS

A. MS GROOVE EVALUATION

MS Groove was the primary collaborative tool for both Strong Angel and TNT MIO Experiment. As stated in Chapter IV, both experiments provided an opportunity to apply the metrics to evaluate MS Groove.

1. Evaluation of MS Groove During Strong Angel III

Based on observations and surveys taken at the Incident Command Post and the Emergency Operations Center, the following evaluation of MS Groove was conducted. During the ad hoc structure that developed during the Strong Angel III demonstration, MS Groove was one of the tools that enabled collaboration and file sharing. The features used by the various Operations Centers were file sharing and whiteboard.

In terms of performance, the ad hoc information network established could not support the weight of all the users on MS Groove workspaces. Without any clear structure to follow, users were sending data simultaneously. The result was the collapse of the network and the need to recycle the disaster relief information network continuously throughout the exercise. In terms of effectiveness, MS Groove could not really prove itself due mainly to the attitudes of people. Every person who brought technology to the Incident Command Post (ICP) wanted to use their technology during the demonstration. As a result, even though MS Groove was slated to be the main tool, it became one of several collaborative tools that were being used by the IC. In fact, the IC refused to even turn on MS Groove in his command post, because he

heard it was degrading the network. As a result, data needed by the IC could not be received via MS Groove, but by VOIP phone.

2. Evaluation of MS Groove During TNT Experiment

Based on observations and surveys taken at the Tactical Operations Center, the USCG District 11 Headquarters, and the Boarding Vessel, the following evaluation of MS Groove was conducted. The features used during the experiment were file sharing, whiteboard, instant messenger, chat, and task manager.

In terms of performance, the ad hoc information network established was able to support the weight of all the users on MS Groove workspaces, although there were only twenty five users active in the workspace during the experiment. The network was able to maintain the weight of the program as users became active in the workspace. More than 50% of packets across the network were Groove packets.

In terms of Situational Awareness and Decision Support, MS Groove Task Manager was able to keep track of the necessary tasks and help provide a common understanding of the situation to develop. This ability was able to foster cooperation between the various operations centers to be able to see what tasks still needed to happen to respond to the situation. Alerts helped the Boarding Officer realize that new information needed to complete the mission was available in MS Groove.

3. MS GROOVE CONCLUSIONS BASED ON BOTH EXPERIMENTS

The conclusions, therefore, of MS Groove is that MS Groove is a great tool when scalability is not a primary concern. It should not be used in an environment where everyone needs to post large amounts of data on a network

simultaneously. However, MS Groove when file sharing, discussion board, and task manager, are enabled the collaborative features of MS Groove make the tool a catalyst for transformation of hierarchical organizational structures into an ad hoc structure that can provide unity of effort for an incident commander.

B. STRONG ANGEL III OBSERVATIONS FOR METRIC REFINEMENT

The Strong Angel III demonstration provided an excellent opportunity in seeing how an ad hoc organizational structure and information network can be established.

1. People/Structure

The first day of the exercise, numerous vendors arrived to demonstrate the capabilities of their technology. For the first twenty-four hours, each vendor was limiting their vision to the capability of their technology. Once vendors realized that other vendors could help demonstrate their capability, collaboration between people began. However, unity of effort between vendors, non-governmental agencies, and other capabilities did not come about until the Incident Command Structure was established on the third day. With an incident commander now dictating requirements and needs, each vendor began to cooperate with other vendors.

As the week progressed, vendors began establishing relationships that helped achieve mission success. One such example was the relationship between a satellite/digital network provider, a teleconference server provider, and a video/audio company that was providing data for a teleconference. On the first sortie, there was a

slight disconnect between the players, and the information took about ten to fifteen minutes to transmit data back to the Emergency Operations Center (EOC). By the second sortie, these same three companies had their equipment set up and operational within five minutes. The only delay was that the EOC Manager was having a “press conference” and requested that the EOC dial into the video teleconference at a later time. Once the EOC dialed in, the data was sent flawlessly.

2. Technology

The first day of Strong Angel III seemed like a trade show with technologies from all across the country being demonstrated for this exercise. This caused several issues. First was that most of the players were using different technologies that made it difficult for the teams to coordinate back to the Incident Commander. On one sortie, a community assessment survey was established in a Groove workspace. The problem was that the Incident Command Post (ICP) who would need the data for coordination of assets was not using MS Groove but another web based application. The teams in the field had various technologies employed but only certain technologies were being monitored by the ICP or the EOC. Voice not digital was the primary means of communicating vital data to the Decision makers.

A second issue that emerged with the technology was interference and de-confliction. Various mobile Network Operations Centers deployed to the Strong Angel III exercise, each performing their own demonstrations and experiments. Many of these technologies operated on similar frequencies, restricted to unlicensed bands. The

network had to be shut down and restarted from scratch to ensure there was little to no interference.

A third issue that emerged was the use of MS Groove as the major collaborative tool. Over 50% of the packets that were coming over the network came from Groove. As scalability of the network increased, so did the clients in the Groove workspaces. With vendors using Groove to post data on the network and without any guidance, post data simultaneously, the network barely supported itself for the first several hours.

C. TNT EXPERIMENT OBSERVATIONS FOR METRIC REFINEMENT

The TNT experiment provided an excellent opportunity to see how technology can support collaboration within a semi-structured environment.

1. People/Structure

Unlike disaster relief operations, the MDA environment did have a semi-structured organization from start to finish. The Maritime Security Office of the Port of Oakland (played by Sweden) was the main authority in coordination. As in the case of disaster relief, command was transferred from local to state once the complexity increased. In the case of the scenario, the incident commander shifted from the MSO to District 11 with the US Navy supporting District 11 efforts for interdiction. The Boarding Party reported directly to the TOC, who in turn reported to District 11. The collaboration on a peer-to-peer relationship was between the boarding officer and the advisors at the various fusion centers and laboratories participating in the experiment.

2. Technology

There were several technologies employed in the TNT 06-4 experiments. The primary means of voice communication was the Voice-Over-IP (VOIP) telephones. The primary collaborative tool used during the experiment was of course MS Groove. Again, MS Groove did place a significant amount of load on the network. However, since the users were limited in the network, the network was able to support the loads. In addition, the Electronic Wall (or E-wall) which collects alerts from various databases and posts them for watch standers was used both at the District 11 Headquarters and the TOC to provide further situational awareness. Finally, the Situational Awareness Agent (SA Agent), a homegrown product of NPS, interfaces with other agents to provide a visual picture using icons, GPS Data, alert postings, network performance, video feed, and IM capability, was further used by participants to monitor and develop a COP.

VI. CONCLUSIONS

A. CRITERIA ESTABLISHMENT

The environments of Emergency Response and Maritime Domain Awareness are both complex and dynamic environments. Collaborative technologies are great catalysts for transforming both informational and organizational structures from hierarchies into peer-to-peer, ad hoc, and mesh structures that can respond to these complex and dynamic changes. However, there are many technologies to pick from and use. Ensuring that the right tool is selected will certainly help the process.

As such, this thesis provided a baseline for criteria in selecting tools for Tactical level MDA and Emergency Response. Measures of Effectiveness looked at Situational Awareness, Interoperability, Decision Support, Commander's Intent, and Information Sharing. Measures of Performance looked at Scalability, Network Effects, Information Availability, Information Security, Interoperability, and Feasibility. Dimensional Parameters looked at Capability, System Requirements, and Information Security. These

Measures of Merit were derived from extending the NATO COBP for C2 Assessment methodology into the MDA Awareness and Emergency Response Relief Operations, both fields not normally associated with NATO. The NATO COBP provides a methodology for establishing criteria that can be used to select the tool operating in a dynamic and complex environment. It looks not only at Measures of Performance, or technical aspects of the tool, but also the social, cognitive, and informational networks needed to achieve mission results. It currently is being used to assess

technology being used in Military Operations Other Than War.

B. THE FUTURE ROLE OF COLLABORATIVE TOOLS

Ad hoc organizational and informational structures are the best types of social and information networks suited for these types of environments. Discussion boards, file sharing, and collaborative chat capabilities offered by companies will become much more needed for these organizations to develop into those architectures. At the same time, people need to be taken into account. If personnel do not want to use the tool, the tool can either be abandoned, as was the case with MS Groove during the Strong Angel III Demonstration, or a tool for micro-management in a hierarchical organization.

As the demand for file sharing, application sharing, and instant messaging tools becomes needed for those transformations to take place, the supply will also increase to meet this demand. More than ever, analysts must ask questions and create the right criteria to evaluate the tools that are being approached into this scenario.

LIST OF REFERENCES

Bordetsky, Alex, et. al. Progress Report on the NJ Emergency Response Network, May 2006.

Bordetsky, Alex, et. al. TNT 06-3 MIO Plan, Scenario, March 2006.

Collins, Thomas, Admiral, USCG, "Collaboration: The Path to Maritime Domain Awareness Success," June 2005.

Department of Homeland Security, National Plan to Achieve Maritime Domain Awareness, October 2005.

Defense Information Systems Agency, NCES Critical Comments, 9 December 2005.

http://www.nimsonline.com, Official NIMS training website, Communications and Information Management Session, 10 June 2006.

National Security Presidential Directive NSPD-41, 21 December 2004.

National Strategy for Maritime Security, Department of Homeland Security, September 2005.

OSD-C4I, DOD Standard Collaborative Tool Implementation Overview, GENADMIN, 101431ZAUG2001.

Net-Centric Enterprise Services Statement of Objectives, Defense Information Systems Agency, 9 December 2005.

Rideout, Brian, et. al. TNT 06-4 MIO Plan, Scenario, June 2006.

SAS-026. NATO COBP for C2 Assessment, CCRP, 2002.

Wiliker, Phil, C2 Division, NORTHCOM, Phone Conversation, 2 February 2006.

www.strongangel3.net/about, Official Strong Angel III Disaster Relief Integration Exercise website, 14 June 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Stan Patty, Directorate of Experimentation, Joint Transformation Command – Intelligence
   Joint Forces Command (USJFCOM)
   Norfolk, VA

4. Phil Wiliker, C2 Division
   US Northern Command (USNORTHCOM)
   Colorado Springs, CO

5. Alex Bordetsky, Ph.D.
   Naval Postgraduate School
   Monterey, California

6. Susan Higgins
   Naval Postgraduate School
   Monterey, California

7. Dan C. Boger
   Naval Postgraduate School
   Monterey, California