NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

FROM THE BATTLEFIELD TO THE HOMELAND: BUILDING THE CASE FOR NETWORK-CENTRIC RESPONSE

by

Michael C. Peterson

March 2007

Thesis Advisor:	Richard Bergin
Second Reader:	Houston Polson

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2007	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE From the Battlefield to the Homeland: Building the Case for Network-Centric Response	5. FUNDING NUMBERS
6. AUTHOR CDR Michael C. Peterson, USN	

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 A

13. ABSTRACT (maximum 200 words)

Our nation's ability to respond to natural or man-made disasters has remained relatively unchanged since the attacks of 9/11. Current response operations are characterized by the inability to efficiently produce a collaborative and effective response to incidents of national significance and address the challenges of the Information Age. The military has adapted network-centric tenants and principles from business applications to effectively operate in the Information Age and increase mission effectiveness. These tenants and principles can be adapted by responders to address current deficiencies and increase mission effectiveness. Implementation of "network-centric response" is both technologically and organizationally feasible. Network-centric response operations would allow responders to meet the challenges and leverage the opportunities of the Information Age, resulting in increased mission effectiveness.

14. SUBJECT TERMS Homeland security, Network-centric operations, Information systems technology, Response, Information Age, Interoperability, Information sharing, Knowledge superiority, Situational awareness, Collaboration, Sensemaking, Decision making, Self-synchronization	15. NUMBER OF PAGES 217
	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

FROM THE BATTLEFIELD TO THE HOMELAND:
BUILDING THE CASE FOR NETWORK-CENTRIC RESPONSE

Michael C. Peterson
Commander, United States Navy
B.S., United States Naval Academy, 1990

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2007

Author: Michael C. Peterson

Approved by: Mr. Richard Bergin
               Thesis Advisor

               Mr. Houston Polson
               Second Reader

               Professor Douglas Porch
               Chairman, Department of National Security
               Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Our nation's ability to respond to natural or man-made disasters has remained relatively unchanged since the attacks of 9/11. Current response operations are characterized by the inability to efficiently produce a collaborative and effective response to incidents of national significance and address the challenges of the Information Age. The military has adapted network-centric tenants and principles from business applications to effectively operate in the Information Age and increase mission effectiveness. These tenants and principles can be adapted by responders to address current deficiencies and increase mission effectiveness. Implementation of "network-centric response" is both technologically and organizationally feasible. Network-centric response operations would allow responders to meet the challenges and leverage the opportunities of the Information Age, resulting in increased mission effectiveness.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AWACS   Air Warning and Control System

C2   Command and Control

CAOC   Combined Air Operations Center

CoI   Communities of Interest

COP   Common Operational Picture

CORP   Common Operational Response Picture

COTS   Commercial Off-the-shelf

DHS   Department of Homeland Security

DoD   Department of Defense

DSCS   Defense Satellite Communications System

EMAC   Emergency Management Assistance Compact

EMP   Electromagnetic Pulse

EOC   Emergency Operations Center

FDNY   Fire Department, New York

FEMA   Federal Emergency Management Agency

GBS   Global Broadcast Service

GOTS   Government Off-the-shelf

GPS   Global Positioning System

HSPD   Homeland Security Presidential Directive

IC   Intelligence Community

ICS   Incident Command System

IP   Internet Protocol

JFO   Joint Field Office

JTF   Joint Task Force

JTRS   Joint Tactical Radio System

NCW   Network-Centric Warfare

NIMS   National Incident Management System

NRP   National Response Plan

NYPD   New York Police Department

PAPD	Port Authority Police Department
RF	Radio Frequency
SAR	Search and Rescue
SOP	Standard Operating Procedure
UAS	Unmanned Aircraft System (formerly called UAV)
UAV	Unmanned Aerial Vehicle
UDOP	User-defined Operational Picture
USNORTHCOM	United States Northern Command
VOIP	Voice Over Internet Protocol
WGS	Wideband Gapfiller System
WMD	Weapon of Mass Destruction
WTC	World Trade Center

ACKNOWLEDGMENTS

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> September 11, 2001, was a day of unprecedented
> shock and suffering in the history of the United
> States. The nation was unprepared. At 8:46 on
> the morning of September 11, 2001, the United
> States became a nation transformed.[1]
>
> *- The 9/11 Commission Report*

Much of the post-9/11 transformation has focused on
the nation's ability to respond to attacks that occur
despite our best efforts to prepare for and prevent attacks
on the homeland. There have been no significant man-made
attacks that have reached the homeland since 9/11, although
several have been disrupted and terrorist groups are
actively seeking new ways to attack the United States and
our allies. Nonetheless, unpreventable natural disasters,
in the form of wildfires and a series of hurricanes,
cumulating with the landfall of Hurricane Katrina on August
29, 2005, have caused significant destruction and suffering
domestically. Natural disasters that feature large
geographic footprints and powerful destructive effects will
continue to occur in the future. Eventually, our efforts
to deter and prevent man-made attacks will fail. When
acknowledging these factors, coupled with the ongoing
pursuit of and advancements in weapons of mass destruction
(WMD) technology by non-state terrorist organizations and
their state sympathizers, the United States should expect

---

[1] National Commission on Terrorist Attacks Upon the United States
(The 9/11 Commission), *The 9/11 Commission Report - Final Report of the
National Commission on Terrorist Attacks upon the United States -
Executive Summary* (Washington DC: U.S. Government Printing Office,
[2004], 1).

its ability to respond to the effects of disasters of national significance, regardless of origins, to be tested repeatedly for the foreseeable future.

A. A MANDATE FOR A COLLABORATIVE NATIONAL APPROACH TO INCIDENT MANAGEMENT

In the years following the attacks of 9/11, the President issued several Homeland Security Presidential Directives (HSPDs) to provide strategic guidance for our nation to be able to better deal with the new threats of a post-9/11 world. Among the directives issued were HSPD-5, whose stated purpose is "to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system" and HSPD-8, whose stated purpose is to establish "policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities."[2]

---

[2] George W. Bush, "Homeland Security Presidential Directive-5, Management of Domestic Incidents" www.fas.org/irp/offdocs/nspd/hspd-5.html (accessed January 29, 2006), 1; George W. Bush, "Homeland Security Presidential Directive-8, "National Preparedness"," www.fas.org/irp/offdocs/nspd/hspd-8.html (accessed January 29, 2006),1.

1. A Comprehensive Approach: The National Response Plan and the National Incident Management System

HSPD-5 states as its policy, "To prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive approach to domestic incident management. The objective of the United States Government is to ensure that all levels of government across the Nation have the capability to work efficiently and effectively together, using a national approach to domestic incident management."[3] HSPD-5 led to the development of the National Response Plan (NRP) and the National Incident Management System (NIMS) that detail how to respond to disasters on strategic and tactical levels respectively. Despite the publication of these documents, individual states, counties, and major metropolitan areas differ on their level of NIMS compliance. Tactical execution of response plans often varies even among entities within the same metropolitan area. These practices result in a lack of synergy in response among tenant response agencies, the inability to organize and coordinate an effective, non-redundant response effort, and inefficiencies in the efforts of supporting agencies, whether neighboring states or federal entities, to provide assistance due to incompatibility of equipment and procedures as evidenced by the response efforts from 9/11 through Hurricane Katrina. According to the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, "Local first responders were largely overwhelmed and unable to perform their duties, and

---

[3] Bush, *Homeland Security Presidential Directive-5, "Management of Domestic Incidents"*, 1.

the National Response Plan did not adequately provide a way for federal assets to quickly supplement or, if necessary, supplant first responders."[4] While these documents have established a framework for a single, comprehensive national incident management system, they fail to discuss the specific processes, tactics, techniques, procedures, and methodology to be used to achieve a collaborative and unified effort within the NRP and NIMS framework.

2.   Standardization and Interoperability

HSPD-8 is a companion to HSPD-5, which "identifies steps for improved coordination in response to incidents."[5] HSPD-8 states that "The Secretary [of Homeland Security], in coordination with State and local officials, first responder organizations, the private sector and other Federal civilian departments and agencies, shall establish and implement streamlined procedures for the ongoing development and adoption of appropriate first responder equipment standards that support nationwide interoperability and other capabilities consistent with the national preparedness goal…."[6] The lack of communications interoperability remains a subject of intense debate as individual States and communities seek independent solutions to their communications problems. The National Interoperability Baseline Survey, release by SAFECOM in

---

[4] Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina* (Washington DC: U.S. Government Printing Office, [February 15, 2006]), 1.

[5] Bush, *Homeland Security Presidential Directive-8, "National Preparedness"*, 3.

[6] Ibid.

December 2006, states that, "longstanding obstacles to interoperability, including turf battles, lack of funding and political will for the development of shared radio communications systems, lack of common standards, and shortfalls in spectrum available to public safety, continued to hamper public safety communications. Over the years [since a 1998 National Institute of Justice Interoperability Study], as these obstacles were addressed, lack of interoperability continued to result in the unnecessary loss of lives and property. As the catastrophic event of September 11, 2001 showed the entire Nation, direct correlation exists between effective communications interoperability and first responders' ability to save lives."[7]

Interoperable communications leading to the ability to provide uninterrupted flow of critical information among responding multi-disciplinary and multi-jurisdictional agencies at all levels of government, is a priority capability.[8] "Communications interoperability underpins the ability of federal, state, local, and tribal entities to work together effectively to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies."[9] Systems "stove piping" is not limited to just communication systems but is pervasive throughout all types of first response systems

---

[7] Department of Homeland Security, *2006 National Interoperability Baseline Survey* (Washington DC: SAFECOM, Department of Homeland Security,[2006]), http://www.safecomprogram.gov/SAFECOM/library/background/1295_2006natio nal.htm (accessed December 11, 2006), 2.

[8] Department of Homeland Security, *National Preparedness Guidance* (Washington DC: DHS, [2005]) (accessed June 16, 2006).

[9] Ibid., 30.

and responder procedures. This practice works in direct opposition to National Preparedness Guidance target capabilities of expanded regional collaboration, strengthening information sharing and collaboration capabilities and strengthening interoperable communications capabilities to enable personnel from different disciplines and jurisdictions to communicate, share information, and collaborate effectively during the response to a major event.[10]

Almost four years passed between the terrorist attacks of 9/11 and the landfall of Hurricane Katrina in the Gulf region. During this period, several measures have been implemented in an attempt to improve this nation's ability to respond to disasters of national significance. Initiatives include, the creation of the Department of Homeland Security (DHS) and a new Secretary; the standup of a new military combatant command, United States Northern Command, whose mission set includes Defense Support of Civil Authorities who are tasked with responding to domestic disasters; the issuance of fourteen Homeland Security Presidential Directives; the formulation and implementation of a National Incident Management System; development and publication of numerous National Strategy Documents, including the National Strategy for Homeland Security and the Strategy for Homeland Defense and Civil Support; and the publication of the National Response Plan. Despite these efforts directed at increasing our nation's homeland security in the areas of prevention, preparedness, response, and recovery and accomplishing the strategic objective to minimize the damage and recover from attacks

---

[10] Department of Homeland Security, *National Preparedness Guidance* (Washington DC: DHS, [2005]) (accessed June 16, 2006).

that occur, our nation's ability to respond to natural or man-made disasters has remained relatively unchanged since the attacks of 9/11.[11]

3. Analog Response in a Digital World

Recent analysis of the attacks of 9/11 specifically states that transferability of information for the purpose of reducing human exposure to the attacks, and hence its consequences, was extremely limited by the capacity and compatibility of communication networks in spite of the fact that facilities were made available to support expanded capacity. Information transfer is a vital dimension of emergency services, and more attention is needed in this area.[12]

---

[11] United States Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters* (Washington DC: GAO,[2006]) (accessed June 3, 2006); George W. Bush, "National Strategy for Homeland Security," *Washington, DC: The White House, July* (2002), 1-72 (accessed December 9, 2006); Federal Emergency Management Agency, *Summary of Post 9/11 Reports "Lessons Learned"* (Washington DC: Federal Emergency Management Agency,[2002]) (accessed November 27, 2006); United States Conference of Mayors, *Five Years Post 9/11, One Year Post Katrina: The State of America's Readiness* (Washington DC: The U.S. Conference of Mayors,[2006]) (accessed November 27, 2006); Keith Bea, *Emergency Management Preparedness Standards: Overview and Options for Congress* (Washington DC: Congressional Research Service,[2004]) (accessed November 27, 2006); Richard Grimmett, *Terrorism: Key Recommendations of the 9/11 Commission and Recent Major Commissions and Inquiries* (Washington DC: Congressional Research Service,[2004]) (accessed November 27, 2006); First Response Coalition, *A Failure to Communicate: A Stocktake of Government Inaction to Address Communications Interoperability Failures Following Hurricane Katrina* (Washington DC: The First Response Coalition,[2005]) (accessed November 30, 2006); United States Government Accountability Office, *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System* (Washington DC: GAO,[2006]) (accessed November 14, 2006).

[12] Rae Zimmerman, "Public Infrastructure Service Flexibility for Response and Recovery in the Attacks at the World Trade Center, September 11, 2001," Institute for Civil Infrastructure Systems, Wagner Graduate School of Public Service, New York University, http://www.colorado.edu/hazards/sp/sp39/sept11book_ch9_zimmerman.pdf (accessed February 12, 2006).

The Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina listed among the finding in their final report "massive communications damage and a failure to adequately plan for alternatives impaired response efforts, command and control, and situational awareness. Massive inoperability had the biggest effect on communications, limiting command and control, situational awareness, and federal, state, and local officials' ability to address unsubstantiated media reports."[13]

Even though inoperability severely affected response operations in the wake of Katrina's destruction, equipment incompatibility remained an issue four years after the attacks of 9/11. As stated in the Federal Response to Hurricane Katrina Lessons Learned, "Although Federal, State, and local agencies had communications plans and assets in place, these plans and assets were neither sufficient nor adequately integrated to respond effectively to the disaster. Many available communications assets were not utilized fully because there was no national, State-wide, or regional communications plan to incorporate them."[14] "Federal, State, and local governments have not yet completed a comprehensive strategy to improve operability and interoperability to meet the needs of emergency responders. This inability to connect multiple communications plans and architectures clearly impeded coordination and communication at the Federal, State, and

---

[13] Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, 3.

[14] The White House, "The Federal Response to Hurricane Katrina: Lessons Learned," (February 23, 2006), 55.

local levels. A comprehensive, national emergency communications strategy is needed to confront the challenges of incorporating existing equipment and practices into a constantly changing technological and cultural environment."[15]

The results of the 2006 National Interoperability Baseline Survey reinforce the fact that the nation has yet to achieve acceptable levels of interoperability for response operations. According to the survey, "Strategic plans for interoperability are the exception rather than the norm. Only 20 percent of agencies have strategic plans to ensure interoperability across disciplines, and 19 percent have plans to ensure interoperability across jurisdictions."[16] About half of all agencies either do not use Standard Operating Procedures (SOPs) or rely on informal SOPs to support interoperable communications.[17] Only 37 percent of primary wireless communications systems used by first responders are multi-agency, multi-jurisdictional, shared systems and 58 percent of all systems are limited to analog communications.[18] The inability to communicate and share information effectively within and among organizations remains critical to the ability to respond effectively to disasters.

The attacks of 9/11 caused the country to reevaluate its ability to respond to disasters of national significance. Despite sweeping organizational changes at

---

[15] Ibid., 56.

[16] Department of Homeland Security, *2006 National Interoperability Baseline Survey*, 23.

[17] Ibid.

[18] Department of Homeland Security, *2006 National Interoperability Baseline Survey*, 23.

the Federal, State, and local level; massive funding of homeland security initiatives; and national attention, the response to Hurricane Katrina demonstrated that agencies continue to suffer from the inability to communicate, share information, and produce a collaborative effort that characterized to response to the attacks of 9/11. The failure of local, State, and Federal governments to respond more effectively to Katrina, which had been predicted in theory for many years, and forecast with startling accuracy for five days, demonstrates that whatever improvements have been made to our capacity to respond to natural or man-made disasters, more than five years after 9/11, we are still not fully prepared despite significant emphasis and funding.[19] "The preparation for and response to Hurricane Katrina show we are still an analog government in a digital age. We must recognize that we are woefully incapable of storing, moving, and accessing information, especially in times of crisis."[20] This is an indicator that, unlike business and military operations, our nation's response operations and methodologies have failed to evolve to account for the new challenges present in the Information Age.

B.   RESEARCH PROBLEM

"National emergency response is a strategic problem, and at the strategic level, thought should always precede

---

[19]   Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, 1-364.

[20]   Ibid.

action. Spending money without an overarching systems architecture and a comprehensive acquisition program will be both wasteful and counterproductive."[21]

Our current response operations are characterized by the inability to efficiently produce a collaborative and effective response to incidents of national significance and address challenges of Information Age.

Efficiency in response refers to the extent to which maximum output is achieved from a given input, or minimum input for a given output. Collaboration, in this context, is defined as a mutually beneficial, well-defined effort between and among entities through which they work together to achieve common goals. The collaborative process involves individuals, organizations, and systems working together, but at a significantly higher degree than through the individual pursuit of common goals that characterizes current response operations.

The Information Age is defined as the current stage in societal development which began to emerge at the end of the twentieth century, after approximately 1970, and followed the Industrial Age. This period is marked by the increased production, transmission, consumption of, and reliance on information. Challenges in this age are derived from our capability to collect, process, disseminate, and utilize information. "Despite considerable advances in our ability to process information, these advances have not been rapid enough to keep pace with the increases in collection. Humans are

---

[21] J. J. Carafano, "Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century," *Heritage Lectures*, no. 812 (2003), 1 (accessed November 27, 2006), 1.

still required to make sense of what is collected. That
will remain the case for sometime to come."[22] The ability
to access useful information on the intended subject,
anywhere, anytime, remains an ongoing challenge, especially
when attempting to complete time-critical tasks with high-
stakes consequences such as those encountered in response
operations.

"Technology is bridging distances and providing the
capability for individuals to be able to interact with each
other in increasingly sophisticated ways, making it easier
for individuals and organizations to share information, to
collaborate on tasks, and to synchronize actions or
effects. But technological advances alone do not define
the Information Age."[23] Of ultimate importance is what is
being done with these newly provided technical
capabilities: enabling individuals and organizations to
create value in new ways.[24]

1.   The Four Basic Tasks

Numerous official after-action reports of the response
operations following the attacks of 9/11 and disasters
leading up to and including the response to Hurricane
Katrina highlight weaknesses in the ability to effectively
access and share information, voice or data, in the
national response infrastructure that have permeated
response operations and the resulting effects on mission

---

[22] D. S. Alberts and others, *Understanding Information Age Warfare*
(Washington DC: DoD Command and Control Research, 2001), 44.

[23] Ibid., 44-45.

[24] Ibid.

accomplishment.[25]   The various Federal, State, and local entities that were charged with responding to significant disasters, whether man-made or natural, that impacted their jurisdiction suffered from the inability to perform the four basic tasks required to accomplish their mission in the Information Age.

The four basic tasks are:

1)   The ability to make sense of the situation;

2)   The ability to work in a interagency collaborative environment;

3)   Possession of the appropriate means to respond; and

4)   The ability to orchestrate the means to respond in a timely manner.[26]

The existence and employment of interoperable and effective voice and data communications and the use of

---

   [25] Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, 1-364; United States Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters*, 1-68; National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report* (Washington DC: National Commission on Terrorist Attacks upon the United States,[2004]); The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 1-217; Federal Emergency Management Agency, *Summary of Post 9/11 Reports "Lessons Learned,"* 1-23; United States Conference of Mayors, *Five Years Post 9/11, One Year Post Katrina: The State of America's Readiness*, 1-12; Bea, *Emergency Management Preparedness Standards: Overview and Options for Congress*, 1-22; Grimmett, *Terrorism: Key Recommendations of the 9/11 Commission and Recent Major Commissions and Inquiries*, 1-38; United States Fire Administration, *Four Years Later - A Second Needs Assessment of the U.S. Fire Service* (Washington DC: Department of Homeland Security, [2006]) (accessed November 23, 2006).

   [26] D. S. Alberts and R. E. Hayes, *Power to the Edge: Command...Control...in the Information Age* (Washington DC: DoD Command and Control Research, 2003), 98.

compatible technology for information sharing directly
affect all but the third of the four basic tasks required
to effectively operate in the Information Age. Possession
of the appropriate means to respond to disasters has more
to do with core mission planning, manning, funding,
training, and equipment procurement than a specific
requirement for information sharing through connectivity
and networking.   However, a high degree of shared
situational awareness and network and communications
connectivity will allow decision makers to identify which
organizations, units, or individuals possess the
appropriate means to respond (i.e., force or equipment
capability combined with the ability to apply these assets
in time and space based on their geographic position
relative to when and where they are needed). Even if a
particular organization lacks the appropriate means to
respond, they can request assistance from an interagency
partner who possesses the appropriate capabilities and can
be quickly identified and directed to assist in the
response.

C.   RESEARCH QUESTION

Can network-centric operations be employed by response
agencies at all levels of government to allow them to
accomplish the four basic tasks required to operate in the
Information Age?   If so, will this lead to improved
response mission effectiveness?

1. Network-Centric Operations

Given the complex and demanding requirements of responding to a determined, protracted, and potentially catastrophic terrorist threat, the fundamental requirement of an effective national response system may be to adopt a "system of systems" or network-centric approach to emergency preparedness.[27] "Network-centric operations generate increased operational effectiveness by networking sensors, decision makers, and emergency responders to achieve shared awareness, increased speed of command, higher tempo of operations, greater efficiency, increased security and safety, reduced vulnerability to potential hostile action, and a degree of self-synchronization. In essence, this means linking knowledgeable entities in the response to emergencies from the local to the national level."[28] "Such a system might produce significant efficiencies in terms of sharing skills, knowledge, and scarce high-value assets, building capacity and redundancy in the national emergency response system, as well as gaining the synergy of providing a common operating picture to all responders and being able to readily share information. Network-centric systems might be especially valuable for responding to large-scale or multiple WMD attacks, where responders will have to surge capacity quickly, adapt to difficult and chaotic conditions, and respond to unforeseen requirements."[29]

---

[27] Carafano, *Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century*, 6.

[28] Ibid., 6-7.

[29] Carafano, *Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century*, 7.

2. Measurement of Effectiveness

Measurable criteria are critical to assessing the impact of adapting network-centric principles to response operations. Response agencies' ability to complete the four basic tasks required to accomplish their mission in the Information Age should be evaluated by assessing the measures of effectiveness listed in Table 1.

Basic Tasks	Measures of Effectiveness
The ability to make sense of the situation	Individual Situational Awareness
The ability to work in a interagency collaborative environment	Ability to Effectively Access and Share Information
Possession of the appropriate means to respond	Collective Situational Awareness
The ability to orchestrate the means to respond in a timely manner	Self-synchronization and Speed of Command and Decision Making

Table 1.   Response Elements to be Evaluated

The specific metrics to evaluate each element will be discussed at the end of Chapter V.

D.   SIGNIFICANCE TO RESPONSE OPERATIONS

On the most basic level, we need to take a step back and focus on the fundamental question: Why was the Department of Homeland Security created? It was not created merely to bring together different agencies under a single tent. It was created to enable these agencies to secure the homeland through joint, coordinated action. Our challenge is to realize that goal to the greatest extent possible.

- Secretary of Homeland Security Michael Chertoff
Statement for the Record before the United States
Senate Subcommittee on Homeland Security
April 20, 2005.[30]

The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina implicitly cites the need to improve response capabilities that could be addressed by implementation of network-centric operations.[31] The continued massive funding of incremental change that has characterized the years since 9/11 will not produce significant improvements in our nation's ability to respond to incidents of national significance and to deal with the challenges of the Information Age. Just as other disciplines (e.g., business corporations and the military) have adapted to the 21st Century, emergency response operations and agencies require a transformational change to adapt to the challenges of the Information Age and leverage it opportunities.

While network-centric operations tenants, principles, and technology have the potential to be effectively applied to enhance the efforts of Federal, regional, State, and local personnel in both the areas of prevention and response, this thesis will be limited to the area of response. The area of response was chosen because responders must manage the effects of time pressure and

---

[30] Secretary Chertoff as quoted in Peter Kind and Katharine Burton, *Information Sharing and Collaboration Business Plan* (Alexandria, Virginia: Institute for Defense Analyses, [2005]) (accessed November 27, 2006).

[31] Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, 1-364.

completeness of information while making decisions and taking action to prevent loss of life and property.

Prevention, like deterrence, is a difficult discipline to assess using metrics. Did an attack fail to occur due to prevention or did other factors come into play? Response can and has been assessed by both congressional committees and first responder communities themselves. The results of these assessments are well-documented and are suitable for scholarly analysis. The documentation of deficiencies in current response operations must be accomplished to determine if the benefits of network-centric operations can be used to fill current gaps in response.

Case studies of efforts in response to the attacks of 9/11 in New York City and the effects of Hurricane Katrina throughout the Gulf region should provide specific details of historical and current inefficiencies and deficiencies in response. The two main case studies were selected to benchmark the recent evolution of response capability for several reasons: date of occurrence, footprint of the disaster's effects, and scope of response. The dates of these two disasters span a significant period of four years that has included significant efforts to better equip this nation to prepare for and respond to national disasters. Simply, they form bookends that represent an awakening in national attention to the problem of terrorism and dealing with its consequences and the accumulation four years of this nation's efforts to increase its ability to respond to significant disasters, regardless of their source. The contrast in the footprint and scope of response to each disaster is used to show the consistencies in deficiencies

in the ability to gain and maintain situational awareness, work in an interagency collaborative environment, and to orchestrate the means to respond in a timely manner. The attacks of 9/11 in New York were confined to a relatively small area, the World Trade Center complex, and were responded to by one of the largest, best-equipped and prepared first responder communities in the nation. The initial damage mechanism and loss of life occurred over the period of a few hours. Hurricane Katrina's effects were distributed over several states and involved a significant federal contribution to response operations to support the efforts of responders from several diverse states and municipalities. Its effects took days to manifest themselves and the loss of life continued for several days. The lasting effects and recovery phase of each event continue to this day.

Once current deficiencies are documented, it is essential to establish the applicability and benefit of network-centric operations tenants, principles, and technology to response operations. A detailed examination of how the military has adapted network-centric operations from the business world and is effectively applying its tenants and principles to the conduct of warfare will demonstrate the benefits of adopting network-centric operations to achieve positive transformational change. The strengths of network-centric warfare will be aligned with the deficiencies in current response operations to present a convincing value proposition for the adaptation of network-centric tenants, principles, and technology to establish a new methodology of performing response operations as a nation: network-centric response.

Determining the applicability of network-centric response to increase the capability of Federal, State, regional and local personnel in responding to an incident of national significance requires the definition of clearly articulated outcomes in a defined context. The defined context of the increased capability will be the four basic tasks to operate in the Information Age. The clearly articulated outcomes to be measured will be derived from the existing network-centric operations conceptual framework that includes: quality of organic information, quality of individual information, quality of individual sensemaking, quality of individual decisions, quality of networking, degree of information sharing, quality of interactions, degree of shared sensemaking, quality of collaborative decisions, degree of decision synchronization, and degree of action/entities synchronized as they contribute to the overall degree of effectiveness of response.[32]

Once the applicability of network-centric operations to response is established, the challenges of a credible implementation strategy must addressed to include the technical and organizational feasibility of making the transformational, vice incremental, evolution of national response to a network-centric based approach. Implementation should be guided by a specific set of core values to ensure that network-centric tenants and principles are correctly adapted to response operations as

---

[32] D. S. Alberts and J. J. Garstka, "Network Centric Operations Conceptual Framework Version 2.0," *U.S. Office of Force Transformation and Office of the Assistant Secretary of Defense for Networks and Information Integration (2004)* (accessed October 2, 2006).

intended while avoiding potential bureaucratic appropriation and exploitation. Core values represented include:

- **Empowerment** - of responders at all levels in the social, cognitive, information and physical domains of response.[33] Most response operations involve a local lead that is reinforced at the State, regional and Federal levels. All levels of response organizations must understand their roles and be employed effectively to sustain a decisive unity of effort and make decisions at the lowest level possible.

- **Service** – through a dedication to mission accomplishment by placing the welfare of our fellow citizens above our own without the expectation of recognition or personal gain.

- **Transparency** - of operations and decision making at all levels to reinforce trust and coordination among disparate agencies that represent various levels of government and the private sector.

- **Speed** - of understanding and decision making. The preservation of life and infrastructure in the immediate aftermath of a catastrophic event has a significant temporal component. Proper naturalistic decision making processes rely on

---

[33] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare* (Washington DC: Director, Force Transformation, Office of the Secretary of Defense, [January 5, 2005]).

rapid assimilation of the situation and an effective application of human and material resources.

- *Agility* – characterized by the ability of response forces, supporting agencies, and decision makers to be robust, flexible, responsive, innovative, resilient, and adaptive in a dynamic environment.

- *Teamwork* - through synchronization of individual assets to contribute to the collective response effort. Self-synchronization increases value of individual initiative to produce a meaningful increase in operational tempo and responsiveness and allows rapid adaptation to dynamic events as they unfold.[34]

If network-centric operational theory holds true, a robustly networked team of interagency responders will improve information sharing; information sharing will enhance the quality of information and shared situational awareness; shared situational awareness will enable collaboration and self-synchronization, which enhances sustainability and speed of command and decision making. These, in turn, will dramatically increase response mission effectiveness.[35]

---

[34] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare* (Washington DC: Director, Force Transformation, Office of the Secretary of Defense, [January 5, 2005]).

[35] Adapted from the benefits of network-centric warfare contained in Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare* (Washington DC: Director, Force Transformation, Office of the Secretary of Defense, [January 5, 2005]).

II. DOCUMENTED DEFICIENCIES IN RESPONSE

> It is a fair inference, given the differing situations in New York City and Northern Virginia, that the problems in command, control, and communications that occurred at both sites will likely recur in any emergency of similar scale. The task looking forward is to enable first responders to respond in a coordinated manner with the greatest possible awareness of the situation.[36]
>
> *- The 9/11 Commission Report*

> Insufficient planning, training, and interagency coordination are not problems that began and ended with Hurricane Katrina. The storm demonstrated the need for greater integration and synchronization of preparedness efforts, not only throughout the Federal government, but also with the State and local governments and the private and non-profit sectors as well.[37]
>
> *- The Federal Response to Hurricane Katrina: Lessons Learned*

The current deficiencies in response that prevent individual responders and organizations from completing the four basic tasks to accomplish their mission in the Information Age can broken down into the areas of communications, information sharing, situational awareness, collaboration, and establishment of a unified command. The lack of interoperability affects each of these areas.

Interoperability in response has two distinct components. The first refers to the ability of voice and

---

[36] National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 315.

[37] The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 50.

data systems, software applications, and networks to seamlessly exchange data in a way that it remains timely, accurate, consistent, and useful to response agencies and decision makers. The second component of interoperability involves the ability of response agency forces to exchange equipment and services, through standardized techniques and procedures, without experiencing a reduction in the capability to perform their intended mission as a result of the exchange.

A.   COMMUNICATIONS

Communications interoperability refers to the ability of first responders to communicate to exchange voice and data information on demand, in real time, when needed, and as authorized. When interoperability is fully realized, police, firefighters, emergency medical personnel and supporting agencies are able to communicate seamlessly to coordinate efforts during a routine incident, disaster situation, or special event.[38] After-action reviews of the response efforts to major disasters during the period from the attacks of 9/11 through the response to Hurricane Katrina cite numerous deficiencies in our response efforts

---

[38] Department of Homeland Security, *2006 National Interoperability Baseline Survey*, 2.

in the areas of interoperable and effective voice and data communications and the use of compatible technology.[39]

> The lack of interoperable wireless communications systems is an issue that continues to affect public safety agencies in communities across the county. In many cases, agencies are unable to communicate or share critical voice and data information with other jurisdictions or disciplines during major events or even in day-to-day operations. The procurement and employment of interoperable communications, the ability to provide uninterrupted flow of critical information among responding multi-disciplinary and multi-jurisdictional agencies at all levels of government, is a priority capability. Communications interoperability underpins the ability of Federal, State, local, and tribal entities to work together effectively to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Analysis of State and Urban Area Homeland Security Strategies, in addition to a number of reports on the status of interoperable communications, reflects persistent shortfalls in achieving interoperability.[40]

According to a 2006 Department of Homeland Security report, most first responders in the country use analog communications systems and the majority of those systems

---

[39] United States Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters*, 1-68; Federal Emergency Management Agency, *Summary of Post 9/11 Reports "Lessons Learned*," 1-23; United States Conference of Mayors, *Five Years Post 9/11, One Year Post Katrina: The State of America's Readiness*, 1-12; Bea, *Emergency Management Preparedness Standards: Overview and Options for Congress*, 1-22; First Response Coalition, *A Failure to Communicate: A Stocktake of Government Inaction to Address Communications Interoperability Failures Following Hurricane Katrina*, 1-5; United States Government Accountability Office, *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System*, 1-141.

[40] Department of Homeland Security, *National Preparedness Guidance*, 30.

are more than ten years old.[41]   Despite the presence of
about 11 billion dollars in Department of Homeland Security
grants to bolster communications, these deficiencies in the
ability to effectively communicate lead to break downs in
situational awareness and unity of effort, as characterized
by a lack of information sharing and collaboration among
interagency partners; the inability to establish a unified
command; and, ultimately, a lack overall response mission
effectiveness.[42]

Communications difficulties experienced during the
response to the attacks of 9/11 in New York City include
the lack of integrated communications and unified command
contemplated in the City's Office of Emergency Management
directive; these problems existed both within and among
individual responding agencies.[43]   "For a unified incident
management system to succeed, each participant must have
command and control of its own units and adequate internal
communications.   This was not always the case at the World
Trade Center (WTC) on 9/11."[44]

"The task of accounting for and coordinating the
[police and fire] units was rendered difficult, if not
impossible, by internal communications breakdowns resulting
from the limited capabilities of radios in the high-rise

---

[41]   Department of Homeland Security, *2006 National Interoperability
Baseline Survey*, 1-50.

[42]   Alan Joch, "Communications Breakdown, First Responders Look for
New Ways to Keep Communications Flowing in Emergencies," FCW.com,
http://www.fcw.com/article91601-12-05-05-Print (accessed June 9, 2006).

[43]   National Commission on Terrorist Attacks upon the United States
(The 9/11 Commission), *The 9/11 Commission Report*, 319.

[44]   Ibid.

environment of the WTC and from confusion over which personnel were assigned to which frequency."[45]

The inability of the Fire Department, New York (FDNY) to coordinate and account for the different radio channels that would be used in an emergency of the scale of 9/11 at the WTC contributed to the early lack of units in the South Tower, whose lobby chief initially could not communicate with anyone outside that tower.[46]

Communications difficulties experienced during the response to Hurricane Katrina include a devastated communications infrastructure across the Gulf Coast that featured incapacitated telephone service, police and fire dispatch centers, and emergency radio systems.[47] Almost three million customer phone lines were knocked out, telephone switching centers were seriously damaged, and 1,477 cell towers were incapacitated. Most of the radio stations and many television stations in the New Orleans area were knocked off the air.[48]

"The magnitude of the storm was such that the local communications system wasn't simply degraded; it was, at least for a period of time, destroyed."[49]

---

[45] National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 319.

[46] Ibid.

[47] The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 34.

[48] Ibid.

[49] Assistant Secretary of Defense (Homeland Defense), Paul McHale as quoted in *The Federal Response to Hurricane Katrina: Lessons Learned*, 34.

Equipment interoperability problems further hindered an integrated response. Similar issues of bifurcated operations and interoperability challenges were also present between the military and civilian leadership. This lack of interoperable communications was apparent at the tactical level, resulting from the fact that emergency responders, National Guard, and active duty military use different equipment.[50]

"People could not communicate. It got to the point that people were literally writing messages on paper, putting them in bottles and dropping them from helicopters to other people on the ground."[51]

"There was no voice radio contact with surrounding parishes or State and Federal agencies. Lives were put at risk and it created a direct operational impact on their ability to maintain control of a rapidly deteriorating situation within the city, carry out rescue efforts and control the evacuation of those who had failed to heed the call for evacuation."[52]

The devastation caused by Hurricane Katrina and uncoordinated response that followed reawakened policymakers to the critical need for interoperable communications. Commitments were made by policymakers to fix the problems of incompatibility, limited spectrum for response operations, and system survivability. This was seen as a national problem that required a national

---

[50] The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 43.

[51] Louisiana State Senator Robert Barham, chairman of the State Senate's homeland security committee as quoted in *The Federal Response to Hurricane Katrina: Lessons Learned*, 37.

[52] Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, 1-364.

solution. Similar commitments to first responders were
made following the 9/11 tragedy that initially brought
failure of the emergency communications system to the
nation's attention. Yet, four years later, the same
failures occurred. Grants for systems procurement have
already been made for 2007 without national standards or
additional spectrum being issued. According to the
Tactical Interoperable Communications Scorecards Summary
Report and Findings issued by DHS in January 2007 that
assessed the maturity of tactical interoperable
communications capabilities in 75 urban/metropolitan areas,
more than $2.9 billion in grant assistance has been
provided to State and local agencies for equipment and
other projects to improve communications interoperability
from FY 2003 through FY 2006 alone.[53]

"… Barriers to interoperable communications are both
technical and operational. Each agency typically has its
own unique legacy technologies, requirements, operating
environments, laws, and processes. Therefore, achieving
interoperability requires that, in addition to addressing
technology and disparate communications systems, agencies
examine governance, procedures, training, exercises, and
usage."[54] Until the issues of communications equipment
compatibility through non-proprietary standards, spectrum
allotment for response operations, and deliberate regional

---

[53] Department of Homeland Security, *Tactical Interoperable
Communications Scorecards Summary Report and Findings* (Washington DC:
Department of Homeland Security, [2007]),
http://www.dhs.gov/xlibrary/assets/grants-scorecard-report-010207.pdf
(accessed January 4, 2007).

[54] Ibid.

communications   planning   are   resolved,   responder communications problems will continue for the foreseeable future.

B.   INFORMATION SHARING

Improving   information   sharing   constitutes   a cornerstone of our nation's ability to protect the American people and our institutions and to defeat terrorists and their support networks at home and abroad.[55] The timely and accurate   sharing   of   information   is   also   critical   to performing   response   operations.   The   9/11   Commission identified   a   breakdown   in   information   sharing   as   a   key factor contributing to the failure to predict and prevent the September 11, 2001 attacks on the United States.[56]   The lack of information sharing also contributed to some of the failures in response on that day.

The   role   of   the   information   sharing   environment   in response to increase the quality of organic information, the quality of individual and collective sensemaking, the quality of networking, the degree synchronization, and the number   of   entities   synchronized   in   pursuit   of   social knowledge building.[57]   In this way, data is contextualized and transformed into information, which is in turn shared, interpreted, and socially transformed into knowledge.   As

---

[55] *Information Sharing Environment Implementation Plan* (Washington DC: Office of the Director of National Intelligence, [Program Manager, Information Sharing Environment]) (accessed November 29, 2006).

[56] National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 1-567.

[57] Kind and Burton, *Information Sharing and Collaboration Business Plan*, 8.

this knowledge is developed and integrated, it can be used by individuals and agencies to operate collaboratively.[58]

The inability to share information, either technically, procedurally, or organizationally, will lead to a lack of situational awareness, increased uncoordinated individual actions, delayed response times, and inappropriate responses as demonstrated by the effects of the lack of information sharing in the responses to the attacks of 9/11 and the effects of Hurricane Katrina.

The lack of information sharing experienced during the response to the attacks of 9/11 in New York City includes the inability of the FDNY to coordinate the number of units dispatched to different points within the 16-acre complex. "As a result, numerous units were congregating in the undamaged Marriott Hotel and at the overall command post on West Street by 9:30, while chiefs in charge of the South Tower still were in desperate need of units. With better understanding of the resources already available, additional units might not have been dispatched to the South Tower at 9:37."[59]

"When the South Tower collapsed the overall FDNY command post ceased to operate, which compromised the FDNY's ability to understand the situation; an FDNY marine unit's immediate radio communication to FDNY dispatch that the South Tower had fully collapsed was not conveyed to chiefs at the scene."[60]

---

[58] Kind and Burton, *Information Sharing and Collaboration Business Plan*, 8.

[59] National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 319.

[60] Ibid.

"The command posts were in different locations, and Office of Emergency Management Headquarters, which could have served as a focal point for information sharing, did not play an integrating role in ensuring that information was shared among agencies on 9/11, even prior to its evacuation."[61]

FDNY decision making capability was hampered by a lack of information from New York Police Department (NYPD) aviation:

> At 9:51 A.M., a helicopter pilot cautioned that "large pieces" of the South Tower appeared to be about to fall and could pose a danger to those below. Immediately after the tower's collapse, a helicopter pilot radioed that news. This transmission was followed by communications at 10:08, 10:15, and 10:22 that called into question the condition of the North Tower. The FDNY chiefs would have benefited greatly had they been able to communicate with personnel in a helicopter.[62]

"The FDNY, Port Authority Police Department (PAPD), and NYPD did not coordinate their units that were searching the WTC complex for civilians. In many cases, redundant searches of specific floors and areas were conducted."[63]

The lack of information sharing experienced during the response to Hurricane Katrina includes the fact that "no one had the total picture of the forces on the ground, the

---

[61] National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 319.

[62] Ibid.

[63] Ibid.

forces that were on the way, the missions that had been resourced, and the missions that still needed to be completed."[64]

> Local, State, and Federal officials were forced to depend on a variety of conflicting reports from a combination of media, government, and private sources, many of which continued to provide inaccurate or incomplete information throughout the day, further clouding the understanding of what was occurring in New Orleans. In fact, some uncertainty about the specific causes and times of the breaches and overtoppings persists to this day.[65]

"At least two different locations were assigning search and rescue tasks to military helicopter pilots operating over New Orleans, and no one had the total picture…."[66]

> The Department of Defense (DoD) had difficulty gaining visibility over supplies and commodities when the Federal Emergency Management Agency (FEMA) asked DoD to assume a significant portion of its logistics responsibilities. However, because FEMA lacked the capability to maintain visibility from order through final delivery of the supplies and commodities it had ordered, DoD did not know the precise locations of the FEMA-ordered supplies and commodities when it assumed FEMA's logistics responsibilities. As a result of its lack of visibility over the meals that were in transit, DoD had to airlift 1.7 million meals to Mississippi to respond to a request from

---

[64] United States Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters*, 1-68.

[65] The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 35.

[66] United States Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters*, 1-68.

the Adjutant General of Mississippi, who was concerned that food supplies were nearly exhausted.[67]

DoD possessed information at different classification levels, including critical surveillance and reconnaissance imagery and video products, that was unable to be shared with interagency partners to its storage on a classified system (i.e., SIPRNET).

Despite spending some 50 billion dollars on information technology per year, two fundamental problems have prevented the Federal government from building an efficient government-wide information storage and distribution system. First, government acquisition of information systems has not been routinely coordinated by either the establishment of operating standards or the restricted use of grant money to purchase interoperable equipment. Over time, hundreds of new systems were acquired to address specific agency requirements. Agencies have not pursued compatibility across the Federal government or with State and local entities which has resulted in islands of technology; distinct networks that obstruct efficient collaboration.[68] Second, legal and cultural barriers often prevent agencies from exchanging and integrating information. Information-sharing capabilities are similarly deficient at the State and local levels and require not only interoperable equipment and standards for use, but comprehensive cross-jurisdictional planning efforts.[69]

---

[67] United States Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters*, 1-68.

[68] Bush, *National Strategy for Homeland Security*, 55-56.

[69] Ibid.

C.   SITUATIONAL AWARENESS

Situational awareness is the capability to extract, or operate on, limited cues within a complex environment and use them to construct mental models of complex events that allows appropriate decisions to be made.[70] Making sense of a situation begins with putting the available information about the situation into context and identifying the relevant patterns that exist.   Developing situation awareness has always been a challenge in response operations that feature the same uncertainty that is often referred to in warfare and "fog and friction".   This implies that a 21st century force needs to be robustly networked with information management capabilities that enable widespread information sharing and support collaboration.

Situational awareness goes beyond sharing information and identifying patterns to an understanding of what is currently occurring, what may occur in the future, and what actions can be taken in response. This involves knowledge of the total available response assets, their location, their capabilities, and their current status. Situational awareness allows for understanding the effects of a course of action before deciding on a particular option.

Many first responders that were killed at the WTC on 9/11 suffered from decreased situational awareness. "At least 24 of the at most 32 companies who were dispatched to and actually in the North Tower received the evacuation

_____

[70] D. Paton and J. Violanti, *Psychology of Terrorism*, eds. Bruce Bongar and others (New York, New York: Oxford University Press, 2006), 237.

instruction-either via radio or directly from other first responders."[71]   What was not made clear is that the South Tower had collapsed or that the North Tower was soon to collapse.   "Nevertheless, many of these firefighters died, either because they delayed their evacuation to assist civilians, attempted to regroup their units, lacked urgency, or some combination of these factors.   In addition, many other firefighters not dispatched to the North Tower also died in its collapse."[72]   The 9/11 Commission concluded that the technical failure of FDNY radios, while a contributing factor, was not the primary cause of the many firefighter fatalities in the North Tower.[73]   How much of a role the lack of situational awareness played remains undetermined.   Even with total awareness of the situation, many responders would have chosen to remain to help survivors of the initial attack. What is unclear is if that choice was clearly understood or consciously made by the responders that died that day.

The Federal response to the effects of Hurricane Katrina suffered from significant organizational and coordination problems during the response period.   "The lack of communications and situational awareness had a debilitating effect on the Federal response."[74]

Even after coordinating elements were in place, Federal departments and agencies continued to have difficulty adapting their procedures to this catastrophic

---

[71]   National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 322.

[72]   Ibid.

[73]   Ibid.

[74]   The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 50.

incident.[75]   The storm demonstrated the need for greater integration and synchronization of preparedness efforts, not only throughout the Federal government, but also with the State and local governments and the private and non-profit sectors as well.[76]

Because of poor situational awareness and communications throughout evacuation operations, FEMA had difficulty transporting and delivering food, water, and other critical commodities to people waiting to be evacuated, most significantly at the Superdome.[77]

The Federal government lacked the timely, accurate, and relevant ground-truth information necessary to evaluate which critical infrastructures were damaged, inoperative, or both.   The FEMA teams that were deployed to assess damage to the regions did not focus on critical infrastructure and did not have the expertise necessary to evaluate protection and restoration needs.[78]

"As with Hurricane Andrew, an underlying problem was the failure to quickly assess damage and gain situational awareness."[79]   "The NRP notes that local and State officials are responsible for damage assessments during a disaster, but it also notes that State and local officials could be overwhelmed in a catastrophe.   Despite this incongruous situation, the NRP did not specify the proactive means

---

[75]   The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 50.

[76]   Ibid.

[77]   Ibid., 56-57.

[78]   Ibid., 61.

[79]   United States Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters*, 1-68.

necessary for the federal government to gain situational awareness when State and local officials are overwhelmed."[80]

D.   COLLABORATION

Currently, there is a lack of standardized pre-incident planning and coordination among State and local governments which impedes collaboration and the ability of the Federal government to effectively plan for and support State and local response efforts. "Exasperating this situation, our States and territories has developed fifty-six unique homeland security strategies, as have fifty high-threat, high-density urban areas."[81]

Individual agencies responding to the attacks of 9/11 and the effects of Hurricane Katrina were unable to produce a unity of effort through collaborative action due to a lack of interoperability, communications compatibility, a lack of information sharing, low individual and organizational situational awareness, and the inability to establish a unified command structure.

At the world trade center complex on 9/11, "there was a lack of comprehensive coordination between FDNY, NYPD, and PAPD personnel."[82]   While each organization was

---

[80]   United States Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters*, 1-68.

[81]   The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 67.

[82]   National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 321.

attempting to respond to the attacks within their own context and understanding, little collaboration was achieved.

The response to the effects of Hurricane Katrina involved significantly more agencies and jurisdictions than those charged with responding to the attacks of 9/11. The additional aspect of a significant Federal response also increased the requirement for the various agencies to work in a collaborative manner.

Despite this fact, the DHS did not establish its NRP-specified disaster site multi-agency coordination center, the Joint Field Office (JFO), until after the height of the crisis. Further, without subordinate JFO structures to coordinate Federal response actions near the major incident sites, Federal response efforts in New Orleans were not initially well-coordinated.[83]

The overall military support of civil authorities did not fair much better in the area of collaboration:

> In the overall response to Hurricane Katrina, separate command structures for active duty military and the National Guard hindered their unity of effort. United States Northern Command (USNORTHCOM) commanded active duty forces [through a Joint Task Force], while each State government commanded its National Guard forces. For the first two days of Katrina response operations, USNORTHCOM did not have situational awareness of what forces the National Guard had on the ground. Joint Task Force Katrina (JTF-Katrina) simply could not operate at full efficiency when it lacked visibility of over half the military forces in the disaster area. Neither the Louisiana National Guard nor JTF-Katrina had a good sense for where each other's

---

    83 The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 53.

forces were located or what they were doing. For example, the JTF-Katrina Engineering Directorate had not been able to coordinate with National Guard forces in the New Orleans area. As a result, some units were not immediately assigned missions matched to on-the-ground requirements. Further, FEMA requested assistance from DoD without knowing what State National Guard forces had already deployed to fill the same needs.[84]

To this day, requests for assistance under an Emergency Management Assistance Compact (EMAC) agreement, to include the use of National Guard forces in a Title 32 (non-federalized) status, have no reporting requirements to the Federal government or DoD, which makes the anticipation of Federal requests and allocation of resources to support State and local efforts very difficult.

Several functions were being untaken by individual agencies without knowledge of other agencies' capabilities or efforts. An example of the lack of collaboration among interagency partners is evident in search and rescue operations.

> Lacking an integrated search and rescue incident command, the various agencies were unable to effectively coordinate their operations. This meant that multiple rescue teams were sent to the same areas, while leaving others uncovered. When successful rescues were made, there was no formal direction on where to take those rescued. Too often rescuers had to leave victims at drop-off points and landing zones that had insufficient logistics, medical, and communications resources, such as atop the I-10 cloverleaf near the Superdome.[85]

FEMA personnel are used to acting in an austere environment where resources drive deadlines. Conversely,

---

84 The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 55.

85 Ibid., 57.

DoD sets deadlines, and resources units accordingly. FEMA planners at the tactical level do not understand the magnitude of the assets that DoD can bring to an operation, and thus are hesitant to ask for them. FEMA operators are also tend to submit their requests in terms of what specific assets they desire instead requesting a particular capability or mission to be performed. An example of this is a FEMA request for a Humvee and driver. After being questioned by DoD personnel, it was learned that the vehicle was requested to drive an engineer around New Orleans to measure flood levels which would take all day, given the significant flooding in some areas. By asking for a mission clarification, DoD representatives were able to change the request to one for a helicopter that could complete the time critical task in less than an hour.

Although individual organizations' efforts to respond to the disasters in New York City and the Gulf region were well-intentioned and heroic, they did not produce the synergistic mission results that would have been achieved through effective collaboration.

E.   ESTABLISHMENT OF A UNIFIED COMMAND

It is important to distinguish between Unity of Command, desired by military organizations, and Unified Command, desired by emergency responders and dictated by the NIMS.

Unity of command is the concept by which each person within an organization reports to one and only one

designated person. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective.[86]

Unified command is an application of the Incident Command System (ICS) that is used when there is more than one agency with incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the unified command, often the senior person from agencies and/or disciplines participating in the unified command, to establish a common set of objectives, strategies, plans, priorities, and public communications.[87] For incidents of national significance, the unified command consists of senior officials from multiple levels of government and provides for and enables joint decisions to be made collectively.[88]

"Recognizing that most incidents are managed locally, the command function under the ICS is set up at the lowest level of the response, and grows to encompass other agencies and jurisdictions as they arrive. Some incidents that begin with a single response discipline (e.g., fire or police department) within a single jurisdiction may rapidly expand to multi-discipline, multi-jurisdictional incidents requiring significant additional resources and operational support."[89] "The concept of unified command is both more

---

[86] The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 13.

[87] Ibid.

[88] Ibid.

[89] Ibid.

important and more complicated when local, State, and Federal commanders are required to coordinate their efforts."[90]

The 9/11 Commission specifically stated that "significant shortcomings within the FDNY's command and control capabilities were painfully exposed on September 11."[91] "Effective decision making in New York was hampered by problems in command and control and in its internal communications."[92] At the World Trade Center complex in New York City, "casualties were nearly 100% at and above the impact zones and were very high among first responders who stayed in danger as they tried to save lives. Despite weaknesses in preparations for disaster, failure to achieve unified incident command, and inadequate communications among responding agencies, all but one hundred of the thousands of civilians who worked below the impact zone escaped, often with the help of emergency responders."[93] New York City's first responder communities continue to be some of the largest and best-equipped metropolitan response agencies in the world. Despite their heroic efforts on 9/11, many lives, especially among the first responder communities themselves, were lost due to a lack of network centricity in response infrastructure that was characterized by the inability to communicate, due to

---

[90] The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 13.

[91] National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 320.

[92] Alberts and Hayes, *Power to the Edge: Command...Control...in the Information Age*, 98.

[93] National Commission on Terrorist Attacks Upon the United States (The 9/11 Commission), *The 9/11 Commission Report - Final Report of the National Commission on Terrorist Attacks upon the United States - Executive Summary*, 1-32.

incompatible communications technology and organizational biases; a lack of individual and shared awareness and sensemaking; the inability to effectively and quickly share and access information to build situational awareness; and the inability to establish a unified effort or command.[94] Although responders possessed the means to respond, they failed to complete the other three of the basic tasks required to effectively accomplish their mission when presented with the challenges of the Information Age.

The NIMS and the ICS were established in the period after 9/11 and prior to Hurricane Katrina but were unable to produce the intended unified command structure due to the inability of agencies to communicate or share information. This resulted in the breakdown in situational awareness with prevented a collaborative response and reduced overall emergency response mission effectiveness.

Hurricane Katrina produced significant structural damage to building and significant flooding which combined with an inoperable and incompatible communications environment following the storm.

> Local emergency response officials found it difficult or impossible to establish functioning incident command structures in these conditions. Such structures would have better enabled local response officials to direct operations, manage assets, obtain situational awareness, and generate requests for assistance to State authorities. Without an incident command

---

structure, it was difficult for local leaders to guide the local response efforts, much less command them.[95]

Members of the Hammond (Louisiana) Fire Department reported receiving "a lot of 'I don't knows' from [local] government officials"; another Louisiana firefighter stated, "the command structure broke down, we were literally left to our own devices."[96]

"Eventually, over 50,000 National Guard members from fifty-four States, Territories, and the District of Columbia deployed to the Gulf Coast, providing critical response assistance during this week of crisis. The robust active duty and National Guard response played a crucial role in the effort to bring stability to the areas ravaged by Hurricane Katrina."[97] While the National Guard and active duty military's ability to fill the void in local and State response efforts was significant, the command structure was fragmented and could be characterized as having failed to establish military unity of command.

"The standard National Guard deployment coordination between State Adjutants General was effective during the initial response but was insufficient for such a large-scale and sustained operation."[98] "A fragmented deployment system and lack of an integrated command structure for both active duty and National Guard forces exacerbated communications and coordination issues during the initial response. Deployments for Title 32 (National Guard) forces

---

[95] The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 37.

[96] Ibid.

[97] Ibid., 43.

[98] Ibid.

were coordinated State-to-State through EMAC agreements and also by the National Guard Bureau. Title 10 (active duty) force deployments were coordinated through USNORTHCOM."[99] Once forces arrived in the Joint Operations Area, they fell under separate command structures, rather than one single command and made no attempt to establish formal information sharing and synchronize support efforts. "The separate commands divided the area of operations geographically and supported response effort separately, with the exception of the evacuations of the Superdome and the Convention Center in New Orleans."[100] Title 32 and Title 10 forces continued to operate under separate chains of command throughout operation with no formal process to coordinate operations.

The lack of collaboration between military units that were supporting response efforts was surprising to many observers. Despite the military's recent history of success in combat operations through unity of effort and collaboration among Services and coalition partners, network-centric operations, which are now the military's main means of collaboration among combat forces, could not effectively be applied to support response operations in the Gulf Region. Even if the military force had successfully employed network-centric operations within its own organization, the lack of technical, organizational, and procedural network-centricity among the supported civil authorities and response agencies would have limited the ability to effectively share information, develop

---

[99] The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 43.

[100] Ibid.

situational awareness, achieve self-synchronization, and produce a collaborative effort among agencies to improve mission effectiveness.

Deficiencies in the areas of communications, information sharing, situational awareness, collaboration, and ability to establish a unified command ultimately prevented individual responders and supporting agencies from completing the four basic tasks to accomplish their mission in the Information Age in response to the attacks of 9/11 and the effects of Hurricane Katrina. Failure to complete these tasks resulted in significantly reduced response mission effectiveness to include significant loss of life, property, and public trust in our nation's ability to respond to disasters of national significance.

THIS PAGE INTENTIONALLY LEFT BLANK

III. NETWORK-CENTRIC WARFARE: THE MILITARY'S RESPONSE TO THE INFORMATION AGE

> Continual change and the need to respond to it compels the commander to carry the whole intellectual apparatus of his knowledge with him. He must always be ready to bring forth the appropriate decision. By total assimilation with his mind and life, the commander's knowledge must be transformed into capability.[101]
>
>   – Carl von Clausewitz *On War*

This chapter will examine the U.S. military's adaptation of network-centric operations in the form of Network-Centric Warfare (NCW). The U.S. military continues to evolve into a highly efficient network-centric force through the application of NCW tenants, principles, and technologies to provide the military with increased situational awareness; efficient communications; rapid and standardized information exchange, asset location, and identification; unity of command and unity of effort; and, ultimately, increased warfighting mission effectiveness.

A. NETWORK-CENTRIC WARFARE DEFINED

"NCW is about human and organizational behavior. NCW is based on adopting a new way of thinking, network-centric thinking, and applying it to military operations."[102] "It focuses on attaining access, access to gather, process, and

---

[101] C. Clausewitz, *On War* [Vom Kriege], trans. and ed. M. Howard and P. Paret, Rev. ed. (Princeton, NJ: Princeton University Press, 1984), 170.

[102] D. S. Alberts, J. J. Garstka and F. P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* CCRP Publications Distribution Center, 1999), 88 (accessed September 29, 2006).

manage information to take advantage of the growing power resident in information networks. It facilitates the creation and sustaining of shared awareness at all command levels."[103] It is characterized by the ability of geographically dispersed forces to create a high level of shared battlespace awareness that can be exploited via self-synchronization and self-organization to accomplish time-critical tasks in accordance with command guidance.[104] "NCW supports speed of command, the conversion of superior information position to action."[105] NCW is transparent to mission, force size, and geography and has the potential to contribute to the coalescence of the tactical, operational, and strategic levels of war.[106] "NCW is not narrowly about technology, but broadly about an emerging military response to the Information Age."[107]

B.   ORIGINS

"Exploration of emergent social structures across domains of human activity and experience lead to an overarching conclusion: as a historical trend, dominant functions and processes in the information age are increasingly organized around networks. Networks

---

[103] A. K. Cebrowski, "Network-Centric Warfare," *Military Technology* 27, no. 5 (May 2003), 16, http://proquest.umi.com/pqdweb?did=358330571&Fmt=7&clientId=65345&RQT=309&VName=PQD.

[104] Ibid; Alberts, Garstka and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority.*

[105] Ibid., 88.

[106] Ibid.

[107] Ibid.

constitute the new social morphology of our societies…."[108] "While the networking form of social organization has existed in other times and spaces, the new information technology paradigm provides the material basis for its pervasive expansion throughout the entire social structure."[109]

Many observers believe that a U.S. military transformation is necessary to ensure U.S. forces continue to operate from a position of overwhelming military advantage in support of national objectives. They believe that DoD must transform to achieve a fundamentally joint, network centric, distributed force structure capable of rapid decision superiority.[110] "To meet this goal, DoD is building doctrine, training, and procurement practices to create a culture of continual transformation that involves people, processes, and systems."[111]

In their 1998 seminal article, Vice Admiral Arthur Cebrowski and John Garstka advocated adapting network-centric operating principles from the business world and applying them to the art of warfare.[112] They noted that:

---

[108] Castells quoted by D. Ronfeldt and J. Arquilla, "Networks, Netwars and the Fight for the Future," *First Monday* 6, no. 10 (2001), 1-25.

[109] Ibid.

[110] Clay Wilson, *Network Centric Warfare: Background and Oversight Issues for Congress* (Washington DC: Library of Congress. Congressional Research Service, [June 2, 2004]).

[111] Ibid.

[112] A. K. Cebrowski and J. J. Garstka, "Network-Centric Warfare: Its Origin and Future," *United States Naval Institute Proceedings* 124, no. 1 (January 1998), 28, http://proquest.umi.com/pqdweb?did=25236401&Fmt=7&clientId=65345&RQT=309&VName=PQD.

Society has changed. The underlying economics and technologies have changed. American business has changed. We should be surprised and shocked if America's military did not. For nearly 200 years, the tools and tactics of how we fight have evolved with military technologies. Now, fundamental changes are affecting the very character of war.[113]

The "fundamental changes" cited by Cebrowski and Garstka are a result of our entering into the Information Age. "Recent advances in information technologies and the ability of organizations and individuals to take advantage of the opportunities these advances provide are profoundly altering the nature of the world in which we live."[114] The Information Age is:

1) Changing how wealth is created;

2) Altering the distribution of power;

3) Increasing the complexity;

4) Shrinking distances around the world; and

5) Compressing time, which increases the tempo of our lives.[115]

Network-centric operations were adapted by the U.S. military by examining smart practices implemented by business organizations in response to the transition from the Industrial Age to the Information Age. The adaptation of these principles to the art of war led to the

---

[113] A. K. Cebrowski and J. J. Garstka, "Network-Centric Warfare: Its Origin and Future," *United States Naval Institute Proceedings* 124, no. 1 (January 1998), 28, http://proquest.umi.com/pqdweb?did=25236401&Fmt=7&clientId=65345&RQT=309&VName=PQD.

[114] Alberts, Garstka and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 15.

[115] Ibid.

implementation of network-centric warfare as the military's response to the Information Age. NCW and all of its associated revolutions in military affairs grow out of and draw their power from the fundamental changes in American society in response to the Information Age.[116] These changes have been dominated by the co-evolution of economics, information technology, business processes, warfare, and organizations, and they are linked by three themes:

- The shift in focus from the platform (a military vehicle, vessel, aircraft, or structure) to the network

- The shift from viewing actors as independent to viewing them as part of a continuously adapting ecosystem

- The importance of making strategic choices to adapt or even survive in such changing ecosystems[117]

These themes have changed the nature of American business today, and they also have changed, and will continue to change, the way we conduct military operations in peace and war.[118] A subsequent adaptation of network-centric principles, tenants, and technology to response operations could lead to the transformational change required to overcome current deficiencies.

---

[116] Cebrowski and Garstka, *Network-Centric Warfare: Its Origin and Future*, 28.

[117] Ibid.

[118] Ibid.

C. TENANTS AND PRINCIPALS

"The network-centric approach to warfare is the military embodiment of Information Age concepts. Studies have shown that networking enables forces to undertake a different range of missions than non-networked forces, by improving both efficiency and effectiveness of operations."[119] "NCW involves collaboration and sharing of information to ensure that all appropriate assets can be quickly brought to bear by commanders during combat operations. Procurement policy to support NCW is intended to improve economic efficiency by eliminating stove-pipe systems, parochial interests, redundant and non-interoperable systems, and by optimizing capital planning investments for present and future information technology systems."[120]

However, technology is only one of the underpinnings of NCW that requires changes in behavior, process, and organization to convert the advances of Information Age capabilities into combat power.[121] "Through new uses of NCW technologies, rigid constructs are transformed into dynamic constructs that can provide new and advantageous flexibility for actions in combat."[122]

---

[119] Wilson, *Network Centric Warfare: Background and Oversight Issues for Congress*, 2.

[120] Ibid.

[121] Ibid.

[122] Ibid.

1.   Tenants of Network-Centric Warfare

"Four basic tenets of NCW and a set of governing principles for a network-centric force have been identified. Together, these tenets and principles comprise the core of NCW as an emerging theory of war in the Information Age. The four tenets of NCW help us understand the enhanced power of networked forces."[123]   At the same time, they constitute a working hypothesis about NCW as a source of warfighting advantage:

- A robustly networked force improves information sharing

- Information sharing enhances the quality of information and shared situational awareness

- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command

- These, in turn, dramatically increase mission effectiveness[124]

2.   Principles of Network-Centric Warfare

The four tenants of NCW are supported by nine governing principles:

- Fight first for information superiority

- Access to information (leading to shared awareness)

- Speed of command and decision making

---

[123] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 7.

[124] Ibid.

- Self-synchronization

- Dispersed forces (non-contiguous operations)

- Demassification

- Deep sensor reach

- Alter initial conditions at higher rates of change

- Compressed operations and levels of war[125]

The fight for information superiority is an attempt to generate an information advantage through better timeliness, accuracy, and relevance of information.[126]

Shared awareness, developed from access to information, is the ability to routinely translate information and knowledge into the requisite level of common understanding and situational awareness across the spectrum of participants in joint (multi-service) and combined (multi-national) operations.[127]

Speed of command and decision making allows our forces to recognize an information advantage and convert it into a competitive advantage by compressing decision timelines to produce decision superiority and decisive effects.[128]

Self-Synchronization increases the opportunity for low-level forces to operate nearly autonomously and to re-

---

[125] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 7.

[126] Ibid.

[127] Ibid.

[128] Ibid.

task themselves through exploitation of shared awareness and the commander's intent.[129]

Dispersed forces allow commanders to move combat power from the linear battlespace to non-contiguous operations through rapid "swarming" of forces when and where they are required.[130] This swarming effect can be initiated autonomously by individual units through increased situational awareness, self-synchronization, and initiative or orchestrated by upper levels of command through rapid unit identification and synergistic re-tasking in real time.

Demassification is the movement from an approach based on geographically contiguous massing of forces to one based upon achieving effects.[131]

Deep Sensor Reach leverages the expanded use of deployable, distributed, and networked sensors, both distant and proximate, that detect actionable information on items of interest at operationally relevant ranges to achieve decisive effects.[132]

Altering initial conditions at higher rates of change allows our military to exploit the principles of high-quality shared awareness, dynamic self-synchronization, dispersed and de-massed forces, deep sensor reach, compressed operations and levels of war, and rapid speed of command to enable the joint force to swiftly identify, adapt to, and change an opponent's operating context to our

---

[129] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 7.

[130] Ibid.

[131] Ibid.

[132] Ibid.

advantage.[133]   "Warfare is highly path-dependent; hence, the imperative to control the initial conditions.   The close coupling in time of critical events has been shown historically to have profound impact both psychologically and in locking out potential responses by the enemy."[134]

Compressed operations and levels of war eliminate procedural boundaries between Services and within processes so that joint operations are conducted at the lowest organizational levels possible to achieve rapid and decisive effects.[135]

"While it is not suggested that the governing principles for a network-centric force have supplanted or are going to replace the time-tested principles of war that include mass, objective, offensive, security, economy of force, maneuver, unity of command, surprise, [and] simplicity; they provide added direction for executing military operations in the Information Age."[136]

D.   INFORMATION AGE DOMAINS OF CONFLICT

The four domains of conflict; physical, information, cognitive, and social, as well as the intersections between the domains, must be understood to successfully continue

---

[133]   Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 7.

[134]   Ibid.

[135]   Ibid.

[136]   Ibid.

the implementation and evolution of network-centric warfare to allow our military forces to further increase their mission effectiveness.[137]

The physical domain is the traditional domain of warfare where forces are employed in time and space. This domain of conflict includes land, sea, air, and space environments where the range of military operations are executed and where the physical forces, platforms, and communications networks that connect them reside.[138]

The information domain is the domain where information is created, manipulated, and shared. It is the domain that facilitates the communication of information among warfighters. This is the domain of sensors and the processes for sharing and accessing sensor products as well where information is given value to produce intelligence. It is where command and control of military forces is communicated and the commander's intent is conveyed.[139]

---

[137] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*; Alberts and others, *Understanding Information Age Warfare*, 1-312; Walter Perry, David Signori and John Boon, *Exploring Information Superiority: A Methodology for Measuring the Quality of Information and its Impact on Shared Awareness* (Santa Monica, CA: RAND National Defense Research Institute, 2004), 141.

[138] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75; Alberts and others, *Understanding Information Age Warfare*, 1-312; Perry, Signori and Boon, *Exploring Information Superiority: A Methodology for Measuring the Quality of Information and its Impact on Shared Awareness*, 141; Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*.

[139] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75; Alberts and others, *Understanding Information Age Warfare*, 1-312; Perry, Signori and Boon, *Exploring Information Superiority: A Methodology for Measuring the Quality of Information and its Impact on Shared Awareness*, 141; Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*.

"The information that exists in the information domain may or may not truly reflect ground truth. For example, a sensor observes the real world and produces an output (data) which exists in the information domain."[140] "With the exception of direct sensory observation, all of our information about the world comes through and is affected by our interaction with the information domain. And it is through the information domain that we communicate with others."[141]

The cognitive domain is in the minds of the participants. This is the place where perceptions, awareness, understanding, beliefs, and values reside and where, as a result of sensemaking, decisions are made. The intangibles of leadership, morale, unit cohesion, level of training and experience, situational awareness, and public opinion are elements of this domain.[142] This is the domain where commander's intent, doctrine, tactics, techniques, and procedures reside. This is also where decisive battlespace concepts and tactics emerge.[143]

[140] Alberts and others, *Understanding Information Age Warfare*, 12.

[141] Ibid.

[142] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75; Alberts and others, *Understanding Information Age Warfare*, 1-312; Perry, Signori and Boon, *Exploring Information Superiority: A Methodology for Measuring the Quality of Information and its Impact on Shared Awareness*, 141; Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0.*

[143] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75; Alberts and others, *Understanding Information Age Warfare*, 1-312; Perry, Signori and Boon, *Exploring Information Superiority: A Methodology for Measuring the Quality of Information and its Impact on Shared Awareness*, 141; Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0.*

All of the contents of the cognitive domain pass through a filter or lens we have labeled human perception. This filter consists of the individual's worldview, the body of personal knowledge the person brings to the situation, their experience, training, values, and individual capabilities (intelligence, personal style, perceptual capabilities, etc.). Since these human perceptual lenses are unique to each individual, we know that individual cognition (understandings, etc.) are also unique. There is one reality, or physical domain. This is converted into selected data, information, and knowledge by the systems in the information domain. By training and shared experience we try to make the cognitive activities of military decision makers similar, but they nevertheless remain unique to each individual.[144]

The social domain is where humans interact, exchange information, form shared awareness and understandings, and make collaborative decisions. This is also the domain of culture, the set of values, attitudes, and beliefs held and conveyed by leaders to the society, whether military or civil.[145] It overlaps but is distinct from the other domains of information age conflict. Cognitive activities by their nature are individualistic; they occur in the minds of individuals. "However, shared sensemaking, the process of going from shared awareness to shared understanding to collaborative decision making, is a socio-

---

[144] Alberts and others, *Understanding Information Age Warfare*, 13-14.

[145] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75; Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0.*

cognitive activity because the individual's cognitive activities are directly impacted by the social nature of the exchange and vice versa."[146]

The intersection of the Information Age Domains of Conflict is illustrated in Figure 1.
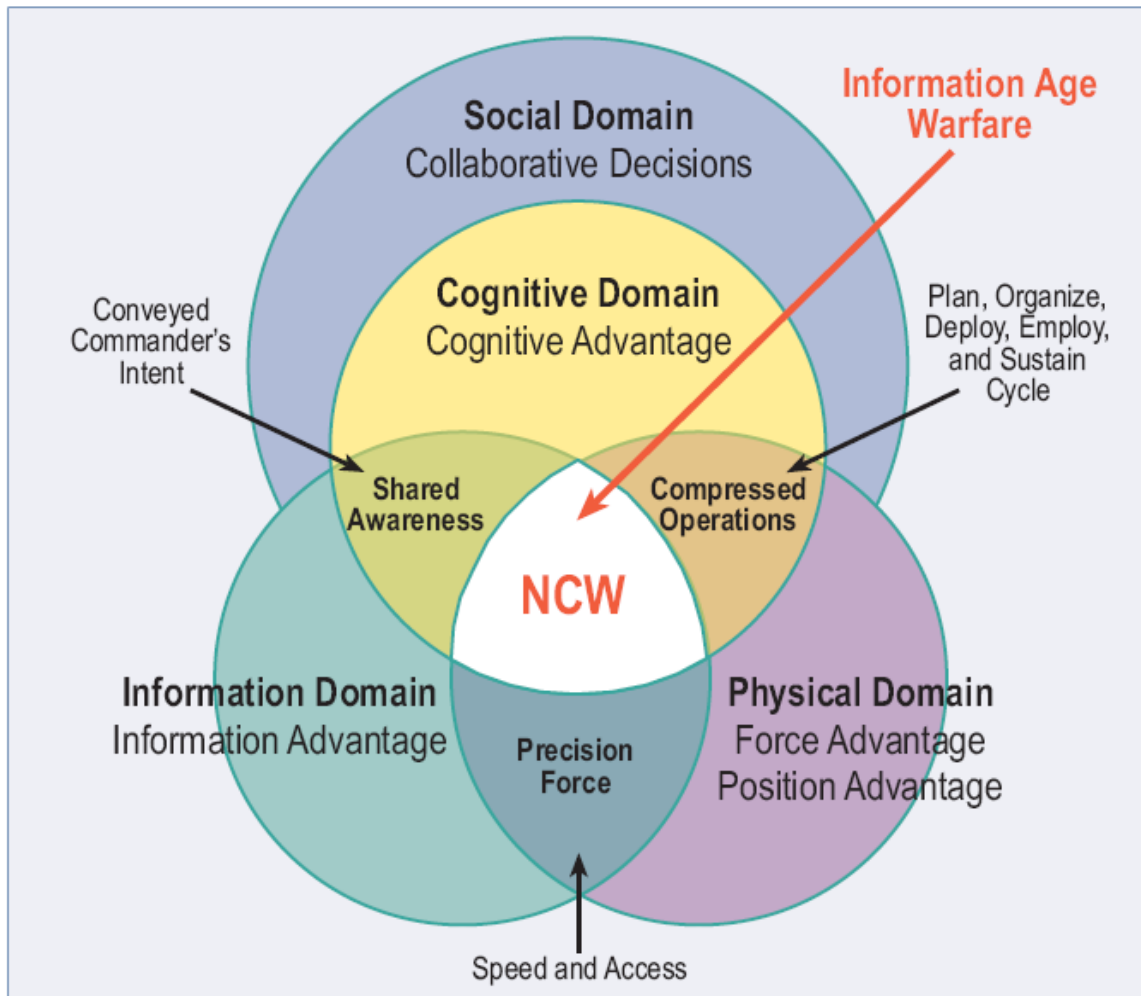
Figure 1.   Information Age Domains of Conflict (From The
            Implementation of Network-Centric Warfare)

The precision force is created at the intersection of the information and physical domains. Shared awareness and

---

[146] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75.

tactical innovation occur at the intersection between the information and cognitive domains. The intersection between the physical and cognitive domains is where compressed operations occur and where high rates of change are developed. NCW, the military's response to the challenges and opportunities of the Information Age, exists where all four domains intersect.[147]

E. COMMON OPERATIONAL PICTURE

The network-centric catalyst to improve information sharing, shared situational awareness, and self-synchronization to enable effective collaboration is the Common Operational Picture (COP). The "picture" provided by the COP is more than a graphic display of the current situation; it is a conceptual understanding or interpretation of the collective information that exists on the network.

Examples of information concerning friendly, enemy, and neutral forces that can be integrated in a COP include:

1) Location (current positions, rate of movement, and predicted future positions);

2) Status (readiness postures including combat capability, whether or not in contact, logistics sustainability, and so forth);

---

[147] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75.

3)   Available courses of action and predicted actions
     for enemy forces (force information also includes
     the capabilities of offensive and defensive
     enemy weapons systems and damage assessment as a
     result of friendly actions); and

4)   The environment (including current and predicted
     weather conditions, the predicted effect of
     weather on planned operations and enemy options,
     and terrain features such as trafficability,
     canopy, sight lines, and sea conditions).[148]

A COP includes both "geospatial displays of the
battlespace and internal intranets that extend vertically
through multiple layers of command and serves as a
commonly-accessible repository of information for military
decision makers. The development of the current generation
COP was motivated largely by the desire to improve
situation awareness within a military command structure,
thus leading to faster and better synchronized planning and
execution decisions."[149] Evidence of success in this area
is demonstrated by examples of operational and tactical
decision making being displayed by networked military
forces in Operation IRAQI FREEDOM, as compared with
decision making just 12 years previously in Operation
DESERT STORM. Examples include the methodical and
efficient destruction of elite Iraqi army divisions, the
quick-responsive and precision attack of high-value targets
by theater-level air and cruise missile assets, and the

---

[148] Alberts, Garstka and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 133-135.

[149] Dennis Leedom, "Functional Analysis of the Next Generation Operating Picture" (Presentation, Evidence Based Research Inc., Vienna, VA, 2003), www.dodccrp.org (accessed October 24, 2006).

speed with which coalition forces move from Kuwait to the Iraqi capital of Baghdad.[150] The next generation COP is being built upon a clear understanding of the sociocognitive processes employed within a military command organization to translate available information into timely and focused action.[151] These processes are variously identified in the research literature as information management, sensemaking, and decision making.[152]

1. Information Management

The COP attempts to mitigate several information management factors that impede the transformation of information into knowledge:

- Lacking sufficient information or lacking confidence in the available information to adequately make sense of a situation (situation uncertainty);

- Being overwhelmed with too much irrelevant information that prevents focusing on the important elements of a situation (information glut);

- Lacking an appropriate, experience-based problem framework for interpreting the available information and associating it with action responses (situation ambiguity);

---

[150] Dennis Leedom, "Functional Analysis of the Next Generation Operating Picture" (Presentation, Evidence Based Research Inc., Vienna, VA, 2003), www.dodccrp.org (accessed October 24, 2006).

[151] Ibid.

[152] Ibid.

- Having multiple, competing problem frameworks for interpreting the available information (explanatory equivocality); and

- Having an experience-based problem framework that yields only limited insight into an evolving or emergent situation (situation emergence)[153]

2. Sensemaking

A modern battlefield is a fluid, dynamic environment in which outcomes and enemy reactions cannot always be predicted with great accuracy.

> Battlespace conditions change, adversary intentions and strategy are not always fully understood, and the fog and friction of war combine to produce both situational novelty and ambiguity. As noted in recent military operations, emergent threats and opportunities can often reflect a mixture of military, political, and diplomatic issues. As a result, when a command organization begins to compare reports and indications of actual events within the battlespace to the prior held set of expectations, discontinuities emerge and give rise to the need for sensemaking.[154]

Sensemaking refers to the sociocognitive activities undertaken by an individual or organization when it is faced with novelty or operational situations that do not conform to prior expectations.[155] "Sensemaking can be both a belief-driven process and an action-driven process. It is a belief-driven process in the sense that the

---

[153] Dennis Leedom, "Functional Analysis of the Next Generation Operating Picture" (Presentation, Evidence Based Research Inc., Vienna, VA, 2003), www.dodccrp.org (accessed October 24, 2006).

[154] Ibid.

[155] Ibid.

interpretation of current events is based on the past experience and accumulated expertise of the commander and his battle staff."[156] This interpretation is also shaped by the context of assigned mission goals and objectives as well as the prior decisions and commitments that have already been made by the commander independent of context. "It is an action-driven process in the sense that organizations often take actions to shape their operating environment and then later attach meaning to these actions to provide them with significance. Both processes operate simultaneously, and as a continuous stream of mental activities, as the commander and staff attempt to impose a mental framework on the chaos of the battlespace, a framework that both simplifies and systematizes their thinking about the unfolding operations."[157] The COP, as employed in a network-centric framework, attempts to answer key questions while resolving ambiguities, often by arranging known facts and held beliefs in story form. "In fact, storytelling has become a commonly recognized method for communicating visions, strategies, structures, identities, goals, and values within both organizations and cultures. Stories also represent a powerful mechanism for communicating themes and evoking visual images."[158] Results of experiments dealing with information and limited time show that color graphic presentations, as represented in a

---

[156] Dennis Leedom, "Functional Analysis of the Next Generation Operating Picture" (Presentation, Evidence Based Research Inc., Vienna, VA, 2003), www.dodccrp.org (accessed October 24, 2006).

[157] Ibid.

[158] Ibid.

COP, were advantageous to actors and decision makers who operated under high time constraints.[159]

There has been additional recognition of the benefit of accommodating storytelling features in the design of computer-supported cooperative work systems, such as a COP. Situational awareness is deemed a major causal factor for improved combat effectiveness for the warfighter involved in network-centric operations.[160] Researchers have demonstrated through controlled experimentation that use of a relatively complete COP by members of a warfighting team results in improved situational awareness, and that this situational awareness is further improved in proportion to the amount of time the warfighting team spends in collaboration using the COP.[161]

3. Decision Making

The final function to be supported by the COP is that of decision making. In one sense, decision making cannot be separated from the activities of information management and sensemaking.[162] It is also noted that different approaches to decision making can arise under varying circumstances of situational ambiguity and time stress. Three primary modes of decision making that are typically

---

[159] N. Ahituv, M. Igbaria and A. Sella, "The Effects of Time Pressure and Completeness of Information on Decision Making," *Journal of Management Information Systems* 15, no. 2 (Fall 1998, 1998), 157 (accessed December 11, 2006).

[160] Paul Hiniker, "Estimating Situational Awareness Parameters for Net Centric Warfare from Experiments" (Presentation, Defense Information Systems Agency, Falls Church, VA, 2005), www.dodccrp.org (accessed October 24, 2006).

[161] Ibid.

[162] Leedom, *Functional Analysis of the Next Generation Operating Picture*, 16.

observed within a military command organization are deliberate decision making, recognition-primed decision making, and incremental decision making.[163]

"Deliberate decision making embodies the traditional military decision making process in which the staff engages in the systematic identification, analysis, and assessment of several course of action responses to an adversary. This process is characterized by a formally communicated commander's assessment, the systematic wargaming of alternative courses of action (for both friendly and adversary forces), and the identification of a preferred course of action that balances expected outcome against risks and resource costs."[164] "Deliberate decision making is engaged in when time stress is relatively low (e.g., pre-hostilities phase of an operation), where the operational situation is understood with some degree of clarity, and where the problem framework is relatively defined in terms of objectives, key variables, and constraints."[165]

Recognition-primed decision making, also referred to in research literature as "naturalistic decision making", is a mode of decision making preferred by experts in high time stress environments that involve substantial time pressure.[166] Recognition-primed decision making occurs when an individual or organization recognizes the type of

---

[163] Leedom, *Functional Analysis of the Next Generation Operating Picture*, 16.

[164] Ibid.

[165] Ibid.

[166] Gary Klein, *Sources of Power – How People Make Decisions*, eds. Devorah Klein and others (Massachusetts: Massachusetts Institute of Technology, 1998), 330.

situation at hand and, from previous experience or mental model, selects the appropriate course of action.[167] "As compared with deliberate decision making, recognition-primed decision making offers the advantage of being both (1) action-oriented (the decision maker always has response options available for execution) and (2) rapid (minimal time is consumed between recognition and response). The recognition-primed model also conforms to the personality of many military leaders since it provides them the opportunity to remain actively involved in the operational situation and requires minimal contemplative thought."[168]

Studies of the effects of time pressure and completeness of information on decision making conclude that, in addition to information management and sensemaking, time and experience play a significant factor in decisions:

- In general, complete information improves performance

- Time pressure usually, but not always, impairs performance

- The more experienced the individual, the less affected they were by time pressure and more information they can digest

---

[167] Paton and Violanti, *Psychology of Terrorism*, 237.

[168] Leedom, *Functional Analysis of the Next Generation Operating Picture*, 19.

- Less experienced individuals tend to make more decisions within a given time interval than experienced commanders who quickly set and follow a strategic plan and modify it to the dynamic environment[169]

"There is a danger, however, in assuming that all military decision making can be characterized by [the recognition-primed decision] model. There is growing evidence that organizations cannot simply employ a naturalistic decision making process in the same way as individuals."[170]

> Individuals make sense of the world largely through the use of internal mental models. This natural human process largely reflects the recognition-primed model just discussed. When functioning in this manner, there is often little or no need for the individual to 'externalize' their knowledge and communicate it with others. In fact, most individuals would find this task to be extremely difficult since much of their expertise exists subconsciously in the form of intuition or tacit (hidden) knowledge. However, such is not the case in an organization where decisions and actions must be synchronized across participants toward a common goal and common understanding of the operational environment, a fact that is beginning to be recognized in some military quarters. In order for such synchronization to take place, individuals must 'externalize' what they know and understand to the degree that it can be shared and reconciled with others. This process of sharing and

---

[169] Ahituv, Igbaria and Sella, *The Effects of Time Pressure and Completeness of Information on Decision Making*, 153-172.

[170] Leedom, *Functional Analysis of the Next Generation Operating Picture*, 19.

reconciling knowledge is exactly what makes cohesive sensemaking difficult to achieve at the organizational level."[171]

Advantages of recognition-primed decision making must be balanced against its limitations. This is particularly true in joint operations where the degree of situational ambiguity is high and various parts of the command organization see the operational situation from different perspectives.[172] The need to cope with situational ambiguity gives rise to the third mode of decision making, incremental decision making. "This mode is defined as a process by which a command organization directs its forces to take incremental steps to contain an adversary's operational advantages while continuing to clarify the overall operational situation. The notion of incremental decision making is consistent with current research literature on organizational sensemaking inasmuch as it acknowledges the need to combine mental analysis with action-taking in order to develop an understanding of the operational situation while, at the same time, shape the operational situation to conform with expectations and desired objectives."[173] This model of decision making is also consistent with research on corporate strategies for dealing with ambiguity and is applicable in both military and response operations.[174]

"At any given time, a command organization is likely to be engaged in all three modes of decision making,

---

[171] Leedom, *Functional Analysis of the Next Generation Operating Picture*, 19.

[172] Ibid.

[173] Ibid.

[174] Ibid.

depending upon the nature of the emerging threats and opportunities. Thus, it is important that the next generation COP provide effective support for each of these decision making modes."[175]

"Shared battlespace awareness emerges when all relevant elements of the warfighting ecosystem are provided with access to the COP. This means that battlespace awareness must be viewed as a collective property (a type of collective consciousness)."[176] Shared situational awareness does not exist at just one place on the network or in the battlespace, but rather at all relevant nodes in the battlespace, across echelons and functional components.[177]

F.   NETWORK-CENTRIC OPERATIONS CONCEPTUAL FRAMEWORK

The network-centric operations conceptual framework was developed jointly over several years by NCW pioneers Cebrowski and Garstka, the DoD's Office of Force Transformation, and the Office of the Assistant Secretary of Defense for Networks and Information Integration.[178] The purpose of developing the network-centric operations conceptual framework was to develop a set of metrics to assess the tenets of NCW. "In order to develop metrics for the tenets, it is first necessary to identify a top level

---

[175]   Leedom, *Functional Analysis of the Next Generation Operating Picture*, 19.

[176]   Alberts, Garstka and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 135

[177]   Ibid.

[178]   Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 31.

or concept level representation of network-centric operations concepts and their relations."[179] While it provides a means to evaluate hypotheses about network-centric operations, it also clarifies and illuminates important aspects of network-centric operational theory that were only implicit in the original tenets.[180]

Figure 2 illustrates a simplified top level view of the network-centric operations conceptual framework and highlights the essential elements of the network-centric operations tenets while introducing new concepts, such as agility.[181]

---

[179] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 57.

[180] Ibid.

[181] Ibid.

Information Domain

Better Quality Networking and Information Sharing

Ensures …

Cognitive & Social Domains

Improved Information Quality

Improved Shared Awareness/Understanding

Enhanced Collaboration/Interactions/Decision Making

More Agile Command and Control

Which contributes to…

More Agile Force Elements

Physical Domain

Which ultimately leads to …

Improved
Mission Effectiveness &
Force Agility

Figure 2.   Simplified Top-Level View of the Network-Centric
Operations Conceptual Framework (After Network-Centric
Operations Conceptual Framework 2.0)

However, in order to develop metrics, further development was made.[182] Figure 3 illustrates the concept level view of the network-centric operations conceptual framework for assessment. The complexity of this view reflects the fact that it is a guide for experimentation and research, and thus, necessarily includes a great deal of detail.[183] In Chapter IV, the network-centric operations conceptual framework will be applied to response operations and its outputs will be mapped to measures of effectiveness (outcomes) that lead to accomplishment of the four basic tasks to operate in the information age (goals).

---

[182] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 57.

[183] Ibid., 58.
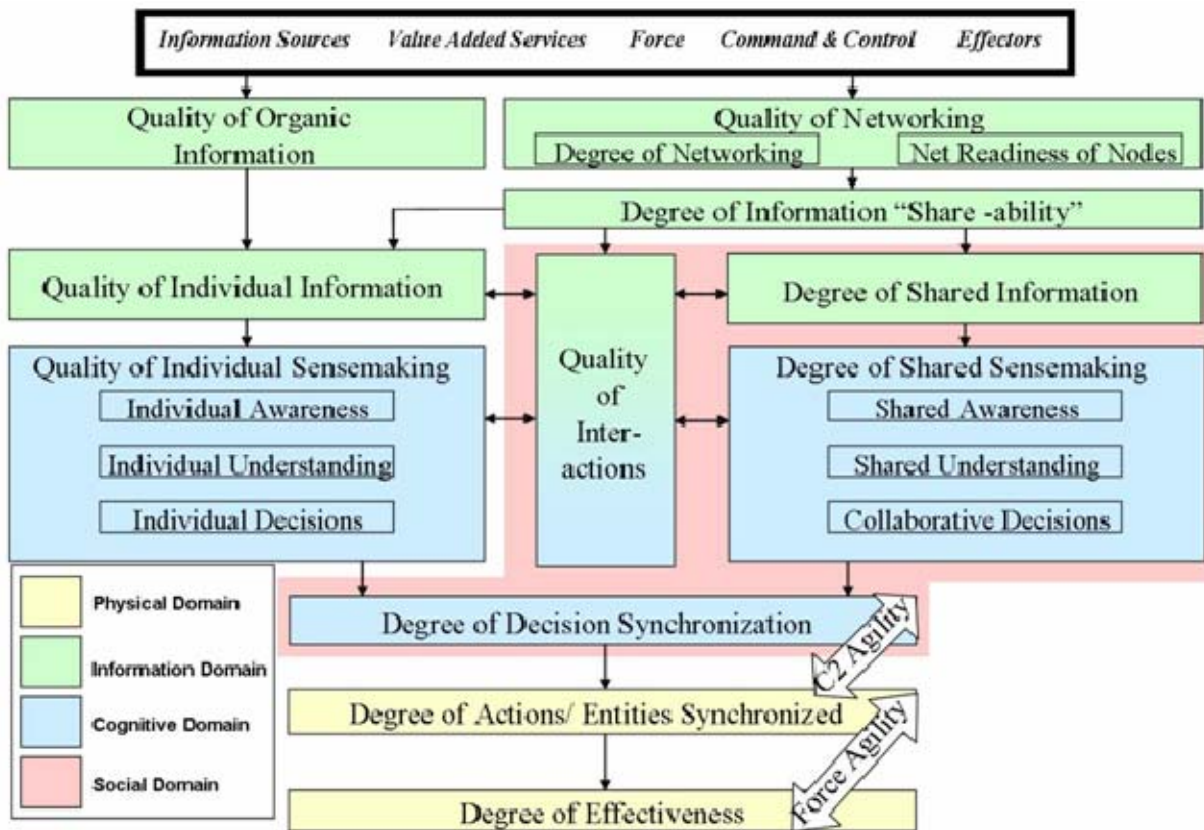
Figure 3.   The Network-Centric Operations Conceptual
Framework (After Network-Centric Operations Conceptual
Framework 2.0)

The Network-Centric Operations Conceptual Framework:

- Builds on the tenets of NCW;

- Is best understood as a generic "process model";

- Explicitly recognizes the key role of the "social domain";

- Incorporates important research on "sensemaking";

- Identifies key concepts important in most workflow processes;

- Identifies potential dependencies among concepts;

- Identifies and defines attributes and metrics for each concept;

- Is scalable across different levels of aggregation;

- Provides a basis for quantitative exploration and/or assessment of network-centric hypotheses; and investment strategies[184]

Network-centric operations are not about technical hardware and routers; they are about people, organizations, and processes. The conceptual framework highlights the fact that network-centric operations cut across several domains: physical, information, cognitive, and social. The central role of social interactions, including collaboration, is evident in the conceptual framework.[185] "…The framework also distinguishes between individuals and groups (teams, organizations, etc.). This is an especially

---

184 Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 59.

185 Ibid.

important innovation as future operations are expected to be joint and involve interagency coordination and international partners."[186]

Development of the conceptual framework also led to the emergence of agility as an especially important concept for network-centric operations which captures the essence of transformation.[187] "Agility refers to the ability to be robust, flexible, responsive, innovative, resilient, and adaptive."[188]

The military continues to evolve its NCW capabilities in pursuit of increased degrees of information sharing leading to an increased benefit from improved information sharing. The current state of NCW evolution and future roadmap are shown in Figure 4.

---

[186] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 59.

[187] Ibid.

[188] Ibid.
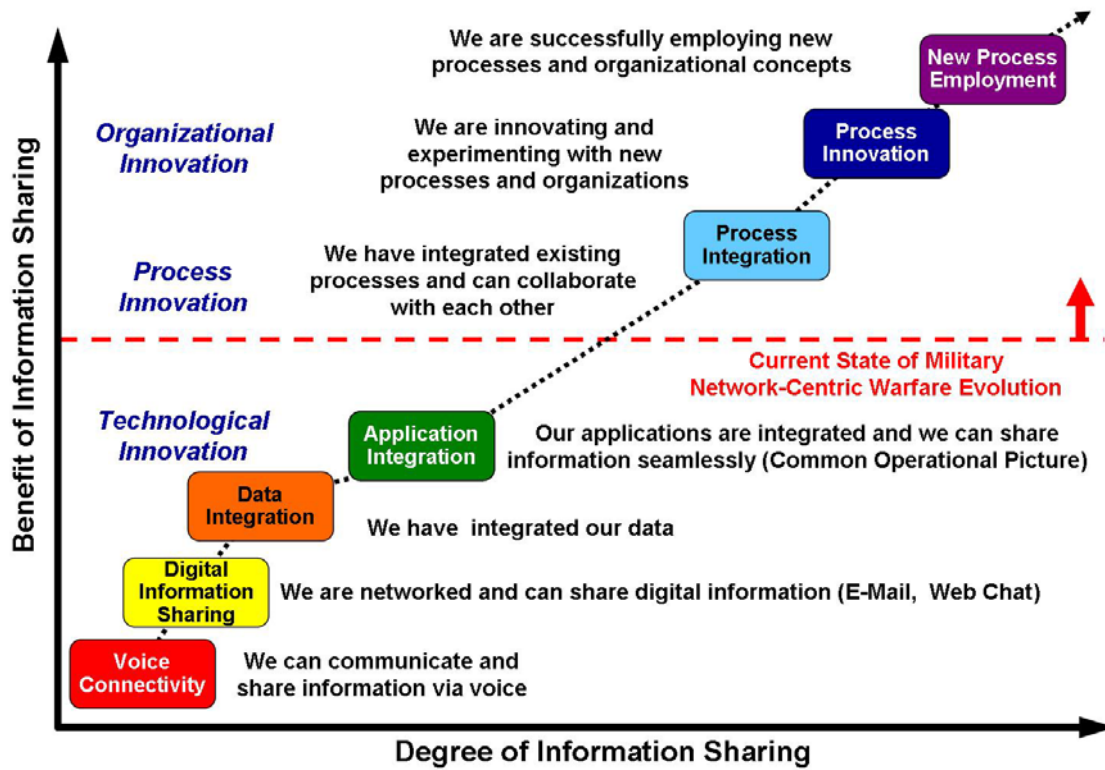
Figure 4.   Evolution of Network-Centric Warfare (After
        Network-Centric Operations: The Power of Information
                Age Concepts and Technologies)

G. BENEFITS OF NETWORK-CENTRIC WARFARE

> NCW is more about networking than networks. It is about the increased combat power that can be generated by a network-centric force. The power of NCW is derived from the effective linking or networking of knowledgeable entities that are geographically or hierarchically dispersed. The networking of knowledgeable entities enables them to share information and collaborate to develop shared awareness, and also to collaborate with one another to achieve a degree of self-synchronization. The net result is increased combat power.[189]

"Emerging literature supports the theory that power is increasingly derived from information sharing, information access, and speed. This view has been supported by results of recent military operational experiences showing that when forces are truly joint, with comprehensively integrated capabilities and operating according to the principles of NCW, they can fully exploit the highly path-dependent nature of information age warfare."[190]

"Evidence accumulated from a wide range of U.S. military activities, including combat operations, training events, exercises, and demonstrations, has strongly supported the validity of NCW as an emerging theory of war and illustrated the power of networked forces. In general, the outcomes have consistently been decisive in favor of forces that are robustly networked."[191]

---

[189] Alberts, Garstka and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 6-7.

[190] Wilson, *Network Centric Warfare: Background and Oversight Issues for Congress*, 7.

[191] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 21.

Networked forces can fight using new tactics. During Operation IRAQI FREEDOM, U.S. and other coalition forces utilized movement that was described by some as "swarm tactics."

> Because networking allows soldiers to keep track of each other when they are out of one another's sight, forces could move forward in Iraq spread out in smaller independent units, avoiding the need to maintain a tight formation. Using "swarm tactics," unit movements are conducted quickly, without securing the rear. All units know each other's location. If one unit gets into trouble, other independent units nearby can quickly come to their aid, "swarming" to attack the enemy from all directions at once.[192]

The concept of "swarm intelligence" is currently being applied to Unmanned Aircraft Systems (UAS). Software programs modeled after swarms of living organisms that often self-organize into highly complex systems that consist of the interaction of many simple individuals (e.g., flocks of birds, schools of fish, and swarms of insects) are being used to task the next generation of smart UAS.[193] "In this initial research, [UAS] are controlled through local rules, but attempt to achieve a common goal as a swarm. Control strategies are based on strictly local information, and other strategies that involve varying degrees of global coordination. The simulator was then extended to allow [UAS] to track moving targets, strike targets, and perform battle damage

---

[192] Wilson, *Network Centric Warfare: Background and Oversight Issues for Congress*, 7.

[193] P. Gaudiano and others, *Swarm Intelligence: A New C2 Paradigm with an Application to Control of Swarms of UAVs* (Washington DC: Command and Control Research Program,[2003]), http://pecolab.colorado.edu/augnet/papers/03swarm.pdf (accessed December 21, 2006).

assessment."[194]   Initial experiments with UAS operating using swarm intelligence programs may benefit other sensor and C2 problems by adopting similar decentralized approaches to military command and control in network-centric environments.[195]

Networked forces can consist of smaller-size units that can travel lighter and faster, meaning fewer troops with fewer platforms and carrying fewer supplies can perform a mission effectively, or differently, at a lower cost.[196]

> In some tactical engagements, superior platforms were decisively defeated by less capable platforms that were able to leverage order-of-magnitude improvements in information sharing enabled by networking. In other engagements, digitized and networked ground forces with a reduced number of platforms were able to substitute information for mass and outperform units equipped with a larger number of platforms not similarly digitized and networked. Even more impressively, the combination of networked and digitized ground and air forces was able to decisively defeat an opposition force with unprecedented lethality by creating and leveraging an information advantage.[197]

The way individual soldiers think and act on the battlefield is also changing. When a unit encounters a difficult problem in the field, they radio the Tactical

---

[194] P. Gaudiano and others, *Swarm Intelligence: A New C2 Paradigm with an Application to Control of Swarms of UAVs* (Washington DC: Command and Control Research Program, [2003]), http://pecolab.colorado.edu/augnet/papers/03swarm.pdf (accessed December 21, 2006).

[195] Ibid.

[196] Wilson, *Network Centric Warfare: Background and Oversight Issues for Congress*, 7.

[197] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 21.

Operations Center, which types the problem into an online chat room using Microsoft Chat software. The problem is then swarmed by experts who may be located as far away as the Pentagon.[198]

The sensor-to-shooter time is reduced. Using NCW systems, soldiers in the field have the capability to conduct an on site analysis of raw intelligence from sensor displays rather than waiting for analysis reports to arrive back from the continental United States.[199]

H. DRAWBACKS TO NETWORK-CENTRIC WARFARE

In theory, NCW will result in the development of a single network but its current state is one of an evolving "network of networks" with all the problems of integration that usually result from such schemes.

The NCW principle of information superiority does not necessarily equate to large quantities of information and/or data, yet some organizations become focused strictly on data collection without regard to relevance or quality. Ultimately more information is not necessarily what is needed, rather it is a better understanding of the information we already have.[200] Additionally, some commanders believe that more information imposes a higher degree of accountability on actions. Failure to minimize casualties or protect civilians may be digitally reviewed and used to politicize flawed military decisions. This

---

[198] Wilson, *Network Centric Warfare: Background and Oversight Issues for Congress*, 7-8.

[199] Ibid.

[200] Ibid.

could lead to an unnatural reluctance or compulsion to act or to reserve decisions for higher levels of command.[201]

"The early products of NCW are encouraging a dangerous trend toward centralized control and execution. If this continues, we will create an organization that has a diminished ability to develop the leadership skills of its junior officer and enlisted personnel and discourages any independent action and stifles innovation."[202] This trend is in direct opposition to the last principle of network-centric warfare, utilization of compressed operations and levels of war to conducted operations at the lowest organizational levels possible.

While NCW benefits the total force, higher echelons of command may forgo the essential human networking in favor of the increased capability to mange the battle remotely, down to the lowest tactical levels possible. "The threat lies not within the core concepts of NCW, which propose universal connectivity and information distribution, but with the possibility that NCW is morphing from a force-multiplier into a technological warfare management system."[203] A commander who covets the information superiority that *he* derives from NCW is likely to focus solely on technical improvements that lead to a greater ability to direct force actions though strict permissive and restrictive orders being issued to dispersed forces rather than encouraging initiative through strategic

---

[201] Wilson, *Network Centric Warfare: Background and Oversight Issues for Congress*, 7-8.

[202] John P. Springett II, "Network Centric War without Art," *United States Naval Institute Proceedings* 130, no. 2 (Feb, 2004), 58, http://proquest.umi.com/pqdweb?did=542511141&Fmt=7&clientId=65345&RQT=309&VName=PQD.

[203] Ibid.

guidance and commander's intent. If NCW tenants and principles are perverted or ignored, access to information by micro-managing command elements can be an enslaving rather than liberating force. In this case, "NCW is likely to become technology-centered and driven, resulting in the focus being more on the network than on the networking. Despite the rhetoric, the human dimension in warfare is more likely to be ignored at the expense of the network."[204]

As the technical implementation goes forward there is the potential for decision makers to forget the human side of NCW theory. In theory, NCW should continue with existing trends towards decentralized command and control. In reality it could easily result in far greater centralization of command at both political and military levels.[205]

"The six months of major combat in Operation ENDURING FREEDOM in Afghanistan saw not only centralized planning, but also a degree of centralized execution that was unique in the U.S. experience. Greatly expanded global communications connectivity provided unprecedented real-time situational awareness at all levels.

That new capability allowed sensor-to-shooter links to be shortened, in some cases, from hours to minutes. It also, however, resulted in an oversubscribed target-approval process that lengthened, rather than compressed, the kill chain. As a result, the human factor became the

---

[204] A. Borgu, "The Challenges and Limitations of Network Centric Warfare–The Initial Views of an NCW Sceptic," *Presentation to the Conference: Network Centric Warfare: Improving ADF [Air Defense Force] Capabilities through Network Enabled Operations* 17 (2003), 2-4 (accessed September 17, 2006).

[205] Ibid., 2-4.

main constraint impeding more effective time-critical targeting."[206] Examples include the use of new Global Positioning System (GPS) guided munitions such as the Joint Direct Attack Munition (JDAM). Previous generations of air-to-ground weapons were guided directly by the aircrew who either selected a weapon impact point using their system or guided the weapon to the target using a laser, data link or some other method. GPS-guided munitions fly to a set of three-dimensional coordinates which are often supplied prior to flight or during the mission by an outside entity. This has relegated aircrew to the role of an ordnance "dump truck" who are reliant upon others for weapon accuracy and targeting.

In one engagement in Operation ENDURING FREEDOM, an F-14 Tomcat aircrew had expended all of its weapons while engaging a Taliban convoy that was traveling east of Masir-e-Sharif, leaving several additional vehicles abandoned but undamaged.[207] The aircrew requested additional aircraft from the Combined Air Operations Center (CAOC) via the E-3 AWACs to complete the destruction of the convoy. A single B-52 was sent to the location that was carrying CBU-103 Wind-corrected Munitions Dispensers (WCMD), GPS-guided cluster munitions that fly to a set of three-dimensional coordinates and release a pattern of cluster weapons that are effective against vehicles. The F-14 was equipped with a laser designator pod that had been modified to generate precise coordinates for GPS-guided munitions. Despite the

---

[206] B. S. Lambeth, "The Downside of Network-Centric Warfare," *Aviation Week & Space Technology* 164, no. 1 (Jan 2, 2006), 86, http://proquest.umi.com/pqdweb?did=958213261&Fmt=7&clientId=65345&RQT=3 09&VName=PQD.

[207] The author was the radar intercept officer in the F-14 involved in this engagement.

insistence by the F-14 crew that the convoy was in a remote location with no possibility of collateral damage and that they could provide precise targeting coordinates directly to the B-52 crew, they were required to read the coordinates of each vehicle to be destroyed through the AWACs to the CAOC. The CAOC staff then validated the coordinates and read them back to the AWACs crew, who then relayed them to the B-52 before weapons were allowed to be employed. This process took over 20 minutes to destroy stationary vehicles that could have been destroyed in much less than half of the time due to over-involvement in the tactical targeting approval process by command elements.

Although NCW should result in making relatively small military forces far more capable, it may result in even smaller forces than we have now as budget planners seek to maintain the current level of mission effectiveness with fewer forces. So while the theory should allow for greater effectiveness, it could be used as a means of gaining greater efficiencies.[208]

While some force reduction may be acceptable, forces cannot be reduced below a certain threshold level without adverse effects. "Applying the principle that networked forces can adequately do the job previously undertaken by numerically superior forces goes against our acceptance of the 'three block war' concept."[209] As former U.S. Marine Corps Commandant Charles Krulak stated:

---

[208] Borgu, *The Challenges and Limitations of Network Centric Warfare–The Initial Views of an NCW Sceptic*, 2-4.

[209] Ibid., 7.

> In one moment in time, our service members will
> be feeding and clothing displaced refugees –
> providing humanitarian assistance. In the next
> moment, they will be holding two warring tribes
> apart – conducting peacekeeping operations.
> Finally, they will be fighting a highly lethal
> mid-intensity battle. All on the same day, all
> within three city blocks. It will be what we
> call the three block war.[210]

Significant force reductions below a threshold level lead to increased force fatigue and inability to effectively "swarm" assets due to significant dispersion in the battlefield or simply the unavailability of forces to quickly assemble and achieve decisive results.

NCW should result in larger numbers of smaller, less complex and less costly platforms/systems operating as nodes in a wider network, but it could result in a smaller number of more complex and more expensive platforms and systems. This would be counter to the NCW principle of demassification. A smaller number of expensive, critical nodes would render the network more vulnerable to attack and less resilient to damage.[211] U.S. Military force structure has traditionally favored technological superiority over superiority of numbers. We sacrifice ship, aircraft, vehicle, and troop numbers to technology even as we decry the resulting stress on operational tempo and global presence (e.g., B-2 and F-22).[212] "Because we are far more likely to encounter targets of influence

---

[210] Borgu, *The Challenges and Limitations of Network Centric Warfare-The Initial Views of an NCW Sceptic*, 7.

[211] Ibid., 2-4.

[212] Thomas Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *United States Naval Institute Proceedings* 125, no. 1 (Jan, 1999), 36, http://proquest.umi.com/pqdweb?did=38107931&Fmt=7&clientId=65345&RQT=309&VName=PQD.

operating in the 'few and cheap' paradigm, what we should bring to the table are 'the many' as opposed to 'the costly'."[213] "The few-and-costly approach puts us in no-win situations, where our entry into crises is self-limited by our tendency, and our opponent's knowledge of that tendency, to treat the loss of any significant network node as grounds for one of two equally bad pathways: escalation or withdrawal."[214]

As Admiral Cebrowski stated regarding the implementation of NCW, it is important to "get the theory right".[215] Network-centric operations are not a panacea for deficiencies in warfare or response operations, if adapted to the area of response. Most drawbacks to the employment of network-centric operations originate from deviations from the tenants and principles through improper or incomplete implementation. Transformation will not be achieved by the implementation of new technology alone, but must include initiatives in all four Information Age domains of conflict and adherence to the underlying principles of network-centric operations.

---

[213] Thomas Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *United States Naval Institute Proceedings* 125, no. 1 (Jan, 1999), 36, http://proquest.umi.com/pqdweb?did=38107931&Fmt=7&clientId=65345&RQT=309&VName=PQD.

[214] Ibid.

[215] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 11.

IV. APPLICABILITY OF NETWORK-CENTRIC OPERATIONS TO RESPONSE

> While we have built a response system that ably handles the demands of a typical hurricane season, wildfires, and other limited natural and man-made disasters, the system clearly has structural flaws for addressing catastrophic events.[216]

> While we remain faithful to time tested principles, we must likewise accept that events such as Hurricane Katrina and the terrorist attacks of September 11, 2001, require us to tailor the application of these principles to the threats we confront in the 21st Century.[217]

Having documented current deficiencies in response operations and conducted an examination of how the military has adapted network-centric operations from the business world and effectively applied its tenants and principles to the conduct of warfare, it is essential to establish the applicability and benefit of network-centric operations tenants, principles, and technology to response operations. The resulting approach to response operations would be correctly labeled as network-centric response.

A. THE PATH TO TRANSFORMATION

Failures in the ability to effectively respond to the attacks of 9/11 and Hurricane Katrina can ultimately be attributed to a lack of network centricity in response

---

[216] The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 52.

[217] Ibid., 11.

infrastructure, planning, organization and execution which resulted in an inability to complete the four basic tasks required to address Information Age challenges.[218] Since the attacks of 9/11, numerous government documents have outlined goals and objectives that emergency respond agencies can pursue in an effort to improve response mission effectiveness. Although not explicitly stated, many of these goals and objectives mark the path for transformation and could be achieved by the implementation of network-centric response.

The National Strategy for Homeland Security, published in 2002, establishes a national vision for the future of emergency preparedness and response:

> We will strive to create a fully integrated national emergency response system that is adaptable enough to deal with any terrorist attack, no matter how unlikely or catastrophic, as well as all manner of natural disasters. Under the President's proposal, the Department of Homeland Security will consolidate federal response plans and build a national system for incident management. The Department would aim to ensure that leaders at all levels of government have complete incident awareness and can communicate with and command all appropriate response personnel. Our Federal, State, and

---

[218] Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, 1-364; National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 1-567; United States Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters*, 1-68; The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 1-217; Federal Emergency Management Agency, *Summary of Post 9/11 Reports "Lessons Learned"*, 1-23; Carafano, *Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century*, 1-7; Grimmett, *Terrorism: Key Recommendations of the 9/11 Commission and Recent Major Commissions and Inquiries*, 1-38.

local governments would ensure that all response personnel and organizations; including the law enforcement, military, emergency response, health care, public works, and environmental communities, are properly equipped, trained, and exercised to respond to all terrorist threats and attacks in the United States.[219]

The 2003 Statewide Template Initiative includes several guiding principles to assist State, local, and tribal authorities in their development of coordinated and comprehensive homeland security plans. Among these principles is the recognition that "our enemy is networked and can only be defeated by a networked system therefore homeland defense must resemble networked PCs rather than a mainframe computer."[220] In addition to the explicit direction to bring network centricity to homeland security operations including response operations, there are several other principles that imply an adaptation of network-centric response in the Statewide Template Initiative. These principles include promoting interoperable and reliable telecommunications capabilities nationwide; promoting integrated and collective training, exercises and evaluations (collaboration); facilitating the adoption of best practices from other jurisdictions (information sharing); and assuring that efforts are State based but locally focused and driven—flexible, scalable, and adaptable (collaboration and self-synchronization).[221]

The National Preparedness Guidance, released by DHS in 2005, lists capability-specific priorities that include

---

[219] Bush, *National Strategy for Homeland Security*, 42.

[220] President's Homeland Security Advisory Council, *Statewide Template Initiative* (Washington DC: White House, [2003]) (accessed October 24, 2006).

[221] Ibid.

network-centric enabling goals. These goals are to strengthen information sharing and collaboration capabilities and to strengthen interoperable communications capabilities.[222] "Information sharing and collaboration capabilities are necessary tools to enable efficient prevention, protection, response, and recovery activities. Information sharing is the multi-jurisdictional, multidisciplinary exchange and dissemination of information and intelligence among the Federal, State, local, and tribal levels of government, the private sector, and citizens."[223] The ability to effectively share information is a prerequisite for collaboration among interagency partners. "Collaboration encompasses a wide range of activities aimed at coordinating the capabilities and resources possessed by various governmental and private sector entities. While Information Sharing seeks to foster a willingness and ability to provide information and/or intelligence, collaboration represents the establishment of formal relationships among various and disparate homeland security entities and systems to interact and cooperate."[224]

A final example of a trail marker on the path to transformation is the Interoperability Continuum developed by the SAFECOM program. The 2006 National Interoperability Baseline Survey represents the first comprehensive effort to survey public safety first responder agencies across law enforcement, fire response, and emergency medical services disciplines in all 50 states and the District of

---

[222] Department of Homeland Security, *National Preparedness Guidance*, 15.

[223] Ibid.

[224] Ibid.

Columbia.[225]   In   contrast   to   other   studies   on
interoperability conducted over the past ten years, this
study assessed five critical elements of governance;
policies, practices, and procedures; technology; training
and exercises; and usage, to determine an organization's
capacity for interoperability.[226]   The Interoperability
Continuum is contained in Figure 5 below.
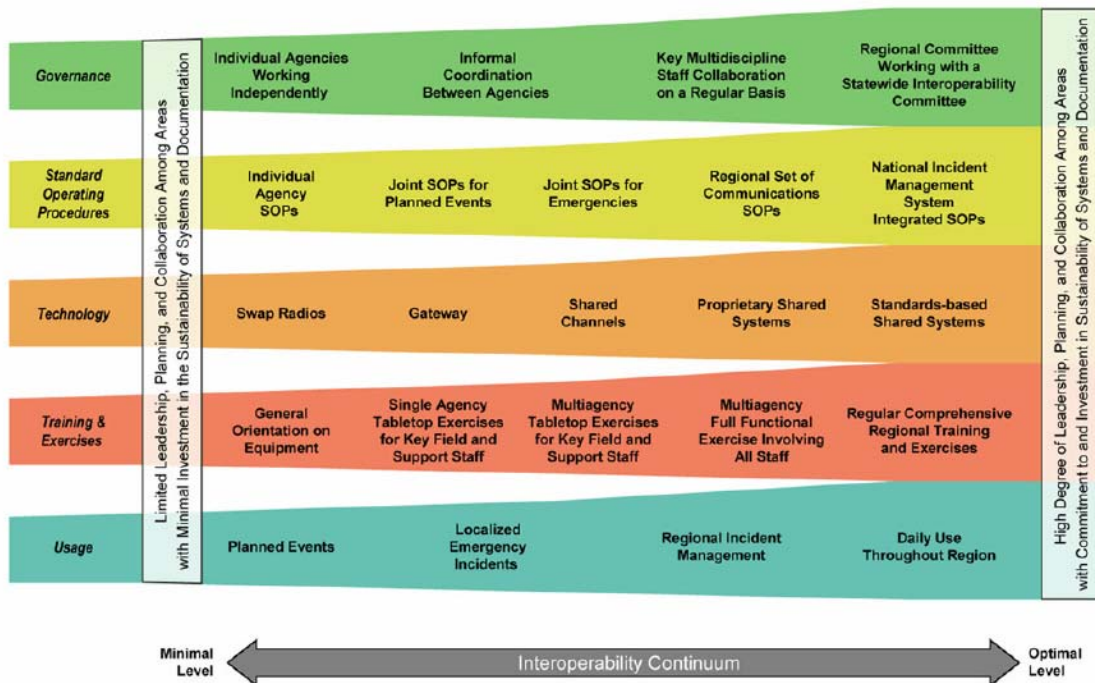
Figure 5.   SAFECOM Interoperability Continuum (From the 2006
              National Interoperability Baseline Survey)

     The level of interoperability that is desired to
support network-centric response operations lies on the far
right of the continuum and encompasses interagency

---

[225] Department of Homeland Security, *2006 National Interoperability Baseline Survey*, 1.

[226] Ibid.

collaboration that is only possible with access to information and ability to share information through interoperable human and technology-based networks.

B. THE "FOG AND FRICTION" OF RESPONSE

In addition to governmental strategic vision for improved response mission effectiveness, the further adaptation of network-centric principles from warfare to response is facilitated by the similarities between the challenges, operating environment, and requirements present in military and emergency response operations as summarized in Table 2 below.

Challenges	Operational Environment Characteristics	Requirements
Time-constrained decisions/actions resulting in the preservation or loss of life	Uncertainty	Ability to effectively communicate and share information
Lack of information	Dynamic conditions	Information management and exchange to support tailorable, dynamic, and timely access to information
Variety in background, training, and experience of force personnel	Multi-agency "joint" operations within a defined area	Real-time mission planning, control, and execution
	Geographically distributed teams of personnel	Deployable sensors and information technology
		Multi-level command centers
Diverse operational roles and equipment	Rapid, decentralized decision making	Coordination and collaboration between "joint" partners
		Individual and shared situational awareness

Table 2.   Similarities Between Military And Response Operations

Warfare and response operations are similar in many ways. They both involve decisions and actions that are constrained in time and result in the preservation or loss of life. The decision and actions are complicated by incomplete information and dynamic environmental conditions.

> The general unreliability of all information presents a special problem: all action takes place, so to speak, in a kind of twilight, …like fog. War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty… The commander must work in a medium which his eyes cannot see, which his best deductive powers cannot always fathom; and which, because of constant changes, he can rarely be familiar.[227]
>
> — Carl von Clausewitz *On War*

"As a result of this enduring characteristic of war, military organizations have, for centuries, been designed to accommodate the lack of available information, that is, how to deal with the fog of war. Fog is all about uncertainty. Uncertainty about where everyone is, what their capabilities are, and the nature of their intentions. Until recently, a commander could not even have a timely and accurate picture of his own forces let alone be comfortable in his knowledge of where the enemy was and what they were up to."[228]

This fog is also found in response operations. There may be a great deal of uncertainty as to the origins of a

---

[227] Clausewitz, *On War*, 161.

[228] Alberts and others, *Understanding Information Age Warfare*, 36–37.

terrorist attack and the potential for follow-on attacks. Emergency response operations are frequently plagued by a lack of information sharing and confusion over responsibilities among policymakers, law enforcement, emergency managers, nonprofit organizations, and federal agencies.[229] Uncertainty can lead to a significant loss of life because many threats require a rapid response capability and operating on compressed timelines which leaves little room for miscues in coordination.[230] In particular, actions taken in the first hours to identify, contain, and treat victims following a chemical or biological attack may significantly reduce the scope of casualties.[231]

"Friction is all about the glitches that occur in carrying out plans to synchronize forces or even to accomplish the most simple tasks. Some of this friction can be attributed to fog, some to poor communications, and some to a lack of shared knowledge."[232]

Network-centric operations attempt to reduce fog (uncertainty) and friction through efficient information sharing, development of situational awareness, and self-synchronization leading to collaboration. While network-centric operations will not lead to reduced risk, their employment allows for improved risk management by accurately identifying the hazards and consequences associated with risk estimates.

---

229 Carafano, *Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century*, 5-6

230 Ibid., 6.

231 Ibid.

232 Alberts and others, *Understanding Information Age Warfare*, 36-37.

The similarity between operational roles of the military and first responders extends to supporting information environments in their attempt to deal with fog and friction and reduce uncertainty. "According to Milligan and Hendler, '…commanders, warfighters, and other combatants need an information management and exchange capability that supports tailorable, dynamic, and timely access to all required information to enable real-time planning, control, and execution of their missions… .'"[233] First responders who need a way to share information among the disparate computing resources of multiple Federal, State, and local agencies that may be involved in responding to an emergency have similar requirements. "For example, just as the future force warrior will have an array of sensors and portable computing devices, first responders are increasingly deployed with information technologies to improve capabilities and life safety. Similarly, there are emergency management centers comparable to theater-level command and control centers. In between there is coordination between agencies handling an emergency similar to joint task force operations, experiencing the same needs for security, privacy, and just-in-time delivery of the right information to the right people."[234]

The main causes of "fog and friction" in current response operations are the inability to use information to make sense of the situation and the inability to

---

[233] W. J. O'Brien and J. Hammer, "Future Force and First Responders: Building Ties for Collaboration and Leveraged Research and Development" (Conference Paper, Austin, TX, 2004), http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA432794&Location=U2&doc=GetTRDoc.pdf (accessed November 3, 2006).

[234] Ibid.

effectively communicate with interagency partners. "Information contributes to every aspect of homeland security and is a vital foundation for the homeland security effort."[235] According to the National Strategy for Homeland Security:

> Every government official performing every homeland security mission depends upon information and information technology. Although American information technology is the most advanced in the world, our country's information systems have not adequately supported the homeland security mission. Today, there is no single agency or computer network that integrates all homeland security information nationwide, nor is it likely that there ever will be. Instead, much of the information exists in disparate databases scattered among Federal, State, and local entities. In many cases, these computer systems cannot share information, either horizontally (across the same level of government) or vertically (between federal, state, and local governments).[236]

The inability to effectively communicate and share information inhibits sensemaking and the development of individual and collective situational awareness. Without situational awareness, individual and organizational self-synchronization and effective collaboration are not possible. These factors result in delayed response timelines and inefficient and flawed decision making that ultimately leads to reduced mission effectiveness.

Just as the military tries to give every individual assess to information to build situational awareness at all levels, "it is often extremely difficult to extend the situational awareness that must be extant in the emergency

---

[235] Bush, *National Strategy for Homeland Security*, 55.

[236] Ibid.

response system to the frontline responders. For example, fire personnel need to know hydrant and standpipe locations, as well as utility and building designs and hazardous material inventories. Often, critical information is stored in locations or formats (e.g., paper records) that prevent them from being readily on hand."[237] "All of this information must be combined and assessed to provide a common operational view for command-and-control. Furthermore, as fire and smoke can develop rapidly, and as new information becomes available (e.g., structural conditions, presence of building occupants, location of operational personnel), the common operational view must be quickly and continuously updated."[238]

First responders are drawn from a wide variety of personnel, including police and fire rescue teams; however, they may be supported by other professionals such as hazmat teams, local utilities, plant and facility operations personnel, and other local officials.[239] "The number of such first responders and associated agencies is very large. Coordination of the broad variety of first responders requires considerable effort."[240] However, like military units, first responders generally work in distributed teams and must make rapid, decentralized

---

237 Carafano, *Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century*, 6.

238 O'Brien and Hammer, *Future Force and First Responders: Building Ties for Collaboration and Leveraged Research and Development*, 2.

239 Ibid.

240 Ibid.

decisions.[241]   "There is a need for the common operational picture to be sent to and updated by distributed teams of first responders."[242]

First responders have diverse operational roles as well. "With respect to response to a fire, first responders have highly specialized roles in terms of search and rescue, combating the fire with various equipment specialists, triage and medical services and evacuation for the injured, hazardous materials handling teams, and, in certain circumstances, special personnel and equipment for sensing and scouting. The diversity of these roles broadly mirrors the specialized roles played by DoD forces. Beyond direct response to an emergency, there are important supporting roles for first responders, including crowd control, directing information to the public and public officials (for example, evacuation information), and coordination with utility and infrastructure maintenance personnel."[243]

Beyond broad conceptual similarities between the military and first responders in terms of coordination of operational teams and needed situational awareness, there are circumstances where direct collaboration between these forces is needed.[244] The military has already been deployed to support relief operations in response to natural disasters (e.g., wildfires, hurricanes, and earthquakes) and may deploy in response to a terrorist attack in the

---

[241] O'Brien and Hammer, *Future Force and First Responders: Building Ties for Collaboration and Leveraged Research and Development*, 2.

[242] Ibid.

[243] Ibid.

[244] Ibid.

future. The primary mission of the United States Northern Command is to conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories and interests within the assigned area of responsibility and, as directed by the President or Secretary of Defense, provide defense support of civil authorities including consequence management operations. Consequence management, in the military context, refers to responding to the effects of a chemical, biological, radiological, or nuclear WMD.

Providing support of civil authorities can be a difficult proposition for the military to coordinate with Federal, State, and local entities when a disaster occurs. Some of the challenges to interoperability between and among military and civil responders cited by the SAFECOM program include:

- More than 60,000 public safety agencies with more than 2.5 million personnel

- The involvement of multiple disciplines (e.g., Law Enforcement, Fire Response, Emergency Medical Services)

- Multiple tiers of government (e.g., township, city, county/parish, State, and Federal)

- Technology differences (e.g., multiple system manufacturers, different communication modes, varied frequency bands)

- Operational differences between public safety disciplines

- Differences in rural versus urban mission operations[245]

Future military forces will have unprecedented access to information provided to field commanders enabling decisive, decentralized decision making while ensuring coordination among diverse units through a common operational picture provided by information technologies.[246] "First Responders have similar operational and information needs as they must coordinate actions of diverse units while providing those units the information needed for rapid and decentralized decision making in response to rapidly changing conditions."[247]

"…It is not surprising that military concepts of operation, organizations, doctrine, and training have always been preoccupied with reducing the effects and risks associated with fog and friction."[248] The implementation of network-centric response offers responders a methodology to cope with and reduce the fog and friction of response.

In its report of the events that transformed our nation and marked the beginning of a generational war on terrorism, the 9/11 Commission understood the wisdom of aligning the strengths of a modern networked military with

---

[245] Department of Homeland Security, *2006 National Interoperability Baseline Survey*, 2.

[246] O'Brien and Hammer, *Future Force and First Responders: Building Ties for Collaboration and Leveraged Research and Development*, 1.

[247] Ibid.

[248] Alberts and others, *Understanding Information Age Warfare*, 36-37.

the deficiencies in response. "If New York and other major cities are to be prepared for future terrorist attacks, different first responder agencies within each city must be fully coordinated, just as different branches of the U.S. military are."[249]

C.   APPLYING THE TENANTS AND PRINCIPLES

The concepts of network-centric operations, shifting competitive spaces, changing underlying rule sets, and co-evolution are not mere theory. They have been applied successfully under demanding conditions with encouraging results. Similarly, these concepts are not limited to a few optimum circumstances in business or warfare. The crime rate in New York City, for example, was reduced dramatically through the application of these concepts.[250]

The tenants of network-centric warfare have direct application to network-centric response operations. A robustly networked force of responders and supporting agencies will improve information sharing among and between interagency partners. Information sharing enhances the quality of information and shared situational awareness. Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command at local, State, regional, and national levels. These factors combine in a synergistic nature to dramatically increase overall response mission

---

[249]   National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 321-322.

[250]   Cebrowski and Garstka, *Network-Centric Warfare: Its Origin and Future*, 28.

effectiveness. This synergic effect is depicted by the Network-Centric Response Value Chain shown in Figure 6.
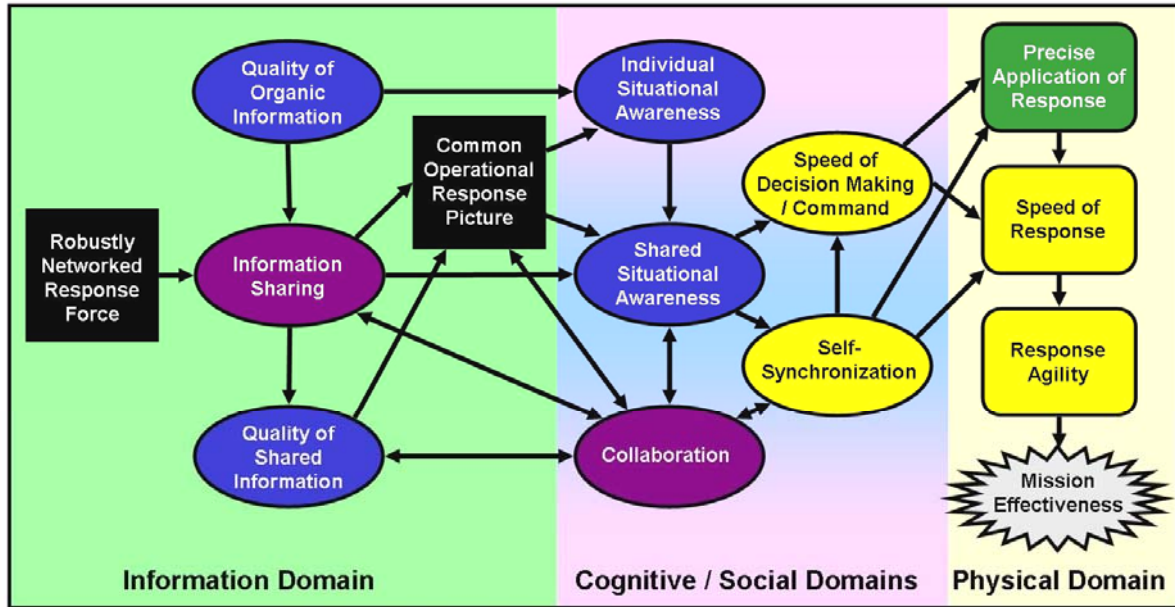
Figure 6. The Network-Centric Response Value Chain (After Implementation of Network-Centric Warfare)

This value chain illustrates how several complementary processes flow across the four domains of conflict and how each element contributes to the accomplishment of one of the four basic Information Age tasks and ultimately contributes to increased mission effectiveness through expression of tangible results in the physical domain.

The principles of network-centric warfare can, likewise, be adopted to achieve network-centric response. The fight for information in the immediate aftermath of a

natural or manmade disaster where initial conditions can be chaotic and difficult to interpret is an essential first step in preparing an effective response. In the case of a terrorist incident with a potential for follow-on attacks that could even target responders, we must assure our information access through a well networked and interoperable force and protection of our information systems, including protection of sensor systems and the first wave of responders to arrive on the scene.[251] The ability to meet initial information demands as quickly as possible and to sustain the flow of information decreases our own information needs, especially in volume, by increasing our ability to exploit all of our collectors.[252]

The employment of a collaborative network of networks, populated and refreshed with quality intelligence and non-intelligence data, both raw and processed, enables responders to build a shared awareness relevant to their needs through efficient access to the data regardless of location.[253] These "information users" must also become "information suppliers," responsible for posting information without delay.[254]

Speed of command and decision making allows responders to leverage information to compress decision timelines to produce decision superiority and decisive effects.[255] Speed of command and decision is essential to effectively address

---

[251] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75.

[252] Ibid.

[253] Ibid.

[254] Ibid.

[255] Ibid.

the effects of a disaster that lead to the loss of life and property. Significant delays in decision making allow lethal effects (e.g., fires, flooding, radiation, biological or toxic chemicals, power losses) to spread and impact a larger population. Rapid assessment of existing threats to life and property, leading to containment or mitigation of these threats is essential to response mission effectiveness.

Self-synchronization increases the value of subordinate initiative to produce a meaningful increase in operational tempo and responsiveness and exploit the advantages of a highly trained, professional force of responders.[256] Additionally, self-synchronization allows responders to rapidly adapt to the dynamic nature of response operations without waiting for members of the unified command to fully comprehend important developments and issue agency-specific guidance and commands.

Dispersed forces allow decision makers at all levels of government to rapidly identify and apply forces when and where they are required upon demand. This principle emphasizes functional control vice physical occupation of the effected area to generate response operations at the proper time and place with the correct capabilities.[257] The value of dispersed forces is increased with the close coupling of intelligence, operations, and logistics to rapidly achieve precise effects.[258]

---

[256] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75.

[257] Ibid.

[258] Ibid.

Demassification uses information to achieve desired effects, limiting the need to mass physical forces within a specific geographical location.[259] This is critical during the initial phase of response where local response forces may be limited in size or capability. Later in response operations when additional and supporting agencies are activated, demassification provides response mission effectiveness with reduced force sizes through effective application of assets operating in a collaborative effort as opposed to individual agencies pursuing common goals independently.

Deep sensor reach leverages the increasingly persistent intelligence, surveillance, and reconnaissance assets that are often allotted to response operations by supporting Federal and DoD agencies (e.g. Unmanned Aircraft Systems, satellites, and mobile command and control units). These sensors augment traditional first responder capabilities to gain and maintain information fidelity and quality. Deep sensor reach enables every response platform to be a sensor, from the individual responder to a satellite, and provides access to this information to the entire response force through technological and organizational networks.[260]

The military seeks to alter initial conditions at higher rates of change to outpace the enemy and keep them off balance. Responders attempt to exploit the principles of high-quality shared awareness, dynamic self-synchronization, dispersed and de-massed forces, deep

---

[259] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75.

[260] Ibid.

sensor reach, compressed operations, and rapid speed of command to quickly assess the situation and slow the rate of change following a natural disaster of terrorist attack.[261]   Response operations, like warfare, are highly path-dependent, so it is essential to control the initial conditions.[262]

Compressed operations increase the convergence in speed of deployment, speed of employment, and speed of sustainment and eliminate the compartmentalization of individual agency processes, decisions, and actions.[263] The goal of compressed operations is to eliminate structural boundaries to merge capabilities at the lowest possible organizational levels (i.e., at the State or local level which has ultimate responsibility for response effectiveness and is supported by regional and Federal entities).[264]

D.   A COMMON OPERATIONAL RESPONSE PICTURE

"Rescue and safety information is in a category of information that is of importance to one or more parties in case of an emergency situation. As of today, almost no information in this group is made readily available through a common information grid, nor are any common data structures or data models established that makes it easy to

---

[261]   Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75.

[262]   Ibid.

[263]   Ibid.

[264]   Ibid.

utilize such information, if it was available."[265] A multi-agency, open technological information sharing network with standardized data structures is critical, even if agencies make the organizational changes required to foster an information sharing culture. "Some of this information is available to some extent in closed systems belonging to police, fire departments, and commercial security providers, but in general this information has to be gathered for each individual case and on a larger scale."[266] If this information was standardized and made available easily and reliably, it would have the potential of making a major contribution to:

- Safety of rescue personnel

- Quicker identification of required resources

- Effective control of escalation/spread

- Protection of most valued assets

- Quicker evacuation and rescue

- Quicker assessment of damage[267]

The presence of integrated information resources through a COP provides considerable opportunities to technologically savvy military operators who are able to leverage these sources.[268] "Information such as building plans, wind conditions, geographic information system

[265] Eldar Aarholt and Olav Berg, *Network Centric Information Structure – Crisis Information Management* (Lysaker, Norway: Defence Division Teleplan AS, [June 2004]).

[266] Ibid.

[267] Ibid.

[268] O'Brien and Hammer, *Future Force and First Responders: Building Ties for Collaboration and Leveraged Research and Development*, 2-3.

terrain data overlaid with utility information, and location of first responders can only aid operations."[269]

In addition to the benefits to information management, sensemaking, and decision making listed in the previous chapter that the military derives from a COP, responders should build upon the current model to produce a flexible, scaleable, adaptable, and resilient Common Operational Response Picture (CORP).

The CORP should be catalyst leading to improved mission effectiveness through better information sharing, situational awareness, self-synchronization, and speed of command at all levels of government and response. The CORP should be an evolutionary improvement of the modern military COP and incorporate the best practices of the current design with the latest information technology initiatives to increase its benefit and usability by responders of all experience levels.

Some recommended improvements include development of technologies that facilitate the brokering of available information together with the specific needs of different information consumers within the unified command at local, State, regional, and national command centers. Specifically, tools and methods should be developed for negotiating the manner in which information is posted to the CORP so that it can serve multiple consumers, each with different intended uses of the information.[270]

---

[269] O'Brien and Hammer, *Future Force and First Responders: Building Ties for Collaboration and Leveraged Research and Development*, 2-3.

[270] Leedom, *Functional Analysis of the Next Generation Operating Picture*, 15-16.

In a related manner, the CORP should provide the means for "information tagging" so that the original context of information posted to the CORP is retained and available to multiple users of that information.[271] Information tagging is thought to be a critical enabler for information aggregation and knowledge creation within an organization and may also assist with the implementation of "electronic tear lines" for information or intelligence that is classified in nature to restrict its access to unintended users. Overuse of classified information will limit its "share-ability" and should only be used if absolutely necessary. A "need-to-share" instead of a "need-to-know" mindset should be adopted by all CORP users.

The CORP should also include technologies that enable the dynamic creation of ad hoc "project teams" or communities of interest that respond to the emergence of specific operational problems that must be framed, addressed, and resolved in an on-going operation.[272] Such technology might employ agent-based software systems to monitor different stakeholder and functional areas and to alert participants to the potential requirement for collaboration.[273] This implies a certain degree of agility is required within the CORP to allow for the dynamic entry of new participants, the posting and sharing of new forms of knowledge, and the support of collaborative problem framing and problem solving.[274]

---

[271] Leedom, *Functional Analysis of the Next Generation Operating Picture*, 15-16.

[272] Ibid.

[273] Ibid.

[274] Ibid.

Development of technologies that facilitate the appropriate filtering, interpretation, and organization of information into actionable knowledge that supports goal-directed actions and decision making should also be considered. "Development of such technologies, however, requires a clear understanding of the distinction between information and knowledge. Specifically, such expert tools would assist the staff in structuring available information, linking it with the decision making focus of the commander, and tailoring it in the form of actionable knowledge that can lead to swift and decisive operations."[275]

Various filters already exist for military COPs that could be adapted for response operations (e.g., geographic, unit type, and/or unit status filters) to aid decision speed and accuracy. Automated decision tools are also available that could indicate mission progress (e.g., areas with completed/incomplete damage assessments, supplies delivered, SAR status) or predetermined trigger events and recommend potential courses of action. Given the diversity of local, State, regional, and Federal response plans, computer-assisted cross referencing of response plans could quickly identify points of concurrence and conflict for members of the unified command when attempting to decide on a proper course of action. All of these applications could be combined with data tags and overlaid on a CORP and tailored to individual user needs.

---

[275] Leedom, *Functional Analysis of the Next Generation Operating Picture*, 15-16.

1.   Decision Making in Response

One of the primary functions of the CORP is to facilitate decision making. Traditional models of military command and control have often reflected decision making as a activity that is focused in the personage of a commander.[276]   NCW dictates that decisions be made at the lowest level possible and encourages initiative through self-synchronization and knowledge of the commander's intent.   While it is true that decision making responsibility and authority in response ultimately reside with the incident commander through the unified command, other individuals within interagency response contribute to various levels of the decision making process.   In this regard, the CORP should be developed in a way that supports each of these levels, all the way down to the individual responder, based on situational awareness, self-synchronization, and understanding of the overall response plan.

The need for more information depends to a great extent on the experience of the subjects involved. More experienced individuals are not as intimidated by information as less experienced individuals due to their ability to select the most relevant data and since they have a more coherent organization of information stored in their memory.[277]   Consequently, they attend to greater amounts of information and process this information more extensively than do inexperienced individuals.[278]

---

[276] Leedom, *Functional Analysis of the Next Generation Operating Picture*, 15-16.

[277] Ahituv, Igbaria and Sella, *The Effects of Time Pressure and Completeness of Information on Decision Making*, 157.

[278] Ibid.

The CORP can support the requirements of deliberate, recognition-primed, and incremental decision making depending on the decision maker's requirements. Of these three modes of decision making, the recognition-primed or naturalistic mode is the most difficult to support but is effectively addressed through a CORP.

The advantages to selecting the deliberate decision model is that it should result in reliable decisions, it is quantitative, it helps novices determine what they don't know, it is rigorous, and it is a general strategy that could be applied in any situation.[279] There are phases of response operations where this model is appropriate to employ, but there are also many instances when time or information constraints inhibit it use, forcing responders to rely on the recognition-primed or incremental approaches.

Deliberate decision making in response is appropriate when:

- Time is available and a choice either requires or may require justification by higher authorities at a later date

- When conflict resolution is a factor among stakeholders, as could be encountered in a unified command

- When optimization is the preferred outcome[280]

Recognition-primed decision making is an important skill when confronted with the dynamic conditions present

---

[279] Klein, *Sources of Power - How People Make Decisions*, 29.

[280] Ibid., 96.

in response operations. "New information may be received, or old information invalidated, and the goals can become radically transformed."[281] Klein's research on how people make decisions in high pressure environments has shown that an average situational change of five times per incident was faced by both first responders and military personnel and that these two groups used similar strategies to make decisions.[282]

Recognition-primed decision making is enabled by the CORP and has been shown to be appropriate under the following circumstances that are frequently encountered in response operations:

- When time pressure is great and it would take too much time to identify all possible alternative courses of action and analyze evaluation criteria

- When people are experienced in their domain, as will be the case when first responders are employed within their area of expertise or representing their individual disciplines in a unified command

- When conditions are significantly dynamic that time and effort expended on deliberate analysis can be rendered useless when the context shifts

- When goals are ill-defined so that evaluation criteria is difficult to define[283]

---

281 Klein, *Sources of Power - How People Make Decisions*, 6.

282 Ibid., 9.

283 Ibid., 95.

Incremental decision making in response is a compromise strategy that can be used to leverage strengths of both the deliberate and recognition-primed methods as mentioned in the previous chapter. In any case, the CORP facilitates each of these methods of decision making and can be filtered or tailored by each organizational level to meet its unique needs and requirements.

The ability to communicate effectively among interagency partners is fundamental to response operations. Network-centric response will not only establish communications connectivity but will produced increased response mission effectiveness through information access and sharing, improved situational awareness, self-synchronization, collaboration, and speed of command and decision making. The NRP established a single, comprehensive approach to domestic incident management that mirrors the unity of effort found in military NCW operations. Network-centric response provides a means of achieving that vision through a collaborative effort.

The military achieves its objectives by employing NCW within the framework of unity of command. While the NIMS directs the use of a unified command, the establishment of common objectives, strategies, and plans does not necessarily foster collaboration among interagency partners as they individually pursue these common goals. The development of shared situational awareness through the implementation of network-centric response will lead to the organizational and individual self-synchronization that is critical to producing a collaborative effort. Self-synchronization and collaboration will enhance the ability

of the unified command to make timely decisions and
efficient application of resources that will dramatically
increase response mission effectiveness.

THIS PAGE INTENTIONALLY LEFT BLANK

V. NETWORK-CENTRIC RESPONSE IMPLEMENTATION CHALLENGES

To be considered as a viable strategy for transformation, network-centric response must be shown to be technically and operationally feasible.

A. TECHNICAL IMPLEMENTATION

Significant technical challenges must be overcome to effectively implement network-centric response that include achieving national voice and data systems interoperability among first responders and supporting agencies and application integration to enable seamless information sharing. Voice and data systems interoperability is the critical foundation upon which the essential technological and human networks of network-centric response are built. Without a technological backbone, reinforced by nationally recognized operating and data structure standards, organizational desires to improve data sharing and collaboration will remain unrealized. The response community lags significantly behind the military in the evolution of network centricity in these core areas of technological innovation. While all of the military services are pursuing increased process integration leading to process innovation and new process employment (e.g., Cooperative Engagement Capability and Future Combat Systems) through the framework of the Global Information Grid, response organizations have yet to achieve national voice communications systems connectivity more than five

years after the attacks of 9/11. The current state of evolution of network-centric operations is shown in Figure 7 below.
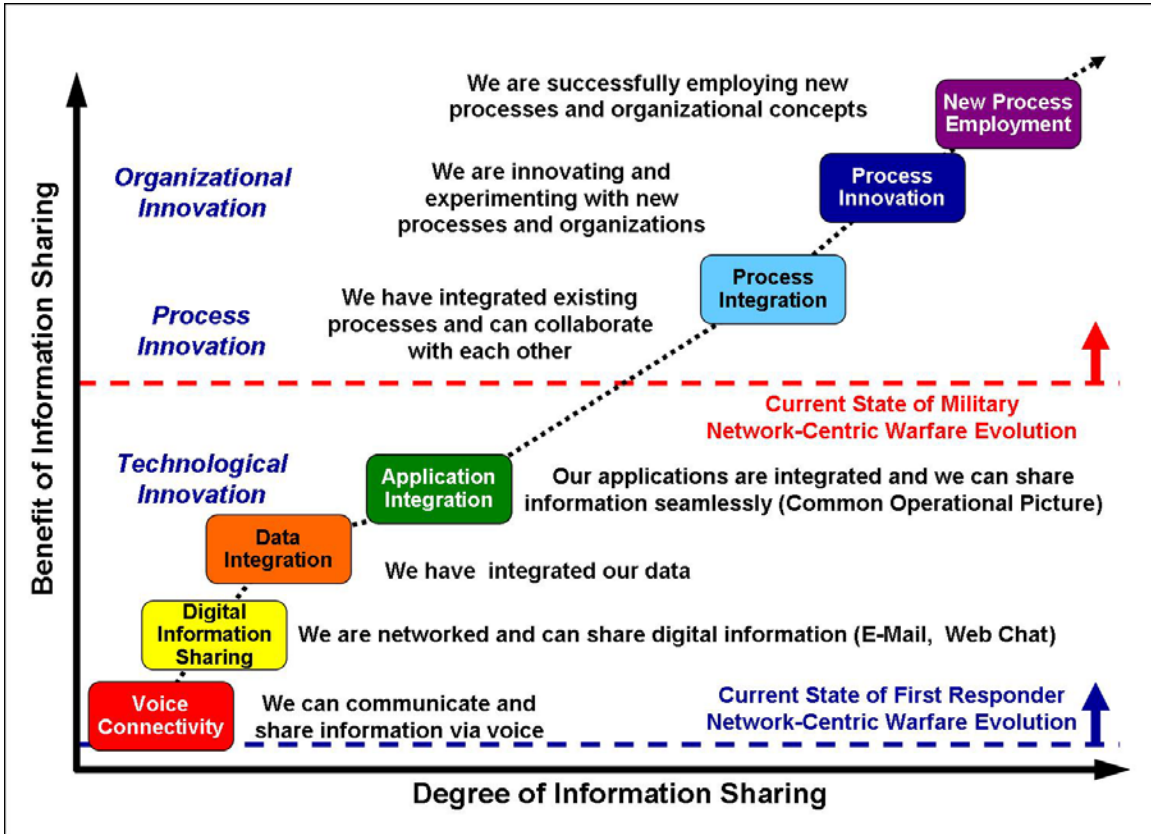
Figure 7.   Evolution of Network-Centric Response Operations for Responders (After Network-Centric Operations: The Power of Information Age Concepts and Technologies)

A properly implemented technological network to support network-centric response operations must exhibit interoperability; survivability; scalability, flexibility, and adaptability; security; spectrum and bandwidth availability; and affordability.

Technical implementation to achieve these characteristics will require the incremental move from a

series of incompatible stove-piped systems toward a system-of-systems approach. To maintain affordability and shorten transformation timelines, technical implementation will focus on existing Commercial off-the-shelf (COTS) and Government off-the-shelf (GOTS) technologies that are available to meet the first two steps toward truly Network Centric Response: interoperable communications and the population of a Common Operational Response Picture. Without interoperable, resilient communications, the best response plans cannot be implemented and unity of effort cannot be achieved. In the worst case, as demonstrated at the WTC following the attacks of 9/11, incompatible communications can cost many lives to be lost.

1. Interoperability

The network-centric road to increased mission effectiveness starts with core voice and data communications interoperability. A critical mass of the response force must be robustly networked as the "entry fee" for adoption of network-centric operations and transformation.[284] This requires a focus on interoperability which must not be sacrificed for near-term considerations.[285] Response entities (centers, units, sensors, and individual responders' equipment) must be designed "net-ready."[286] In addition, increased emphasis must be placed upon research in developing shared situational awareness and new organizational approaches to

---

[284] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75.

[285] Ibid.

[286] Ibid.

achieving synchronization.[287] Setting national, non-proprietary standards for interoperability is a critical step towards network-centric transformation.

The DoD Office of the Assistant Secretary of Defense for Networks and Information Integration has published a network-centric checklist to assist organizations in understanding the network-centric attributes that their programs need to implement to achieve greater network centricity as part of a service-oriented architecture.[288] Service-oriented design focuses on the following best practices:

- Design application and system functionality as accessible and reusable services

- Expose service functionality through programmatic interfaces

- Maintain an abstraction layer between service interfaces and service implementations

- Describe service interfaces using standard metadata

- Advertise and discover services using standard service registries

- Communicate with services using standard protocols[289]

---

[287] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 1-75.

[288] Office of the Assistant Secretary of Defense for Networks and Information Integration, *Net-Centric Checklist Version 2.1.3* (Washington DC: Department of Defense,[2004]) (accessed December 4, 2006).

[289] Ibid.

"Metadata (information about information) helps increase accuracy and extends data use, while context and circumstances help turn the data into information. The interpretation of that information by communities with specific backgrounds and expertise leads to understanding. The process of internalizing these new interpretations of information in context leads to the creation of new knowledge. Knowledge and meaning on an individual basis enable individual action. Information sharing implies availability in multiple places but information sharing alone is not effective without context and mutual understanding. Experts may argue about at which level or at how many levels the sharing should take place, but the objective is to jointly construct shared knowledge, enabling meaning and unified action."[290]

The network-centric checklist could be adopted for use by first responder organizations as they make the transformational changes required to implement network-centric response operations form a technical perspective. At a macro level, the network-centric checklist recommends the following data strategy:

- Ensuring that data are visible, available, and usable when needed and where needed to accelerate decision-making

- "Tagging" of all data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery of data by users

---

[290] Kind and Burton, *Information Sharing and Collaboration Business Plan*, 1-73.

- Posting of all data to shared spaces to provide access to all users except when limited by security, policy, or regulations

- Advancing from defining interoperability through point-to-point interfaces to enabling "many-to-many" exchanges typical of a network environment[291]

Candidate systems should allow transmission of not only voice and text data, but other data sets as well to include video, unit status, positional data, and other selectable metadata fields to contribute to and benefit from the CORP. A growing number of Federal, State, and local jurisdictions are turning to interconnection devices that bridge two-way radio communications with incompatible handsets and landline and cellular phones.[292] These mitigating technologies are technically and fiscally effective for current employment until national standards for interoperability for first responder equipment procurement and operation can be developed and enforced.

Examples of interconnection technology include Communications-Applied Technology's Incident Commanders' Radio Interface device, Aegis Assessments' SafetyNet Radio Bridge, and Raytheon JPS Communications' ACU-1000. Vendors also offer portable versions for transport into emergency locations to blend communications among first responders from a variety of jurisdictions.[293]

---

[291] Office of the Assistant Secretary of Defense for Networks and Information Integration, *Net-Centric Checklist Version 2.1.3*, 1–22.

[292] Joch, *Communications Breakdown, First Responders Look for New Ways to Keep Communications Flowing in Emergencies*, 1.

[293] Ibid.

One system under development by the DoD that encompasses most of the desirable technological features to enable the transformation to network-centric response is the Joint Tactical Radio System (JTRS). By capitalizing on emerging software-defined radio technology, the program plans to develop and procure hundreds of thousands of JTRS radios, which are expected to interoperate with existing radio systems and provide the warfighter with additional communications capability to access maps and other visual data, communicate via voice and video with other units and levels of command, and obtain information directly from battlefield sensors.[294]

> Survivability and lethality in warfare are increasingly dependent on smaller, highly mobile, joint forces that rely on superior information and communication capabilities. The single function hardware design of DoD's existing radio systems lack the functionality and flexibility necessary to achieve and maintain information superiority or to support the rapid mobility and interoperability required by today's armed forces. To support new operational or mission requirements, DOD determined that the large number and diversity of legacy radios in use would require wholesale replacement or expensive modifications. Software-defined radios such as JTRS primarily use software rather than hardware to control how the radio works and, because they are programmable, JTRS offers significant flexibility to meet a wide variety of needs. Rather than developing radios that are built to different standards and operate on different fixed frequencies, as was the case in the past, JTRS is to be a single, interoperable family of radios based on a common set of standards and applications. The radios are expected to not

---

[294] United States Government Accountability Office, *Defense Acquisitions: Restructured JTRS Program Reduces Risk, but Significant Challenges Remain* (Washington DC: GAO, [2006]) (accessed November 19, 2006).

only satisfy the requirements common to the military's three operational domains- air, sea, and ground— but be able to communicate directly with many of DoD's existing tactical radios. To facilitate interoperability, JTRS will develop a set of waveforms (software radio applications) designed with the same operating characteristics as many of DoD's existing radios. Depending on operational needs, different waveforms could be loaded onto a JTRS radio and used to communicate with a variety of other radios. In addition to supporting interoperability, JTRS is to contribute to DoD's goal of network-centric warfare operations by introducing new wideband networking waveforms that dramatically increase the amount of data and speed at which the data can be transmitted. As such, the waveforms would facilitate the use of maps, imagery, and video to support the decision making of tactical commanders at all echelons.[295]

The JTRS or other software-defined radio systems have a great potential to be employed for response operations as they were created to fill gaps in connectivity that are common in the military and domestic response operations at all levels of government.

2. Survivability

Disasters that combine significant damage mechanisms with a large geographic footprint, such as Hurricane Katrina or the future use of a nuclear weapon, could destroy non-resilient communications infrastructure over a large area. The electromagnetic pulse (EMP) from a high altitude nuclear detonation could destroy non-EMP hardened communications equipment in excess of a thousand mile radius from the blast location.

---

[295] United States Government Accountability Office, *Defense Acquisitions: Restructured JTRS Program Reduces Risk, but Significant Challenges Remain* (Washington DC: GAO, [2006]) (accessed November 19, 2006).

"Follow-on terrorist strikes may not be limited to the initial attack site. To complicate consequence management, attacks might be launched at hospitals, police stations, and emergency operations centers. Many state and city emergency operations centers are particularly vulnerable. Often, they lack physical security protection and redundant communications. Back-up centers and mobile command posts usually do not exist."[296]

"For example, the New York City Emergency Operations Center was on the 23rd floor of 7 World Trade Center. When the building was destroyed during the 9/11 attacks, the city had no adequate secondary command and control capability available. It took three days to reconstitute all the functions and capabilities lost by the destruction of the emergency operations center. In the future, terrorists might deliberately attack emergency operations centers to replicate such outcomes."[297]

A survey of first responder communication systems used during the response to the effects of Hurricane Katrina that worked included:

- Interconnection devices that bridge two-way radio communications with incompatible handsets, and landline and wireless phones

- Portable communications gear that uses voice-over-internet protocol (VOIP) technology to send voice over data networks, including satellite links

---

[296] Carafano, *Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century*, 3.

[297] Ibid., 4.

- Paging and two-way messaging that sometimes helped emergency response teams communicate when voice systems failed[298]

Systems that failed in the wake of the hurricane include:

- Communications networks that relied on fixed terrestrial infrastructures, such as telephone lines and cell towers, which were knocked out

- Incompatible mobile radio systems that couldn't bridge communications among local, state and federal authorities[299]

Even though response equipment should be built with survivability in mind, a rapidly deployable communications capability is needed to bridge the gap until local infrastructure is restored in the event that existing communications infrastructure is rendered inoperable or destroyed. This capability could exist with federal supporting agencies (e.g., DHS, DOD) or could exist at the local level and be deployed under Emergency Management Assistance Compacts between states.

The U.S. Coast Guard uses a portable version of the ACU-1000 in a mobile communications unit it calls the Transportable Communications Center, which provides connectivity among VHF radio, UHF capabilities, and Military Satellite Communications systems.[300] "We can duplicate the communications capability of any of our

---

298 Joch, *Communications Breakdown, First Responders Look for New Ways to Keep Communications Flowing in Emergencies*, 1.

299 Ibid.

300 Ibid.

command centers," said Captain Bob Day, chief of the Pacific Area's Communications, Command and Control Division of the Coast Guard, based in Alameda, California. His division established a mobile command center in Louisiana in Katrina's aftermath.[301]

The dispersed network-based architecture leveraged by network-centric response provides its own degree of resilience and survivability through the ability to self-heal and re-form the network when one or more nodes are damaged or destroyed.

3.   Scalability, Flexibility, and Adaptability

The fundamental technological and human networks that comprise network-centric response should be used on a daily basis by all response organizations (e.g., police, fire, and ambulance dispatch). During large scale exercises or real-world events of significant scope, individual networks using common operating procedures, data structures, and compatible equipment could be integrated into larger State, regional, or national networks to provide a scaleable, comprehensive CORP.

> Expanded Internet Protocol (IP) networks, including voice over IP, are other candidates for better communications reliability. Because of their ubiquity, IP-based public and private networks provide a level of resiliency for voice and data communications that exceeds standard point-to-point communications networks. Networking vendors, such as Cisco Systems, offer commercial products that use IP for first responder communications.

---

[301] Joch, *Communications Breakdown, First Responders Look for New Ways to Keep Communications Flowing in Emergencies*, 1.

Cisco's IP Interoperability and Communications System adds a special router to first responder networks that can turn analog voice signals from radio handsets into IP data packets. Cisco said the router facilitates interoperability among radios that use proprietary and open communications standards. The radios can also communicate with other devices connected to the IP network, including laptop and desktop PCs, IP phones and handheld computers.[302]

Other communication systems use a mesh networking protocol to connect Wi-Fi (wireless) devices without the need for functioning access points or communication servers.[303] "The resulting network is IP-based and lets users connect via [personal computers] and personal digital assistants. The mesh technology can turn every communications node into a repeater so the network is self-forming and it doesn't rely on terrestrial infrastructure. The network is self-forming enough that as other terrestrial infrastructure becomes available, it will take advantage of it, so if you have some backup communications, you can utilize them. If you have none at all, the local teams of responders can still communicate with one another."[304]

Once a local network is established, either formally or an ad hoc network formed following the loss of existing infrastructure, is can be connected into a satellite antenna which allows it to be integrated as one hub on a small word network that contains the cumulative national response picture. Satellite communication links are

---

[302] Joch, *Communications Breakdown, First Responders Look for New Ways to Keep Communications Flowing in Emergencies*, 1.

[303] Ibid.

[304] Ibid.

important because they extend the range of the network globally and act as an efficient way to distribute large amounts of data due to the bandwidth and throughput available. Satellite connectivity for all individual assets would be fiscally prohibitive and could saturate the system if all technology was satellite communications based. Establishing satellite connectivity at critical nodes balances fiscal constraints with increased access and allows for prioritization of essential information and users until increased communications connectivity and throughput can be established in a disaster area.

4. Security

High-quality shared awareness requires secure and assured networks and information that can be defended.[305] Cyber attacks on response network infrastructure may occur prior to, during, or after physical attacks by terrorists or in conjunction with forecasted natural disasters in an attempt to impede response efforts and magnify the destruction and loss of life.

If classified military systems are going to be brought to bear in support of civil authorities engaged in response operations, we must assure that our classified technology and sources are not compromised.

To implement an information assurance strategy to transition to a net-centric environment, programs must take advantage of integrated identity management, permissions

---

[305] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 8.

management, and digital rights management while ensuring that adequate confidentiality, availability, and integrity are provided.[306]

Consideration must be given to balance the requirement for information assurance and data security with the ability to intended users to be able to quickly access the shared data. Survivability and connectivity of interoperable systems, however, remains the critical first step toward technical implementation.

5. Spectrum and Bandwidth Availability

Even if all first responder systems were compatible today, they would still complete for space and priority due to a limited amount of spectrum and bandwidth available for response operations. Spectrum is defined as a range of frequencies available for voice or data communications transmission. Bandwidth, in this context, is defined as a measure of the capacity of a communications channel. The higher a channel's bandwidth, the more information it can carry. Certain applications or data formats consume significantly more bandwidth that other applications (e.g., streaming video versus plain text).

> Television broadcasters are scheduled to vacate analog broadcast channels in the 700 MHz band, and some of those channels have been reserved for public safety use. These channels are needed to relieve much of the congestion in public safety bands. Still, only 13 percent of first responder agencies currently use or plan to use this spectrum (located between 764 and 776 MHz), and almost one-half say they do not currently use it nor plan to use it. The availability of this

---

[306] Office of the Assistant Secretary of Defense for Networks and Information Integration, *Net-Centric Checklist Version 2.1.3*, 1-22.

spectrum may be a factor in the responses to this question because broadcasters currently occupying the band are not required to cease operations until early 2009. This delay has created an element of uncertainty in the planning process for new 700 MHz public safety systems. In a related question, 68 percent indicated that their organization has not yet determined the applicability of this spectrum for their use. Of the responding agencies, 15 percent indicated no need or desire to use 700 MHz frequencies.[307]

In addition to the pursuit of increased spectrum availability, new technology is making more bandwidth available. First responders may be able to leverage the military's requirements for increased bandwidth to support its NCW capabilities through defense support for civil authorities in the form of bandwidth and frequency allocation.

The Wideband Gapfiller System (WGS) satellites, due to be launched in 2007, will be the DoD's most capable and powerful communication satellites. The WGS will provide near-term continuation and augmentation of the services currently provided by the Defense Satellite Communications System (DSCS) and the Global Broadcast Service (GBS) Ka services currently provided by GBS payloads on other satellites.[308] "WGS is a high-capacity satellite communications system designed to support the warfighter with newer and far greater capabilities than those provided by current systems, yet it is compatible with existing control systems and terminals. WGS will provide two-way X-band and Ka-band communications as well as Ka-band

---

[307] Department of Homeland Security, *2006 National Interoperability Baseline Survey*, 44.

[308] Global Security, "Wideband Gapfiller System," Global Security, http://www.globalsecurity.org/space/systems/wgs.htm (accessed December 16, 2006).

broadcast services to U.S. Armed Forces and other agencies worldwide."[309] "The DSCS system will be replaced by five fully operational Wideband Gapfiller Satellites, each of which will be able to downlink 2.4 gigabytes per seconds of data to tactical users. The very first Wideband Gapfiller satellite in orbit will provide greater capability and bandwidth than all the DSCS satellites combined."[310]

Beyond the addition of modern technology, a paradigm shift is required for first responders to effectively turn a user-defined version of the CORP into a useful response assessment and command and control tool. While a complete CORP is an invaluable tool resident in command centers at all levels of government, bandwidth and physical equipment size limitations may restrict accessibility to full CORP functionality by deployed individual first responders. In these cases a smaller User-Defined Operational Picture (UDOP) may be preferable to a remote version of the complete CORP. A UDOP is a selected subset of the CORP that contains only the information that is relevant to the user's need and is displayed in a readily accessible format for ease of use. Several unique UDOPs could exist depending on individual agency or responder preferences.

6.   Affordability

We must recognize that some of the stakeholders are not going to be able to make the transition to the newest and best systems in the short term, so mitigating

---

[309] Global Security, "Wideband Gapfiller System," Global Security, http://www.globalsecurity.org/space/systems/wgs.htm (accessed December 16, 2006).

[310] Ibid.

technologies must be adopted.[311]   In the future, we can't develop and procure individual systems such that they isolate others.[312]

> The results of the National Baseline Assessment conducted by the SAFECOM Program show that most agencies have at least a minimum technological capability to achieve tactical interoperable communications.   Whether through mature, shared systems or simply through swapped radios, the technology that many agencies possess is not the primary issue hampering communications interoperability.   Moreover,   each urban/metropolitan area has different technology solutions because achieving interoperability is dependent on the existing types of communications equipment and infrastructures each agency employs. Therefore, the voice communications solution that would be considered ideal in one area could be unsuited for another.   As the interdependencies of the [SAFECOM] Interoperability Continuum [Figure 5] illustrate, it is the ability to use technology during incident response that allows an area to have improved tactical interoperable communications.[313]

The procurement of common equipment will lower the overall cost per unit and will also reduce future operation and maintenance costs.

Network-centric response must become the daily standard for normal operations as well as crisis response if it is to be successfully adapted by first responders and supporting agencies nation-wide.   Technical and fiscal achievability are easy to document by referencing

---

[311] "Center Outlines Network Centric Warfare Concept's Challenges," *Defense Daily* 209, no. 56 (March 23, 2001), 1, http://proquest.umi.com/pqdweb?did=72676666&Fmt=7&clientId=65345&RQT=30 9&VName=PQD.

[312] Ibid.

[313] Department of Homeland Security, *Tactical Interoperable Communications Scorecards Summary Report and Findings*, 2.

initiatives and products being offered by numerous corporations to fill the growing market for homeland security-enabling technologies. Organizational adaptation with be more difficult to demonstrate, but could be assessed by referencing training exercises where network-centric-enabling technologies were made available to first responders and the outcomes and lessons learned from these exercises.

Despite the promise of current technology, the critical element to achieving a transformation to network-centric response in not lodged in technology, commercial off-the-shelf or otherwise.[314] Network-centric response requires that the interagency partners at all levels of government, local to federal, make the "cultural change" of getting its response agencies to recognize the advantages of efficiently interlinking their information.[315]

B. ORGANIZATIONAL IMPLEMENTATION

Organizations that attempt to implement transformational strategies, vice incremental improvements to an existing strategy, must overcome four key organizational hurdles.[316]

---

[314] "Center Outlines Network Centric Warfare Concept's Challenges," *Defense Daily* 209, no. 56 (March 23, 2001), 1, http://proquest.umi.com/pqdweb?did=72676666&Fmt=7&clientId=65345&RQT=309&VName=PQD.

[315] Ibid.

[316] W. Chan Kim and Renee Mauborgne, *Blue Ocean Strategy* (Boston, Massachusetts: Harvard Business School Press, 2005), 147.

The first hurdle is cognitive, instilling belief in the need for change in the stakeholders.[317] The second hurdle is limited resources. The greater the shift in strategy, the greater it is assumed are the resources needed to execute it.[318] The third is motivating the stakeholders to act to implement the desired strategy.[319] The fourth hurdle is overcoming the collective political forces that will resist transformational change, regardless of the potential increase in productivity or mission effectiveness to be gained.[320] Essential to efficiently overcoming these hurdles is the employment of decisive leadership that focuses on the technology, organizations, processes, and individuals that exercise a disproportionate influence on the response operations mission effectiveness.[321]

1. The Cognitive Hurdle

A transformational change may be required to reach desired goals, but existing strategies feel comfortable and may have offered incremental, but small, gains in the past.[322] Organizations tasked with responding to our nation's disasters must embrace the need for transformational change or risk the lack of collaboration and persistent mediocrity that has characterized response

---

[317] W. Chan Kim and Renee Mauborgne, *Blue Ocean Strategy* (Boston, Massachusetts: Harvard Business School Press, 2005), 147.

[318] Ibid.

[319] Ibid.

[320] Ibid., 148.

[321] Ibid., 151.

[322] Ibid., 147.

efforts of the last half decade despite significant funding, the best of intentions, and heroic individual efforts.

The current deficiencies in response are well-documented by Congressional commissions, the Government Accountability Office, and a variety of first responder organizations, but our nation's leaders in Congress and the Department of Homeland Security have yet to be influenced to make anything more than incremental changes through increased funding of existing programs and agencies.[323] Even the most ambitious initiatives, such as the National Response Plan, have offered incremental change within the existing framework of response. Firsthand exposure to the deficiencies in the current state of response and the resulting consequences may trigger the need to implement the transformational strategy associated with network-centric response.[324]

Decision makers at all levels of government should be made to leave the safe confines of Washington DC and regional command centers to experience the devastation of the next disaster firsthand. Not only would they be exposed to the frustration of first responders who are

[323] Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, 1-364; National Commission on Terrorist Attacks upon the United States (The 9/11 Commission), *The 9/11 Commission Report*, 1-567; United States Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters*, 1-68; The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, 1-217; United States Government Accountability Office, *Opportunities Exist to Enhance Collaboration at 24/7 Operations Centers Staffed by Multiple DHS Agencies* (Washington DC: United States Government Accountability Office,[2006]), http://www.gao.gov/new.items/d0789.pdf.

[324] Kim and Mauborgne, *Blue Ocean Strategy*, 152.

unable to communicate or effectively share information with interagency partners to produce a synergistic response effort, they would be forced to personally acknowledge the destruction and loss of life that results from gaps and redundancies in individual organizations response efforts.

In the absence of the next major disaster, senior leadership should see increased participation in State, regional, and national level response exercises, such as the ARDENT SENTRY series of exercises sponsored by United States Northern Command. It is important that these exercises be conducted to stress the national response system and not merely validate current capabilities and methods through the employment or notional assets in a hypothetical environment in reaction to a possible threat. Real-world exercise of systems, plans, and personnel should be conducted against a significant threat in an as realistic setting as possible. Rather than preplanning responses from a known script, organizations should be made to react to dynamic events as they unfold to stress the requirement for naturalistic decision making and a coordinated, collaborative response effort. Learning from failures, in addition to success, should be the goal of the exercises to identify and address gaps in planning, procedures and response capabilities. "Coming face-to-face with poor performance is shocking and inescapable, but actionable."[325]

In addition to firsthand exposure to the deficiencies in response and the results of these deficiencies, leadership should be exposed to the segment of the public

---

[325] Kim and Mauborgne, *Blue Ocean Strategy*, 153.

that has been affected by disasters.[326]   Performance
indicators that have been traditionally used to measure
response operations (e.g., search and rescue operations
completed, forces deployed, evacuees moved, meals served,
etc) may not accurately reflect the public's priorities and
expectations of mission performance by first responders and
supporting organizations.   Personal interactions with the
public that was affected by disasters may reveal
operational gaps and mismanaged expectations that are not
evident when reviewing numerically-based performance
indicators and other statistics.[327]

Once the need to implement a transformational response
strategy is understood, the strategy must be implemented
enterprise-wide.   It will not be enough to implement
network-centric capabilities, conduct network-centric
operations, and test the theory of network-centric response
only in a "critical mass of the joint force" or in certain
high priority municipalities, as we can not anticipate
where or when the next attack will occur.[328]   Instead, the
capabilities must be developed and the theory applied
enterprise-wide, throughout all levels of government, and
exercised on a daily basis.   Network-centric response must
become the steady state of daily operations at all levels
and not just the response to major disasters.

---

[326]   Kim and Mauborgne, *Blue Ocean Strategy*, 155.

[327]   Ibid.

[328]   Director, Force Transformation, Office of the Secretary of
Defense, *The Implementation of Network-Centric Warfare*, 11.

2.   The Resource Hurdle

Using current response strategies, logic would dictate that incremental improvements in performance can only be achieved with proportion increments in resources.[329] Network-centric response attempts to concentrate collective resources on the areas that will result in the greatest improvements in overall response; communications compatibility and connectivity, and information sharing. At the most fundamental level, no collaboration can exist within or among the various organizations and agencies that are tasked with responding to national disasters if they cannot communicate with each other effectively.

Fortunately, the technology on which a network-centric response operates has been developed and is already being fielded and improved upon in areas outside of response. Specifically, network-centric warfare systems currently receive and will continue to receive significant funding from the military as network-centric warfare doctrine and systems continue to evolve. Therefore, there is significant resource savings to be gained in the areas of research and development, technical production, and employment techniques when moving to a network-centric response strategy.

Congress has already enacted legislation to facilitate the adaptation of existing military technology. "Section 1401 of Public Law 107-314, the Technology Transfer Program, was signed into law on December 2, 2002 to

---

[329] Kim and Mauborgne, *Blue Ocean Strategy*, 157.

leverage DoD's technological and logistic capabilities to assist first responders."[330] Objectives of the Technology Transfer Program include:

- Enhancing the capabilities of Federal, State and local first responder and public safety officials

- Developing an efficient, effective, and coordinated process for transferring DoD equipment and technology to first responders and making those items available

- Improving compatibility and interoperability between DoD and Federal, State and local first responders

- Collaborating on research, development, testing, and evaluation of high-priority technology, items, and equipment

- Assisting the national effort to support first responders by contributing to the "Enable" activities of the Department, as outlined in the DoD Strategy for Homeland Defense and Civil Support[331]

Current DoD network-centric enabling technology can be adapted for response operations under the Technology Transfer Program and new products can be developed jointly with domestic response use incorporated at all levels of system planning and development. It is important that

---

[330] Donald Lapham, "1401 Technology Transfer Program" (PowerPoint Briefing, Technologies for Public Safety in Critical Incident Response Conference 2006, Office of the Assistant Secretary of Defense for Homeland Defense, 2006), http://www.nlectc.org/training/nijconf.html (accessed November 5, 2006).

[331] Ibid.

system development occur with stakeholder input outside of traditional military research and development channels if the developed products are going to adequately address the needs of all potential users.

The Joint Tactical Radio System received approval for the restructuring of their program in March of 2006 to address and reduce program risks that the Government Accountability Office and others have documented in recent years.[332] While still meeting key requirements, including those related to DoD's network centric transformation effort that would also benefit response operations, the revised approach is expected to develop and field capabilities in increments rather than attempting to develop and field the capabilities all at once.[333] This programmatic restructuring offers first responder organizations a window of opportunity to represent their requirements to the JTRS Joint Program Executive Office and influence final production designs and capabilities. Acquisition of this radio system by first response agencies across the nation in significant numbers will not only assist in their transformation to network-centric response but will decrease unit cost for all users while distributing future operational and maintenance costs as well.

If achieved, the transformation to network-centric response will lead to a demassification of individual agency forces required, resulting in human resource savings as well.

---

[332] United States Government Accountability Office, *Defense Acquisitions: Restructured JTRS Program Reduces Risk, but Significant Challenges Remain*, 1-34.

[333] Ibid.

3. The Motivation Hurdle

"When most business leaders want to break from the status quo and transform their organizations, they issue grand strategic visions and turn to massive top-down mobilization initiatives."[334] But this is often a cumbersome, expensive, and time-consuming process and overarching strategic visions often inspire lip service instead of the intended action.[335] Rather than spreading implementation efforts equally across all the possible stakeholders, it is more efficient and effective to target the key influencers at each level of government that have the ability to set policy, influence the procurement of equipment, and direct response operations. If these key targets can be effectively engaged, they will serve at the catalyst to transformation to network-centric response.

Specific target audiences should include:

- DHS and DoD, who provide significant support to locally lead response operations when the scope or capability of local response is exceeded. Because their response capabilities could be employed in any of the thousands of jurisdictions throughout the 54 States and providences, compatibility and a common methodology is of significant interest to these organizations.

- State Adjutants General, who work for the Governor of the State in a Title 32 status and are often employed to assist neighboring States under Emergency Management Assistance Compact

---

[334] Kim and Mauborgne, *Blue Ocean Strategy*, 161.

[335] Ibid.

146

authority but could also be federalized into Title 10 service. Due to their unique position, National Guard forces must maintain connectivity and compatibility with both Federal and State and local interagency partners.

- State Emergency Operation Center (EOC) Directors, who can enforce conformity within their jurisdictions, yet wish to leverage their access to information that would be resident in larger regional constructs when dealing with disasters that affect several States or cross geographic boundaries. These State EOC Directors also exert considerable influence over the metropolitan areas within their State, allowing individual cities and agencies to me motivated and embrace network-centric response through their leadership.

Once key influential stakeholders have been engaged and motivated to implement a new strategy, their progress toward transformation must be based on transparency, inclusion, and fair process.[336] The current state of their individual organizations' technical and inter-organizational networks should be benchmarked and future goals should be established using a collaborative development process. Progress toward network centricity should be monitored and published periodically to all stakeholders and explained by each key organization. As implementation of a network-centric strategy progresses,

---

[336] Kim and Mauborgne, *Blue Ocean Strategy*, 162.

147

all stakeholders must be involved in the development of tactics, techniques, and procedures to best leverage its advantages for response.

Framing of the transformational process is also critical to motivating key stakeholders. When viewed as a national initiative, network-centric response can seem overwhelming and unattainable at the local level. Transition to network-centric operations should be broken down into small building blocks at the State and local levels with emphasis on local interagency connectivity, interoperability, and data sharing among local interagency and State partners. A common operational response picture, with subset user-defined operational pictures, can be employed to coordinate local police and fire response and asset allocation just as well as it can be used by the military to run a major theater war. Scalability through common technology and processes will allow the local pictures to be fused into a State picture, which contributes to a regional picture, which could be used to populate a national Common Operational Response Picture. Ultimately, a deployed local search and rescue asset that participates in the response network could have access to overhead information, surveillance, and reconnaissance images that were previously only available in national command centers. Each individual responder could effectively benefit and contribute to the CORP.

Governance at the State level must be stressed to counter the susceptibility of network-centric operations to lead to a federalized central control of assets. This potential should be easier to combat than in the military doctrine of network-centric warfare where a strict

148

hierarchal structure (i.e., the chain of command) could lead to micro management of tactical assets because response operations are already established as being led locally with federal entities in a supporting role in almost every case. Improvements to the command and control architecture and guidance from the unified command should emphasize decentralized execution at every stage. "Finally, the temptation to push centralized control up the chain should be resisted ruthlessly. The effort to flatten the command and control hierarchy must be examined not only through the eyes of the network-centric operations technology experts, but also through the eyes of sociologists, so that we do not end up destroying an already effective human organization only to model our own machines."[337]

4. The Political Hurdle

"Organizational politics is an inescapable reality of corporate and public life."[338] It is essential to identify who has the most to gain or lose from the implementation of a network-centric response strategy if the political hurdle is to be cleared.

Proponents of this strategy would include any first responder organization that desires to increase their mission effectiveness through collaboration and teamwork. However, sometimes individual organization recognition takes priority over the collective effort of several organizations working in concert. The "battle of badges" has raged in New York City since it's founding with Police

---

[337] Springett, *Network Centric War without Art*, 58.

[338] Kim and Mauborgne, *Blue Ocean Strategy*, 165.

and Fire communities vying for incident control through their City Incident Management System and leading to equipment incompatibility and redundancy in capabilities (e.g., Hazardous material response and search and rescue teams). Professional response organizations such as the International Association of Chiefs of Police and International Association of Fire Fighters must embrace transformation to promote acceptability by their membership.

Organizations that may resist the movement to network-centric response include the Intelligence Community (IC) and, ironically, the DoD. Members of the IC have traditionally derived their power by controlling access to information, not by sharing it with outside organizations. The cultural transformation from the "need to know" to the "need to share" within the IC is far from complete. To prevent the compromise of classified information, electronic "tear sheets" may have to be implemented to allow access to certain information or intelligence overlays only to approved users. The end user of intelligence products is ultimately at the tactical level. While sources and systems can be protected, the effectiveness of response ultimately depends on the flow of information to decision makers at the lowest levels.

The DoD may not eagerly welcome additional stakeholders into push for further network-centricity among the military services who are pursuing increasingly swift and lethal warfare capabilities. Response requirements may be seen as a challenge to the schedules set for the deployment of systems designed primarily to enhance our ability to conduct warfare. The benefits of the economics

of conglomeration must be emphasized. Response organization entry into the world of network-centric operations should only accelerate the national movement toward compliance and system development.

C. METRICS FOR ASSESSMENT

Concrete metrics are essential to establishing the degree and level of effectiveness of network-centric operations once they are implemented as network-centric response. The outputs of the network-centric conceptual framework are mapped to the five measures of effectiveness that will be used to assess the ability of network-centric response forces to complete the four basic tasks required to operate in an Information Age security environment in Figure 8. Completion of the four basic tasks will lead to improved mission effectiveness.
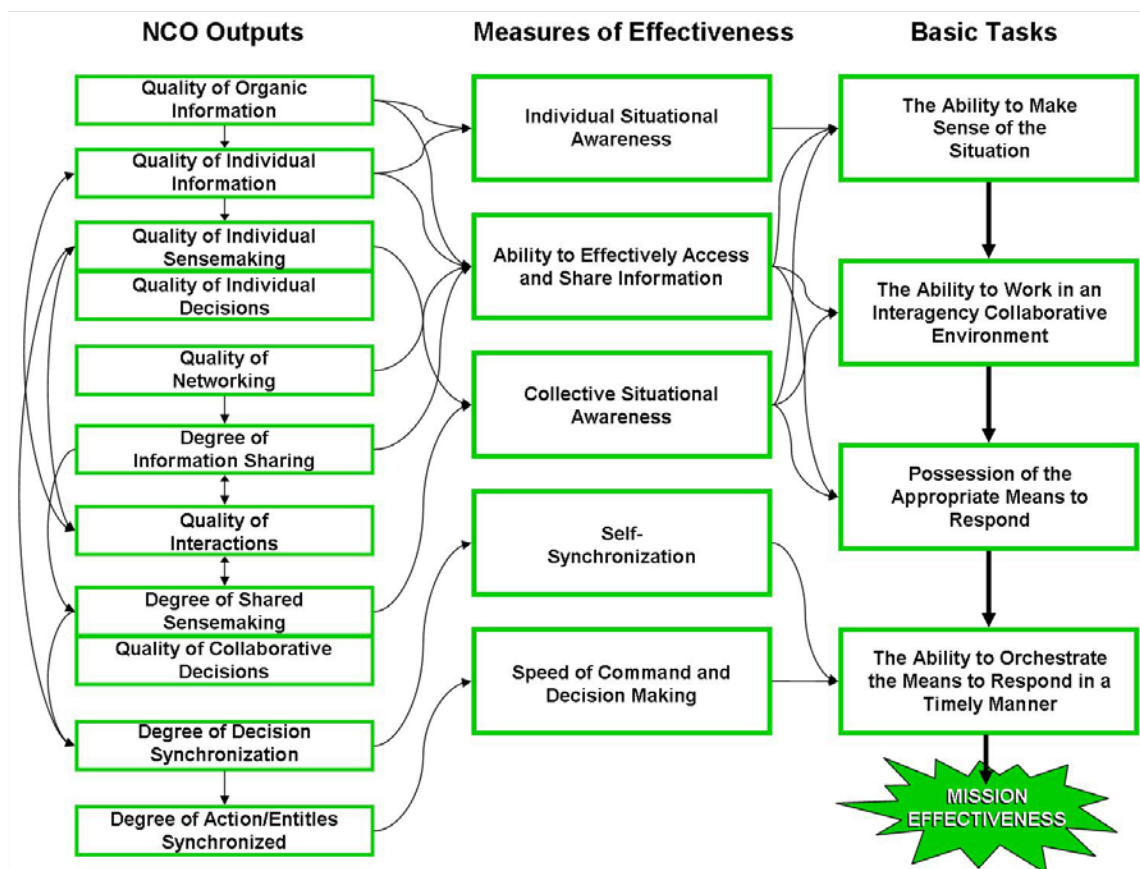
Figure 8.   Mapping of Network-Centric Operations Outputs to
Measures of Effectiveness

Each of the five measures of effectiveness, and overall mission effectiveness, will be evaluated using criteria developed as part of the network-centric operations conceptual framework.

1. Ability to Effectively Access and Share Information

The first measure of effectiveness is the ability to effectively access and share information. This function is a requirement within and among interagency partners tasked with performing emergency response operations and is critical to establishing network centricity with the response force. If this function is not performed adequately, the other measures of effectiveness will suffer, which will ultimately affect the accomplishment of the four basic tasks.

"Networking involves much more than the physical communication links between people and information systems that they use. Information systems in network-centric operations must produce coherent information that can be transformed into awareness and then understanding."[339] Information systems that support response operations must have the ability to adjust quickly to changing requirements due to the dynamic environment in which that information exists. These information systems must produce information that is both cohesive and flexible.[340]

Metrics to measure responders' and supporting agencies' ability to access and share information can be

---

[339] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 103.

[340] Ibid.

broken down into the categories of quality of organic information, quality of individual information, degree of information "share-ability", degree of shared information, and degree of networking as shown in the tables below.

Attribute	Definition
Objective Measures: Measures quality in reference to situation independent criteria	
Correctness	Extent to which information is consistent with ground truth
Consistency	Extent to which information is consistent with prior information
Currency	Age of information
Precision	Level of measurement detail of information item
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Extent to which information relevant to ground truth is collected
Accuracy	Appropriateness of precision of information for a particular use
Relevance	Proportion of information collected that is related to task at hand
Timeliness	Extent to which currency of information is suitable to its use

Table 3.   Quality of Organic Information Definitions (From Network-Centric Operations Conceptual Framework 2.0)

Attribute	Metric
Objective Measures: Measures quality in reference to situation independent criteria	
Correctness	Correspondence with ground truth (1 = no correspondence with ground truth, 5 = full correspondence with ground truth). Data matrix comprised of relevant information items estimates (for instance: detection, ID, location, heading, etc.)
Consistency	Degree of 'deviation' from previous information
Currency	Age of information
Precision	Level of measurement detail of information item
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Percentage of ground truth relevant and needed information collected
Accuracy	Degree to which precision matches what is needed (1 = no match, 5 = high degree of matching between precision level needed and available)
Relevance	Proportion of information collected that is related to task at hand
Timeliness	Degree to which currency matches what is needed (1 = no match, 5 = high degree of matching between currency level needed and available)

Table 4.   Quality of Organic Information Metrics (From Network-Centric Operations Conceptual Framework 2.0)

Organic information is information that is derived from the unit, community, or response organization. In other words, organic information is information derived from or gathered by an entity that is not shared and is unavailable to the network and, for the most part, remains local to the entity.[341]

---

[341] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 104.

Attribute	Definition
Objective Measures: Measures quality in reference to situation independent criteria	
Correctness	Extent to which information obtained and utilized is consistent with ground truth
Consistency	Extent to which information is consistent with relevant and already existing information (across time) for a given decision making
Currency	Age of information
Precision	Level of measurement detail of information item
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Extent to which information relevant to ground truth is obtained
Accuracy	Degree to which precision matches what is needed for a particular use
Relevance	Proportion of information retrieved that is related to task at hand
Timeliness	Extent to which currency of information is suitable to its use
Uncertainty	Subjective assessment of information uncertainty

Table 5.   Quality of Individual Information Definitions
(From Network-Centric Operations Conceptual Framework
2.0)

Attribute	Metric
Objective Measures: Measures quality in reference to situation independent criteria	
Correctness	Correspondence with ground truth (1 = no correspondence with ground truth, 5 = full correspondence with ground truth). Data matrix comprised of relevant information items (for instance: detection, ID, velocity, location, etc.)
Consistency	Degree of 'deviation' from previously existing information
Currency	Age of information
Precision	Level of measurement detail of information item
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Percentage of ground truth relevant and needed information
Accuracy	Degree to which precision matches what is needed (1 = no match, …, 5 = high degree of matching between precision)
Relevance	Proportion of information that is related to task at hand
Timeliness	Degree to which currency matches what is needed (1 = no match, …, 5 = high degree of matching between currency level needed and available)
Uncertainty	Individual's perception of information uncertainty (1 = highly uncertain, …, 5 = highly certain)

Table 6.   Quality of Individual Information Metrics (From
Network-Centric Operations Conceptual Framework 2.0)

Individual information is the first form of non-organic information that entities in the response network encounter. "Individual information refers to all the information available or presented to an entity. Individual information provides the basis for awareness and understanding. It differs from organic information, because it also includes information that has been distributed over a network and obtained through some interaction."[342]

---

[342] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 106.

Attribute	Definition
Quantity of Posted Information	Amount of collected information that is posted
Ease of Use of Posted Information	Amount of information which is in a format that facilitates use across a range of possible applications. Dependent upon the extent of metadata and application independent data on network
Retrievability of Information	Extent to which posted information is easily retrieved Determined by the following: Awareness of Information: Degree to which the existence of the information is advertised to force member Access to Information: Degree to which access to information is controlled Metadata of Information: Degree to which information has labels describing what it is and how it may be used (facilitates indexing and searching)

Table 7.   Degree of Information "Share-ability" Definitions (From Network-Centric Operations Conceptual Framework 2.0)

Attribute	Metric
Quantity of Posted Information	Percent of collected information posted
Ease of Use of Posted Information	Percent of information with meta-tagging Percent of application independent information
Retrievability of Information	Categorical rating (1 = not retrievable,..., 5 = highly retrievable)

Table 8.   Degree of Information "Share-ability" Metrics (From Network-Centric Operations Conceptual Framework 2.0)

"Information share-ability refers to a network's ability to accept, index, and transmit particular pieces of information, including data elements, data files, and streams of information quickly and accurately. Information

share-ability is only concerned with whether or not it is easy to make data or information available to the network, and whether data and information can be found by force entities."[343] "It only considers whether or not what is submitted to the network is indexed correctly, stored without degradation, transmitted accurately and on demand, and presented to the receiver in a manner equivalent to what was initially submitted. The degree of information share-ability is influenced by the physical properties of the network, including the transmission speed, accuracy, and the support for posting and retrieving different types of information."[344]

---

[343] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 107.

[344] Ibid.

Attribute	Definition
Objective Measures: Measures quality in reference to situation independent criteria	
Extent	Proportion of information in common across force entities, within and across communities of interest (CoI) Proportion of force entities that share an information item
Correctness	Extent to which shared information is consistent with ground truth
Consistency	Extent to which shared information is consistent within and across CoI
Currency	Age of shared information
Precision	Level of measurement detail of shared information item
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Extent to which shared information relevant to ground truth is obtained
Accuracy	Appropriateness of precision of shared information for a particular use
Relevance	Proportion of shared information retrieved that is related to task at hand
Timeliness	Extent to which currency of shared information is suitable to its use

Table 9.   Degree of Shared Information Definitions (From Network-Centric Operations Conceptual Framework 2.0)

Attribute	Metrics
Objective Measures: Measures quality in reference to situation independent criteria	
Extent	Percentage of force entities that share an information item
Correctness	Correspondence with ground truth 1 = no correspondence,…, 5 = high correspondence
Consistency	1 = high deviation from within and across CoI,…, 5 = low deviation from within and across CoI
Currency	Age of information (seconds, minutes, days, weeks, etc.)
Precision	1 = low granularity of information, …, 5 = high granularity of information
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Percentage of critical information shared
Accuracy	Confidence rating
Relevance	Percentage of information pertaining to the task at hand
Timeliness	Time interval between creation of information and when the information is shared

Table 10.   Degree of Shared Information Metrics (From Network-Centric Operations Conceptual Framework 2.0)

Shared information is information that is derived from the network and/or exchanged on the network. The concept of extent separates the attributes for shared information from those for individual information.[345] This attribute measures the proportion of information that is held in common across response force entities.[346] "The degree of shared information captures both the quality of the shared information and the extent to which information is shared."[347]

---

[345] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 108.

[346] Ibid.

[347] Ibid.

Attribute	Definition
Reach	Number of force elements on the net
Quality of Service	Ability of network to provide a variety of communications services
Network Assurance	Extent to which network provides services that facilitate the assurance of information in the areas of privacy, availability, integrity, authenticity, and non-repudiation
Network Capacity	Measure of how large (in terms of number of nodes) the network can expand to before notable decreases in quality of service and throughput

Table 11.   Degree of Networking Definitions (From Network-Centric Operations Conceptual Framework 2.0)

Attribute	Metric
Reach	Percent of nodes that can communicate in desired access modes, information formats, and applications
Quality of Service	Vector of performance metrics, including average bandwidth provided (available and bottleneck), packet delay, delay jitter, average down time, and data loss
Network Assurance	Categorical rating from 1 = not secure to 5 = highly secure based on a vector of factors (privacy, availability, integrity, authenticity, and non-repudiation)
Network Capacity	Maximum size of network (number of nodes) that can be simultaneously connected in desired access modes (with requisite throughput and quality of service)

Table 12.   Degree of Networking Metrics (From Network-Centric Operations Conceptual Framework 2.0)

In addition to the degree of networking, network agility should be measured to determine its suitability to be employed in the adverse conditions often encountered during response operations.

Attribute	Definition
Robustness	Effectiveness of network across a range of operational conditions (environments, mission types)
Adaptability	Ability of network to quickly and efficiently: set up, shut down, and/or relocate
Responsiveness	Ability of network to quickly and appropriately respond to changing operational needs
Resilience	Ability of network to perform effectively despite attacks and or perturbations
Flexibility	Extent to which network supports multiple connectivity access modes

Table 13.   Network Agility Definitions (From Network-Centric Operations Conceptual Framework 2.0)

Attribute	Metric
Robustness	Number of differing conditions/environments over which network is capable of operating at a given level of effectiveness (baseline level determined by simulation, analysis, empirical analysis, etc.) Number of tasks/missions which the network is capable of operating at a given level of effectiveness (baseline level determined by simulation, analysis, empirical analysis, etc.)
Adaptability	Time and effort (man hours) required to set up, take down and relocate network (or significant sub-components of network)
Responsiveness	The timeliness and appropriateness of the response to a change (1 = not appropriate nor timely, … 5 = highly appropriate and timely) baseline level determined by simulation, analysis, empirical analysis, etc.)
Resilience	Number and type of nodes removed before degradation in quality of service occurs Time lag between attack/damage and degradation of quality of service
Flexibility	Number and type of connectivity modes supported (RF, wire, etc.)

Table 14.   Network Agility Metrics (From Network-Centric Operations Conceptual Framework 2.0)

A network that exhibits a high degree of agility is ideally suited for network-centric response applications. Agility in the network will lead to agility in the response

force, which will benefit mission effectiveness across all four basic tasks required to operate in the Information Age.

Once it is determined that core information access and sharing is possible, the contribution of this information to building individual and collective shared awareness should be assessed.

2.   Individual and Collective Situational Awareness

Individual and collective sensemaking lead to individual and collective (shared) situational awareness. The creation and maintenance of situational awareness is critical to the completion of the first basic task, the ability to make sense of the situation. Individual and collective situational awareness can be broken down into the categories of individual awareness and understanding and shared awareness and understanding.

Attribute	Definition
Objective Measures: Measures quality in reference to criteria that are independent of the situation	
Correctness	Extent to which awareness is consistent with ground truth
Consistency	Extent to which awareness is consistent with relevant awareness at an earlier time period
Currency	Time lag of awareness
Precision	Level of granularity of awareness
Fitness for Use Measures: Measures quality in reference to criteria that are determined by the situation	
Completeness	Extent to which awareness necessary to form understanding is obtained
Accuracy	Appropriateness of precision of awareness for a particular use
Relevance	Extent to which awareness obtained is related to task at hand
Timeliness	Extent to which currency of awareness is suitable to its use
Uncertainty	Subjective assessment of awareness uncertainty

Table 15.   Individual Awareness Definitions (From Network-
Centric Operations Conceptual Framework 2.0)

Attribute	Metric
Objective Measures: Measures quality in reference to situation independent criteria	
Correctness	Categorical rating (1 = highly inconsistent with ground truth, …, 5 = highly consistent with ground truth)
Consistency	Degree of deviation from awareness from previous time period
Currency	Time lag of awareness
Precision	Level of granularity of awareness (1 = low,…5 = high)
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Extent to which awareness is necessary to form understanding is obtained: 1 = incomplete,…, 5 = complete and sufficient
Accuracy	Degree to which precision matches what is needed (1 = no match, …, 5 = high degree of matching between precision level needed and available)
Relevance	Proportion of time spent gaining awareness that is related to task at hand (not time spent distracted, irrelevant, etc.)
Timeliness	Degree to which currency matches what is needed (1 = no match, …, 5 = high degree of matching between currency level needed and available)
Uncertainty	Perceived uncertainty of awareness (1 = highly uncertain, … ,5 = highly certain)

Table 16.   Individual Awareness Metrics (From Network-Centric Operations Conceptual Framework 2.0)

"Timeliness reflects the degree to which the currency of the information comprising awareness suitably supports the use of this awareness for building understanding and making decisions. In other words, timeliness expresses the degree to which the currency of awareness provides an adequate window of decision making opportunity for the decision making staff."[348]   Granularity is the level of detail at which information is viewed or understood.

---

[348] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 111-112.

Attribute	Definition
Objective Measures: Measures quality in reference to situation independent criteria	
Correctness	Extent to which understanding is consistent with ground truth
Consistency	Extent to which understanding is internally consistent with prior understanding
Currency	Time lag of understanding
Precision	Level of granularity of understanding
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Extent to which understanding necessary for decision making is obtained
Accuracy	Appropriateness of precision of understanding for a particular use
Relevance	Extent to which understanding obtained is related to task at hand
Timeliness	Extent to which currency of understanding is suitable to its use
Uncertainty	Subjective assessment of understanding uncertainty

Table 17.   Individual Understanding Definitions (From Network-Centric Operations Conceptual Framework 2.0)

Attribute	Metric
Objective Measures: Measures quality in reference to situation independent criteria	
Correctness	Correspondence with ground truth-correlation coefficient (1= no correspondence, … 5 = full correspondence between individual's understanding and ground truth)
Consistency	Degree of 'deviation' from understanding gained from previous time period
Currency	Time lag of understanding
Precision	Level of granularity of understanding
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Complete, incomplete but sufficient, incomplete
Accuracy	Degree to which precision matches what is needed (1= no match, …, 5 = high degree of matching between precision level needed and available)
Relevance	Proportion of time spent gaining understanding that is related to task at hand
Timeliness	Degree to which currency matches what is needed (1 = no match, …, 5 = high degree of matching between currency level needed and available)
Uncertainty	Perceived uncertainty of understanding (1= highly uncertain, … ,5 = highly uncertain)

Table 18.   Individual Understanding Metrics (From Network-Centric Operations Conceptual Framework 2.0)

Collective or shared awareness and understanding build upon the definition and metrics applied to individual response elements.

Attribute	Definition
Objective Measures: Measures quality in reference to situation independent criteria	
Extent	Proportion of awareness in common across force entities, within and across communities of interest (CoI) Proportion of force entities that share a given awareness
Correctness	Extent to which shared awareness is consistent with ground truth
Consistency	Extent to which shared awareness is consistent within / across CoI
Currency	Time lag of shared awareness
Precision	Level of granularity of shared awareness
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Extent to which relevant shared awareness is obtained
Accuracy	Appropriateness of precision of shared awareness for a particular use
Relevance	Proportion of shared awareness obtained related to the task at hand
Timeliness	Extent to which currency of shared awareness is suitable to its use
Uncertainty	Subjective assessment of confidence in shared awareness Decision maker's degree of belief/measure of the decision maker's lack of knowledge

Table 19.   Shared Awareness Definitions (From Network-Centric Operations Conceptual Framework 2.0)

Attribute	Metrics
Objective Measures: Measures quality in reference to situation independent criteria	
Extent	1 = low awareness in common across force entities, within and across communities of interest (CoI), …, 5 = high awareness in common across force entities, within and across communities of interest (CoI) 1 = low number of force entities that share a given awareness, …, 5 = High number of force entities that share a given awareness
Correctness	Correspondence with ground truth 1 = no correspondence,…, 5 = high correspondence
Consistency	1 = high deviation from within and across CoI,…, 5 = low deviation from within and across CoI
Currency	Age of information (seconds, minutes, days, weeks, etc..)
Precision	1 = low granularity of awareness, …, 5 = high granularity of awareness
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Extent to which shared awareness is necessary to form shared understanding is obtained: 1 = incomplete,…, 5 = complete and sufficient
Accuracy	Degree to which precision matches what is needed (1 = no match, 5 = high degree of matching between precision level needed and available)
Relevance	Proportion time spent gaining shared awareness that is related to task at hand (not time spent distracted, irrelevant, etc.)
Timeliness	Degree to which currency matches what is needed (1 = no match, 5 = high degree of matching between currency level needed and available)
Uncertainty	Perceived uncertainty of shared awareness (highly certain, … ,highly uncertain)

Table 20.   Shared Awareness Metrics (From Network-Centric Operations Conceptual Framework 2.0)

Attribute	Definition
Objective Measures: Measures quality in reference to situation independent criteria	
Extent	Proportion of understanding in common across force entities, within and across communities of interest (CoI) Proportion of force entities that share a given understanding
Correctness	Extent to which shared understanding is consistent with ground truth
Consistency	Extent to which shared understanding is consistent within and across CoI
Currency	Time lag of shared understanding
Precision	Level of granularity of shared understanding
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Extent to which relevant shared understanding is obtained
Accuracy	Appropriateness of precision of shared understanding for a particular use
Relevance	Proportion of shared understanding that is related to task at hand
Timeliness	Extent to which currency of shared understanding is suitable to its use
Uncertainty	Subjective assessment of confidence in shared understanding

Table 21.   Shared Understanding Definitions (From Network-Centric Operations Conceptual Framework 2.0)

Attribute	Metrics
Objective Measures: Measures quality in reference to situation independent criteria	
Extent	Proportion of Command and Control (C2) Elements that share a given understanding
Correctness	Percentage of key elements of shared understanding obtained that are consistent with ground truth
Consistency	Proportion of key elements of shared understanding which are held in common
Currency	Time lag of shared understanding
Precision	Level of granularity of shared understanding
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Completeness	Percentage of key elements of shared understanding obtained
Accuracy	Degree to which precision matches what is needed (1 = no match, 5 = high degree of matching between precision level needed and available)
Relevance	Proportion of time spent gaining shared understanding that is related to task at hand
Timeliness	Appropriateness of time required to achieve shared understanding in relation to mission needs
Uncertainty	Perceived uncertainty of shared understanding (1 = highly uncertain, … ,5 = highly uncertain)

Table 22.   Shared Understanding Metrics (From Network-Centric Operations Conceptual Framework 2.0)

When individual and collective situational awareness are combined with the ability to effectively access and share information, these factors lead to completion of the second and third basic tasks; the ability to work in an interagency collaborative environment and possession of the appropriate means to response.   Resources are still required to possess the appropriate means to respond, but rapid identification and allocation of these resources is dependant on collective situational awareness and the ability to effectively access and share information.

3. Self-synchronization

Synchronization is defined as purposeful arrangement in time and space and falls into one of the three categories depicted in Figure 9 below.[349]

| **Conflicted** | **Deconflicted** | **Synergistic** |
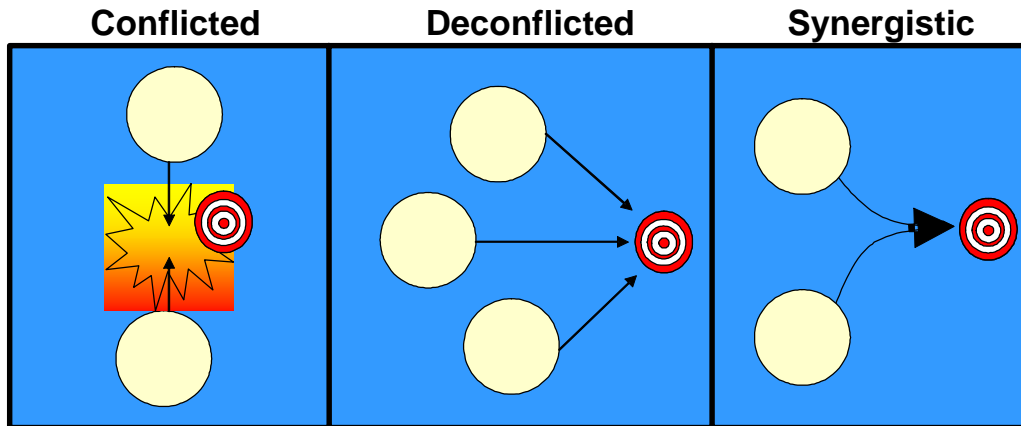
Figure 9.   Synchronization Categories (From Network-Centric Operations Conceptual Framework 2.0)

Conflicted actions occur when two or more actions or entities interfere with one another.[350] An example would be one agency sending additional response personnel to perform mission tasks at a location that was ordered to be evacuated.

Deconflicted actions occur when actions or entities are prevented from interfering with one another by separation in time, space, or both.[351] An example would be assigning U.S. Coast Guard search and rescue (SAR) assets

---

[349] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 90.

[350] Ibid., 91.

[351] Ibid.

responsibility for conducting SAR in a defined geographic area while assigning State Urban SAR assets a separate area of responsibility.

Synergistic actions occur when actions and entities reinforce one another's desirable impacts on the operating environment.[352] One example would be combining mass sheltering operations with medical assessment teams to separate sick or infected survivors from the general population as they arrive at mass shelter locations, thus preventing additional infections on a large scale.

The response environment can be highly dynamic and feature new and changing threat conditions, unforeseen challenges, and novel situations. Individuals or organizations empowered with a high degree of situational awareness can recognize changes and take action in this environment without further specific command direction through self-synchronization.

Self-synchronization can be measured by assessing the degree of decisions and plans that are synchronized, and the degree of actions and entities synchronized.

Attribute	Definition
Synchronized Decisions/Plans	Proportion of decisions/plans that are conflicted, de-conflicted or synergistic

Table 23.   Degree of Decisions/Plans Synchronized Definitions (From Network-Centric Operations Conceptual Framework 2.0)

---

[352] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 91.

Attribute	Metrics
Synchronized Decisions/Plans	-1 = conflicted, 0 = deconflicted, 1 = synergistic

Table 24.   Degree of Decisions/Plans Synchronized Metrics (From Network-Centric Operations Conceptual Framework 2.0)

Because each jurisdiction maintains a response plan that should strive to be based on the NRP and the NIMS, explicit, written plans requiring strict compliance are not essential in all response operations. In many dynamic situations, particularly in network-centric response operations with very flat organizational structures and doctrines that encourage self-synchronization, plans may be largely implicit, expressed very briefly, and depend on prior training, shared mental models, and the intent of the unified command.[353]

Attribute	Definition
Synchronized Actions	Proportion of actions that are conflicted, deconflicted, or synergistic
Synchronized Entities	Proportion of force entities whose positions are conflicted, deconflicted, or synergistic

Table 25.   Degree of Actions/Entities Synchronized Definitions (From Network-Centric Operations Conceptual Framework 2.0)

---

[353] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 92.

Attribute	Metrics
Synchronized Actions	-1 = conflicted, 0 = deconflicted, 1 = synergistic
Synchronized Entities	-1 = conflicted, 0 = deconflicted, 1 = synergistic

Table 26.   Degree of Actions/Entities Synchronized Metrics (From Network-Centric Operations Conceptual Framework 2.0)

Self-synchronization of elements of the response force is critical to completing the fourth basic task to operate in the Information Age, the ability to orchestrate the means to respond in a timely manner. Individuals and organizations that can, based on overall guidance, quickly assess and react to changes in the environment will greatly shorten the response timeline. Entities that take these actions in a synchronized manner will increase their relative contribution to increased mission effectiveness.

4.   Speed of Command and Decision Making

Despite the network-centric principle of compressed operations to eliminate procedural boundaries between agencies and within processes so that collaborative operations are conducted at the lowest organizational levels possible to achieve rapid and decisive effects, the human interface at the command level can be the largest obstacle to effective response operations. The military experience with NCW has shown that increased access of information at the command level has, in some circumstances, led to micro management of tactical forces which has countered the benefits of self-synchronization

and speed of command.[354] "Senior leaders often intervened at the tactical level not because it was necessary, but simply because they could."[355]

Measurement and assessment of the quality and agility of individual and collaborative decision making is critical to ensure that network-centric theory is correctly applied to response operations to maintain tactical initiative at lower levels of the response force while avoiding the desire to over-manage operations at all command levels.

---

[354] Lambeth, *The Downside of Network-Centric Warfare*, 86; Barnett, *The Seven Deadly Sins of Network-Centric Warfare*, 36.

[355] Lambeth, *The Downside of Network-Centric Warfare*, 86.

Attribute	Definition
Objective Measures: Measures quality in reference to situation independent criteria	
Consistency	Extent to which decisions are internally consistent with prior understanding and decisions
Currency	Time taken to make decision (start time- external signal)
Precision	Level of granularity of decisions
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Appropriate-ness	Extent to which decisions are consistent with existing understanding, command intent and values
Completeness	Extent to which relevant decisions encompass the necessary: Depth: range of actions and contingencies included Breadth: range of force elements included Time: range of time horizons included
Accuracy	Appropriateness of precision of decision (plan, directives) for a particular use
Relevance	Extent to which decision is significant to task at hand
Timeliness	Extent to which currency of decision making is suitable to its use
Uncertainty	Subjective assessment of decision uncertainty
Mode of Decision Making	Type of decision making process utilized (naturalistic, deliberate, incremental, or other)

Table 27.   Quality of Individual Decisions Definitions
(After Network-Centric Operations Conceptual Framework
2.0)

Attribute	Metric
Objective Measures: Measures quality in reference to situation independent criteria	
Consistency	Categorical rating 1 = highly inconsistent, …, 5 = highly consistent
Currency	Time (minutes, days, weeks,…) taken to make a decision
Precision	Level of granularity of decision 1 = low granularity, …,5 = high granularity
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Appropriate-ness	Decision consistency with higher command intent 1 = highly inconsistent,…5 = highly consistent
Completeness	1 = incomplete and insufficient, 2 = incomplete but sufficient, 3 = complete
Accuracy	1 = inappropriate decision,…, 5 = very appropriate decision (based on established criteria)
Relevance	1 = irrelevant to task at hand, …, 5 = very relevant to task at hand
Timeliness	Extent to which currency of a decision is appropriate to the mission
Uncertainty	Perceived uncertainty of decision (1 = highly uncertain, … ,5 = highly uncertain)
Mode of Decision Making	Mode of Decision making (naturalistic, deliberate, incremental, or other)

Table 28.   Quality of Individual Decisions Metrics (After Network-Centric Operations Conceptual Framework 2.0)

Attribute	Definition
Robustness	Degree to which decision is dominant across a range of situations
Resilience	Degree to which decision is applicable under degradation conditions
Flexibility	Degree to which decision allows force entities to maintain flexibility (i.e., incorporates multiple ways of succeeding)
Adaptability	Degree to which decision facilitates force entities' ability to alter the decision, decision making participants and/or decision making process and implement appropriate modifications

Table 29.   Agility of Individual Decisions Definitions (From Network-Centric Operations Conceptual Framework 2.0)

Attribute	Metric
Robustness	1 = decision is not dominant to any situation, …, 5 = dominant across all situations
Resilience	1 = not applicable under degradation, …, 5 = very applicable under degradation
Flexibility	1 = does not allow force entities to be flexible,…, 5 = allows force entities to be very flexible
Adaptability	1 = very rigid, no room for entities to alter decision,…, 5 = facilitates entities ability to alter the decision

Table 30.   Agility of Individual Decisions Metrics (From Network-Centric Operations Conceptual Framework 2.0)

In addition to the attributes of individual decisions assessed, collaborative decisions involve the additional measure of extent.[356] Extent is defined in this context as the proportion of force entities effectively involved in reaching a collaborative decision.   In addition, the definitions of other measures are expanded to reflect the shared nature of the process. For example, appropriateness of collaborative decisions is measured with respect to the

---

[356] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 122.

degree it reflects shared understanding, unified command intent, and shared team or organizational values.[357]

Attribute	Definition
Objective Measures: Measures quality in reference to situation independent criteria	
Extent	Proportion of force entities that reach a collaborative decision
Consistency	Extent to which decisions are in agreement across force entities, within and across CoI
Currency	Time lag of decisions
Precision	Level of granularity of decisions
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Appropriateness	Extent to which decisions are consistent with existing shared understanding, command intent and shared team values
Completeness	Extent to which relevant decisions encompass the necessary: Depth: range of actions and contingencies included Breadth: range of force elements included Time: range of time horizons included
Accuracy	Appropriateness of precision of decisions for a particular use
Relevance	Proportion decisions that are important to the accomplishment of the task at hand
Timeliness	Extent to which currency of decision making is suitable to its use
Uncertainty	Inter-subjective assessment of confidence in decisions
Risk Propensity	Extent of risk aversion
Mode of Decision Making	Type of collaborative decision making structure utilized (authoritative decision making, consensus building, majority rule, etc.)

Table 31.   Quality of Collaborative Decisions Definitions
(After Network-Centric Operations Conceptual Framework
2.0)

---

[357] Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 122.

Attribute	Metrics
Objective Measures: Measures quality in reference to situation independent criteria	
Extent	Percentage of Command and Control (C2) elements participating in collaboration
Consistency	Extent to which decisions are internally consistent with prior understanding and decisions 1 = low correlation with prior understanding and decisions,…, 5 = high understanding with prior understanding and decisions
Currency	Time required to make the decision
Precision	Level of granularity of decision 1 = low granularity, …,5 = high granularity
Fitness for Use Measures: Measures quality in reference to situation dependent criteria	
Appropriateness	Extent to which a decision is consistent with higher command intent (1 = low, … 5 = high) Extent to which a decision is consistent with shared understanding (1 to 5) Extent to which a decision is consistent with shared values (1 to 5)
Completeness	1 = incomplete and insufficient, 2 = incomplete but sufficient, 3 = complete
Accuracy	1 = inappropriate decision,…, 5 = very appropriate decision (based on established criteria)
Relevance	1 = irrelevant to task at hand, …, 5 = very relevant to task at hand
Timeliness	Extent to which currency of a decision is appropriate to the mission
Uncertainty	Perceived uncertainty of decision (1 = highly uncertain, … ,5 = highly uncertain)
Risk Propensity	1 = low aversion to risk, …, 5 = high risk aversion
Mode of Decision Making	Type of collaborative decision making structure utilized (authoritative decision making, consensus building, majority rule, etc.)

Table 32.   Quality of Collaborative Decisions Metrics (After Network-Centric Operations Conceptual Framework 2.0)

Attribute	Definition
Robustness	Degree to which collaborative decision is dominant across a range of situations and degradation conditions
Flexibility	Degree to which collaborative decision allows force entities to maintain flexibility (i.e., incorporates multiple ways of succeeding)
Responsiveness	Degree to which collaborative decision is relevant and timely
Innovativeness	Degree to which collaborative decision reflects novel ways to perform known tasks and/or develops new ways of doing novel tasks
Adaptability	Degree to which collaborative decision facilitates force entities' ability to alter the decision, decision making participants and/or decision making process and implement appropriate modifications

Table 33.   Agility of Collaborative Decisions Definitions
(From Network-Centric Operations Conceptual Framework
2.0)

Attribute	Metrics
Robustness	1 = decision is not dominant to any situation, …, 5 = dominant across all situations
Flexibility	1 = not applicable under degradation, …, 5 = very applicable under degradation
Responsiveness	1 = does not allow force entities to be flexible,…, 5 = allows force entities to be very flexible
Innovativeness	1 = very rigid, no room for entities to alter decision,…, 5 = facilitates entities ability to alter the decision
Adaptability	1 = decision is not dominant to any situation, …, 5 = dominant across all situations

Table 34.   Agility of Collaborative Decisions Metrics (From
Network-Centric Operations Conceptual Framework 2.0)

When combined with self-synchronization, overall response force agility will be enhanced by agility of command elements through their individual and collaborative decisions.

5.   Overall Response Mission Effectiveness

The ultimate goal of the implementation of network-centric response is to increase response mission effectiveness while adhering to the values of empowerment, service, transparency, speed, agility, and teamwork. As stated at the end of the first chapter, a robustly networked team of interagency responders will improve information sharing; information sharing will enhance the quality of information and shared situational awareness; shared situational awareness will enable collaboration and self-synchronization, which enhances sustainability and speed of command and decision making. These, in turn, will dramatically increase response mission effectiveness.

Attribute	Definition
Achievement of Objectives	Degree to which strategic, political, life-saving, economic, social, information, and infrastructure objectives were achieved
Agility	The degree to which response force entities were robust, resilient, flexible, responsive, innovative, and adaptable
Time	Time required to achieve objective
Efficiency	Total cost of achieving objective

Table 35.   Response Mission Effectiveness Definitions (After Network-Centric Operations Conceptual Framework 2.0)

Attribute	Metrics
Achievement of Objectives	Extent to which the unified command's intent was achieved 1 = intent was not achieved, …, 5 = intent was achieved
Agility	See above
Time	Months, days, hours needed to achieve the mission
Efficiency	Vector of cost-benefit metrics

Table 36.   Response Mission Effectiveness Metrics (After Network-Centric Operations Conceptual Framework 2.0)

Mission effectiveness must be baselined and then reassessed to determine the overall impact of applying network-centric tenants, principles, technology, and methodologies to response operations.

Effectiveness metrics share with synchronization metrics the need to identify an appropriate level of analysis.[358]   When applying the metrics derived from the network-centric operations conceptual framework to various aspects of response across all governmental levels, that is when it is used to evaluate specific areas of past or future response or utilized in specific experimentation efforts, the key units are clearly missions.[359]   Missions may include the preservation of life and property, search and rescue, damage assessment, defense support of civil authorities, containment of lethal effects, public affairs campaigns, or maintenance of civil order following a disaster.   However, there will often be layers of missions assigned to different elements of the response force, in different functional areas (logistics, intelligence, etc.), and over time.   Therefore, the degree of mission

[358]   Alberts and Garstka, *Network Centric Operations Conceptual Framework Version 2.0*, 97.

[359]   Ibid.

accomplishment may differ across these arenas and the
relevant metrics will include both assigning values to
individual metrics and "roll up" calculations that create
mission accomplishment indices.[360] As with synchronization
metrics, time or periods of time may need to be considered
to accurately reflect the effectiveness of overall response
efforts.

_____

    [360] Alberts and Garstka, *Network Centric Operations Conceptual
Framework Version 2.0*, 97.

VI. CONCLUSIONS

> So far, across this new landscape of conflict, the edge has gone to the networks. Hierarchy-oriented states must learn to transform themselves along networked lines, or they will face the increasingly daunting prospect of struggling against a rising tide of both civil and uncivil networks enabled, and impelled forward, by the information revolution.[361]

Our current response operations are characterized by the inability to efficiently produce a collaborative and effective response to incidents of national significance and address the challenges and leverage the opportunities of the Information Age.

Massive funding of homeland security and response agencies has made little impact on our nation's ability to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies since the attacks of 9/11. Transformational change is required to ensure that all levels of government across the nation have the capability to work efficiently and effectively together, using a comprehensive national approach to domestic incident management.

The current deficiencies in response in the areas of communications, information sharing, situational awareness, collaboration, and establishment of a unified command and interoperability issues in these areas must be addressed if the nation's ability to respond to disasters is going to improve beyond its current capabilities.

---

[361] Ronfeldt and Arquilla, *Networks, Netwars, and the Fight for the Future*, 1-25.

The military has adapted network-centric tenants and principles from business applications to effectively operate in the Information Age and increase mission effectiveness through employment of a robustly networked force to improve information sharing, the quality of information, and shared situational awareness. These factors lead to self-synchronization, collaboration, and improved speed of command which dramatically increase mission effectiveness.

Governmental strategic vision for improved response effectiveness suggests the implementation of network-centric operations. The further adaptation of network-centric principles from warfare to response is facilitated by the similarities between the challenges, operating environment, and requirements present in military and emergency response operations.

The tenants and principles of network-centric operations can be adapted by responders and supporting agencies at all levels of government to address current deficiencies and increase response mission effectiveness by enabling them to accomplish the four basic tasks required to operate in the Information Age.

The implementation of a network-centric response strategy is both technically and organizationally feasible if key hurdles are identified and effectively addressed. Transformation must include not only technological and organizational changes, but must include the way in which we train, organize, and equip our forces. While the technical network is an enabling force, the human networking that results from network-centric response operations is the key to empowering individuals at all

levels of government and decision making to efficiently produce significantly improved emergency response mission effectiveness.

The procurement of interoperable voice and data communications technology, the establishment of standards for its use, and comprehensive regional communications planning is the critical first step on the road to network-centric response.

Due to the potential vast geographic and multi-jurisdictional scope of future disasters, communications interoperability on a national level that exhibits the optimum level characteristics of the SAFECOM Interoperability Continuum (Figure 5) is required. Without a backbone of communications technology that exhibits interoperability; survivability; scalability, flexibility, and adaptability; security; spectrum and bandwidth availability; and affordability, response operations at all levels of government cannot make significant improvements in response mission effectiveness.

Strategic Federal guidance may be required to achieve a significant degree of network-centricity in response operations due to the national scope of response operations, but should be tempered with State and local stakeholder empowerment and input and responder community buy in. Stakeholder identification and engagement, particularly at the State and local level, in the development of operating standards and technology will serve as a catalyst to future organizational collaboration and a willingness to share information through the network.

Once the enabling technology is procured or adapted to network-centric response operations, it is important to "get the theory right". Response agencies should learn from the strengths and weaknesses of the military's adaptation of network-centric operating principles in the form of network-centric warfare and adopt best practices while avoiding any drawbacks that have been observed by deviating from network-centric operations core tenants and principles. Adherence to the values of empowerment, service, transparency, speed, agility, and teamwork is critical to obtaining and maintaining critical tactical-level stakeholder support of network-centric response operations.

Finally, response organizations must continue to research further benefits to be derived from the application of network-centric response operations that have not been experienced by business organization or the military. As network-centric response theory and employment continues to evolve, future process innovation and new process employment could lead to greater mission effectiveness that is not currently envisioned by today's advocates of network-centric theory.

Future research should focus on practical application of network-centric response technology, tenants, and principles in an operational environment and assessment of the impact on mission effectiveness through the use of metrics adapted from the network-centric operations conceptual framework.

LIST OF REFERENCES

Information Sharing Environment Implementation Plan. Washington DC: Office of the Director of National Intelligence, Program Manager, Information Sharing Environment (accessed November 29, 2006).

"Center Outlines Network Centric Warfare Concept's Challenges." *Defense Daily* 209, no. 56 (March 23, 2001): 1, http://proquest.umi.com/pqdweb?did=72676666&Fmt=7&clientId=65345&RQT=309&VName=PQD.

Aarholt, Eldar and Olav Berg. *Network Centric Information Structure - Crisis Information Management*. Lysaker, Norway: Defence Division Teleplan AS, June 2004.

Ahituv, N., M. Igbaria, and A. Sella. "The Effects of Time Pressure and Completeness of Information on Decision Making." *Journal of Management Information Systems* 15, no. 2 (Fall 1998, 1998): 153-172 (accessed December 11, 2006).

Alberts, D. S. and J. J. Garstka. "Network Centric Operations Conceptual Framework Version 2.0." *U.S. Office of Force Transformation and Office of the Assistant Secretary of Defense for Networks and Information Integration (2004)* (accessed October 2, 2006).

Alberts, D. S., J. J. Garstka, R. E. Hayes, and D. A. Signori. *Understanding Information Age Warfare*. Washington DC: DoD Command and Control Research, 2001.

Alberts, D. S., J. J. Garstka, and F. P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority* CCRP Publications Distribution Center, 1999 (accessed September 29, 2006).

Alberts, D. S. and R. E. Hayes. *Power to the Edge: Command...Control...in the Information Age*. Information Age Transformation Series. Washington DC: DoD Command and Control Research, 2003.

Barnett, Thomas. "The Seven Deadly Sins of Network-Centric Warfare." *United States Naval Institute Proceedings* 125, no. 1 (January 1999): 36, http://proquest.umi.com/pqdweb?did=38107931&Fmt=7&client Id=65345&RQT=309&VName=PQD.

Bea, Keith. *Emergency Management Preparedness Standards: Overview and Options for Congress*. Washington DC: Congressional Research Service, 2004 (accessed November 27, 2006).

Borgu, A. "The Challenges and Limitations of Network Centric Warfare – The Initial Views of an NCW Skeptic." *Presentation to the Conference: Network Centric Warfare: Improving ADF [Air Defense Force] Capabilities through Network Enabled Operations* 17, (2003) (accessed September 17, 2006).

Bush, George W. "Homeland Security Presidential Directive-5, Management of Domestic Incidents." www.fas.org/irp/offdocs/nspd/hspd-5.html (accessed January 29, 2006).

———. "Homeland Security Presidential Directive-8, "National Preparedness"." www.fas.org/irp/offdocs/nspd/hspd-8.html (accessed January 29, 2006).

———. "National Strategy for Homeland Security." *Washington, DC: The White House, July* (2002): 1-72 (accessed December 9, 2006).

Carafano, J. J. "Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century." *Heritage Lectures* no. 812 (2003): 1-7 (accessed November 27, 2006).

Cebrowski, A. K. "Network-Centric Warfare." *Military Technology* 27, no. 5 (May 2003): 16, http://proquest.umi.com/pqdweb?did=358330571&Fmt=7&clien tId=65345&RQT=309&VName=PQD.

Cebrowski, A. K. and J. J. Garstka. "Network-Centric Warfare: Its Origin and Future." *United States Naval Institute Proceedings* 124, no. 1 (January 1998): 28, http://proquest.umi.com/pqdweb?did=25236401&Fmt=7&client Id=65345&RQT=309&VName=PQD.

192

Clausewitz, C., *On War* [Vom Kriege]. Translated and Edited by M. Howard and P. Paret. Rev. ed. Princeton, NJ: Princeton University Press, 1984.

Department of Homeland Security. *2006 National Interoperability Baseline Survey*. Washington DC: SAFECOM, Department of Homeland Security, 2006, http://www.safecomprogram.gov/SAFECOM/library/background /1295_2006national.htm (accessed December 11, 2006).

———. *National Preparedness Guidance*. Washington DC: DHS, 2005 (accessed June 16, 2006).

———. *Tactical Interoperable Communications Scorecards Summary Report and Findings*. Washington DC: Department of Homeland Security, 2007, http://www.dhs.gov/xlibrary/assets/grants-scorecard-report-010207.pdf (accessed January 4, 2007).

Director, Force Transformation, Office of the Secretary of Defense. *The Implementation of Network-Centric Warfare*. Washington DC: Director, Force Transformation, Office of the Secretary of Defense, January 5, 2005.

Federal Emergency Management Agency. *Summary of Post 9/11 Reports "Lessons Learned*." Washington DC: Federal Emergency Management Agency, 2002 (accessed November 27, 2006).

First Response Coalition. *A Failure to Communicate: A Stocktake of Government Inaction to Address Communications Interoperability Failures Following Hurricane Katrina*. Washington DC: The First Response Coalition, 2005 (accessed November 30, 2006).

Gaudiano, P., B. Shargel, E. Bonabeau, and B. Clough. *Swarm Intelligence: A New C2 Paradigm with an Application to Control of Swarms of UAVs*. Washington DC: Command and Control Research Program, 2003, http://pecolab.colorado.edu/augnet/papers/03swarm.pdf (accessed December 21, 2006).

Global Security. "Wideband Gapfiller System." Global Security. http://www.globalsecurity.org/space/systems/wgs.htm (accessed December 16, 2006).

Grimmett, Richard. *Terrorism: Key Recommendations of the 9/11 Commission and Recent Major Commissions and Inquiries*. Washington DC: Congressional Research Service, 2004 (accessed November 27, 2006).

Hiniker, Paul. "Estimating Situational Awareness Parameters for Net Centric Warfare from Experiments." Presentation, Defense Information Systems Agency, Falls Church, VA, www.dodccrp.org (accessed October 24, 2006).

Joch, Alan. "Communications Breakdown, First Responders Look for New Ways to Keep Communications Flowing in Emergencies." FCW.com. http://www.fcw.com/article91601-12-05-05-Print (accessed June 9, 2006).

Kim, W. Chan and Renee Mauborgne. *Blue Ocean Strategy*. Boston, Massachusetts: Harvard Business School Press, 2005.

Kind, Peter and Katharine Burton. *Information Sharing and Collaboration Business Plan*. Alexandria, Virginia: Institute for Defense Analyses, 2005 (accessed November 27, 2006).

Klein, Gary. *Sources of Power - How People Make Decisions*, edited by Devorah Klein, Rebecca Klein, Karen Getchell-Reiter, Diane Chiddester, Ken Clark, Michael Ames, Paula John and Rose Olszewski. Massachusetts: Massachusetts Institute of Technology, 1998.

Lambeth, B. S. "The Downside of Network-Centric Warfare." *Aviation Week & Space Technology* 164, no. 1 (January 2, 2006): 86, http://proquest.umi.com/pqdweb?did=958213261&Fmt=7&clientId=65345&RQT=309&VName=PQD.

Lapham, Donald. "1401 Technology Transfer Program." PowerPoint Briefing, Office of the Assistant Secretary of Defense for Homeland Defense, http://www.nlectc.org/training/nijconf.html (accessed November 5, 2006).

Leedom, Dennis. "Functional Analysis of the Next Generation Operating Picture." Presentation, Evidence Based Research Inc., Vienna, VA, www.dodccrp.org (accessed October 24, 2006).

National Commission on Terrorist Attacks upon the United
    States (The 9/11 Commission). *The 9/11 Commission
    Report*. Washington DC: National Commission on Terrorist
    Attacks upon the United States, 2004.

National Commission on Terrorist Attacks Upon the United
    States (The 9/11 Commission). *The 9/11 Commission Report
    - Final Report of the National Commission on Terrorist
    Attacks upon the United States - Executive Summary*.
    Washington DC: U.S. Government Printing Office, 2004.

O'Brien, W. J. and J. Hammer. "Future Force and First
    Responders: Building Ties for Collaboration and
    Leveraged Research and Development." Conference Paper,
    Austin, TX, http://stinet.dtic.mil/cgi-
    bin/GetTRDoc?AD=ADA432794&Location=U2&doc=GetTRDoc.pdf
    (accessed November 3, 2006).

Office of the Assistant Secretary of Defense for Networks
    and Information Integration. *Net-Centric Checklist
    Version 2.1.3*. Washington DC: Department of Defense,
    2004 (accessed December 4, 2006).

Paton, D. and J. Violanti. *Psychology of Terrorism*, edited
    by Bruce Bongar, Lisa Brown, Larry Beutler, James
    Breckenridge and Philip Zimbardo. New York, New York:
    Oxford University Press, 2006.

Perry, Walter, David Signori, and John Boon. *Exploring
    Information Superiority: A Methodology for Measuring the
    Quality of Information and its Impact on Shared
    Awareness*. Santa Monica, CA: RAND National Defense
    Research Institute, 2004.

President's Homeland Security Advisory Council. *Statewide
    Template Initiative*. Washington DC: White House, 2003
    (accessed October 24, 2006).

Ronfeldt, D. and J. Arquilla. "Networks, Netwars, and the
    Fight for the Future." *First Monday* 6, no. 10 (2001):
    1-25.

Select Bipartisan Committee to Investigate the Preparation
    for and Response to Hurricane Katrina. *A Failure of
    Initiative: Final Report of the Select Bipartisan
    Committee to Investigate the Preparation for and
    Response to Hurricane Katrina*. Washington DC: U.S.
    Government Printing Office, February 15, 2006.

Springett, John P.,II. "Network Centric War without Art."
    United States Naval Institute. Proceedings 130, no. 2
    (February 2004): 58,
    http://proquest.umi.com/pqdweb?did=542511141&Fmt=7&clien
    tId=65345&RQT=309&VName=PQD.

The White House. "The Federal Response to Hurricane
    Katrina: Lessons Learned." (February 23, 2006, 2006): 1-
    217.

United States Conference of Mayors. *Five Years Post 9/11,
    One Year Post Katrina: The State of America's Readiness*.
    Washington DC: The U.S. Conference of Mayors, 2006
    (accessed November 27, 2006).

United States Fire Administration. *Four Years Later - A
    Second Needs Assessment of the U.S. Fire Service*.
    Washington DC: Department of Homeland Security, 2006
    (accessed November 23, 2006).

United States Government Accountability Office.
    *Catastrophic Disasters: Enhanced Leadership,
    Capabilities, and Accountability Controls Will Improve
    the Effectiveness of the Nation's Preparedness,
    Response, and Recovery System*. Washington DC: GAO, 2006
    (accessed November 14, 2006).

———. *Defense Acquisitions: Restructured JTRS Program
    Reduces Risk, but Significant Challenges Remain*.
    Washington DC: GAO, 2006 (accessed November 19, 2006).

———. *Hurricane Katrina: Better Plans and Exercises Needed
    to Guide the Military's Response to Catastrophic Natural
    Disasters*. Washington DC: GAO, 2006 (accessed June 3,
    2006).

———. *Opportunities Exist to Enhance Collaboration at 24/7
    Operations Centers Staffed by Multiple DHS Agencies*.
    Washington DC: United States Government Accountability
    Office, 2006, http://www.gao.gov/new.items/d0789.pdf.

Wilson, Clay. *Network Centric Warfare: Background and
    Oversight Issues for Congress*. Washington DC: Library of
    Congress. Congressional Research Service, June 2, 2004.

Zimmerman, Rae. "Public Infrastructure Service Flexibility for Response and Recovery in the Attacks at the World Trade Center, September 11, 2001." Institute for Civil Infrastructure Systems, Wagner Graduate School of Public Service, New York University. http://www.colorado.edu/hazards/sp/sp39/sept11book_ch9_ zimmerman.pdf (accessed February 12, 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. Department of Homeland Security
    Office for Interoperability and Compatibility
    Washington D.C.

4. Potomac Institute for Policy Studies
    Arlington, Virginia

5. Professor Douglas Porch
    Chairman, Department of National Security Affairs
    Naval Postgraduate School
    Monterey, California