NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A COMMUNICATIONS STRATEGY FOR DISASTER RELIEF

by

Eric Michael Folsom

March 2015

Thesis Advisor: Brian Steckler
Second Reader: Rebecca Goolsby

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2015	Master's Thesis

4. TITLE AND SUBTITLE
A COMMUNICATIONS STRATEGY FOR DISASTER RELIEF

5. FUNDING NUMBERS

6. AUTHOR(S) Eric Michael Folsom

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. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The problem with current international disaster relief is ineffective communication, coordination, cooperation, and collaboration (4C). Ineffective international 4C allows chaos and anarchy to significantly hinder disaster-relief efforts.

After action reports (AARs) and disaster relief (DR) materials were examined to identify system-level issues during DR missions. These issues were examined to determine if DR exhibits characteristics of a wicked problem.

The results of systems-thinking analysis show that anarchy, social complexity, and stress within the DR system have a negative impact on all components of the system. To improve the effectiveness of DR missions and help mission teams to present a unified front for DR, anarchy, social complexity, and stress must be reduced.

This work proposes a communication strategy for DR missions that harnesses capabilities of information communication and technology (ICT) solutions, introduces a cloud-based hierarchical trust model, and outlines a common integration interface. The strategy encourages open and transparent 4C between DR mission teams and the international DR community. Properly implemented, this communication strategy could reduce system-level anarchy and social complexity, resulting in reduced post-disaster damage, injuries, and loss of life.

14. SUBJECT TERMS
disaster relief, emergency response, information communications and technology, integration, interface, cloud, security, disaster response, communications strategy

15. NUMBER OF PAGES
155

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A COMMUNICATIONS STRATEGY FOR DISASTER RELIEF

Eric Michael Folsom
Captain, United States Army
B.S., Methodist University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2015

Author: Eric Michael Folsom

Approved by: Brian Steckler
Thesis Advisor

Dr. Rebecca Goolsby
Second Reader

Dr. Cynthia Irvine
Chair, Cyber Academic Group
Graduate School of Operational and Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The problem with current international disaster relief is ineffective communication, coordination, cooperation, and collaboration (4C). Ineffective international 4C allows chaos and anarchy to significantly hinder disaster-relief efforts.

After action reports (AARs) and disaster relief (DR) materials were examined to identify system-level issues during DR missions. These issues were examined to determine if DR exhibits characteristics of a wicked problem.

The results of systems-thinking analysis show that anarchy, social complexity, and stress within the DR system have a negative impact on all components of the system. To improve the effectiveness of DR missions and help mission teams to present a unified front for DR, anarchy, social complexity, and stress must be reduced.

This work proposes a communication strategy for DR missions that harnesses capabilities of information communication and technology (ICT) solutions, introduces a cloud-based hierarchical trust model, and outlines a common integration interface. The strategy encourages open and transparent 4C between DR mission teams and the international DR community. Properly implemented, this communication strategy could reduce system-level anarchy and social complexity, resulting in reduced post-disaster damage, injuries, and loss of life.

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

AAR	After Action Report
APAN	All Partners Access Network
ASEAN	Association of Southeast Asian Nations
BGAN	Broadband Global Area Network
BoT	Behavior over Time
CAP	Common Alerting Protocol
CDRP	Contingency Disaster Response Plan
COP	Common Operational Picture
C2	Command and Control
DDOS	Distributed Denial of Service
DOS	Denial of Service
DOD	Department of Defense
DR	Disaster Relief
DRP	Disaster Response Plan
EMOPS	Emergency Operations
ETC	Emergency Telecommunications Cluster
FACT	First Assessment and Coordination Teams
FAQ	Frequently Asked Questions
FEMA	Federal Emergency Management Agency
FITTEST Team	Fast IT and Telecommunications Emergency and Support
FLAK	Fly Away Kit
FMP	Frequency Management Plan
GSM	Global System for Mobile Communications
HA/DR	Humanitarian Assistance and Disaster Relief
HFN	Hastily Formed Networks
ICT	Information and Communications Technology
IFRC	International Federation of Red Cross/Red Crescent
IGO	International Government Organizations

IHC	International Humanitarian Community
InSTEDD	Innovative Support To Emergency Diseases and Disasters
ISP	Internet Service Provider
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NDMA	National Disaster Management Agency
NGOs	Nongovernmental Organizations
NPS	Naval Postgraduate School
OCHA	Office for Coordination of Humanitarian Affairs
PDC	Pacific Disaster Center
QDR	Quadrennial Defense Review
RTAT	Rapid Information and Communication Technology Assessment Team
SLA	Service Level Agreement
UN	United Nations
UNDAC	United Nations Disaster Assessment and Coordination
US	United States
VSAT	Very Small Aperture Terminal
VoIP	Voice Over Internet Protocol
WFP	World Food Program
Wi-Fi	Wireless Fidelity (802.11 standard)
WiMAX	Worldwide Interoperability for Microwave Access (802.16 standard)
WPF	Working Partners Foundation
4C	Communications, Coordination, Cooperation, Collaboration

ACKNOWLEDGMENTS

First, I would like to give thanks to God. Through His love and comfort, I was able to endure the late nights. I would also like to thank God for providing me with a loving and supportive family. Thank you, Yvonne, Wesley, Kady, and Michael, for your love, support, and inspiration throughout this last eighteen months. Without you guys, I would not be where I am today.

A special thank-you goes to Brian Steckler, Dr. Rebecca Goolsby, Dr. Nancy Roberts, and Brooks King for providing support, insight, education, and freely contributing their expertise to this endeavor. Their contributions to this project provided a unique perspective, created excitement, fostered creativity, and kept me on target.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THESIS OVERVIEW

A. INTRODUCTION

A disaster can occur anywhere with little to no warning. The devastating effects of disasters have global implications. For example, in December 2004, an earthquake in Indonesia formed a series of tsunamis that resulted in the death of approximately 230,000 people in Southeast Asia.[1] In August 2005, Hurricane Katrina wiped out most of New Orleans and the Mississippi delta.[2] In January 2010, an earthquake in Haiti destroyed the infrastructure, resulting in more than 220,000 deaths.[3] Finally, in November 2012, Typhoon Haiyan ravaged the islands of the Philippines, affecting over thirteen million people throughout the Pacific.[4]

Disasters provide the international community with opportunities to work together to help victims recover from disasters. As fellow inhabitants of this orb, we must do everything in our power to provide support and stability to the victims and governments that are affected. The stakeholders in disaster relief (DR) include all parties impacted by disasters. Stakeholders include the victims and their families, early responders, governments, militaries, commercial organizations, non-profit organizations, and essentially every country on the planet.

Over the last sixty years, stakeholders have attempted to improve support for disaster relief through organizational restructuring, establishing national

1. Raziye Akkoc, "2004 Boxing Day Tsunami Facts," *The Telegraph*, Accessed 3 March 2015, http://www.telegraph.co.uk/news/worldnews/asia/11303114/2004-Boxing-Day-tsunami-facts.html.

2. Bryan L. Bradford, Steve Urrea, and Brian Steckler, "After Action Report and Lessons Learned from The Naval Postgraduate School's Response to Hurricane Katrina" (master's thesis, Naval Postgraduate School, September 2005), 2–231.

3. Brian Steckler, "Hastily Formed Networks in Haiti, Haiti Earthquake After Action Report and Lessons Learned (AAR/LL)" (Naval Postgraduate School, 8 September 2010), 1–23.

4. Joshua Wadell and Brian Steckler, "Marine C2 in support of HA/DR: Observations and Critical Assessments Following Super-Typhoon Haiyan" (19th International Command and Control Research and Technology Symposium, 2013).

policies, and implementing innovative technologies. International organizations, such as the United Nations, changed their organizational structures to provide organization and stability to the victims of disasters.[5] National policies, such as the U.S. Quadrennial Defense Review, express the nation's intent to support DR efforts. International DR mission teams are harnessing cutting-edge technologies to provide on-site relief assistance to the people affected by disasters. Organizations provide innovative platforms to facilitate collaboration and situational awareness for DR missions.

B. PROBLEM STATEMENT

The United Nations states "governments and militaries are systems that have a major role in disaster relief and assistance."[6] Prior to the Internet boom, they were the best systems for organizing relief efforts and providing services and resources in a disaster[7]: "The old way of doing things made the hierarchy entirely responsible for the outcome, be that the government, the military or whatever entity was at the top of the hierarchy."[8] This includes failures due to factors outside of the organization's control.

This problem becomes more complex when multiple (country, state, and city) governments become involved, each with its own culture of responsibility and methods of dealing with failure. Governments and militaries of the same nation-state have different standards, processes, and procedures. When dealing with complex events jointly, these standards, processes, and procedures can create internal conflict. This situation is further complicated by the lack of

5. United Nations, *UN Humanitarian Civil-Military Coordination Officer Field Handbook* (Office for the Coordination of Humanitarian Affairs Civil-Military (Emergency Services Branch, Geneva, 2008).

6. Ibid.

7. Ibid.

8. Ibid.

international legislation and alignment between civil and military entities that deal with joint concerns inherent in disaster relief.[9]

This also leads to the development of "dysfunction in the system."[10] Hidden agendas, compartmentalization, proprietary information, information hoarding, and trust issues reduce the willingness for organizations to work together constructively. Past assumptions were that the government, military, and other hierarchical organizations best understood the situation because they possessed the best channels of communication and the resources needed to address the problems.[11]

Disaster relief (DR) is an international based system of systems because its individual components are part of another complex system. All subsystems within DR, governments, militaries, nongovernmental organizations, commercial organizations, and victims of the disaster constitute the system-level stakeholders. The internal issues inherent in the subsystems compound issues within the DR system. Some of the main issues within the DR system are the lack of command and control, common collaboration and situational awareness, and communication enabling capability.

To correct these issues the stakeholders worked independently to provide solutions to the system-wide issues of DR. The United Nations established the cluster system,[12] the U.S. Government established the All Partners Access Network (APAN),[13] and the commercial sector developed information and communications technology deployment kits. All of these solutions provided key functions to resolve issues identified within the DR system. The restructuring and technological advancements represented an unparalleled capability for the relief

9. Ibid.

10. Ibid.

11. Ibid.

12. United Nations, "About," Office for Coordination of Humanitarian Affairs, Accessed 23 September 2014, http://www.humanitarianresponse.info/about.

13. All Partners Access Network. "About page," accessed 26 October 2014. https://community.apan.org/p/about.aspx.

effort. These solutions improved communications, coordination, cooperation, and collaboration between the responders and resulted in lives saved. However, due to legislative issues, information hoarding, and complex social implications of interdependent systems, the solutions only treat the symptoms of the system-level problem in DR. These solutions do not resolve problems at the system level for DR.

Today, a new, less hierarchical system of organizations and information streams addresses the wicked problem of disaster. Problems that are considered wicked are very complex and possess significant social implications due to the variety of stakeholders. These less hierarchical systems are ad hoc, disjointed, and have their own problems. The new dysfunctions are in some ways, the same as the old dysfunctions: information hoarding to maintain control, avoid blame, get credit and recognition, and improve one's performance over one's competitors. However, the new flatter, more diverse system also results in information fragmentation as more and more people hold critical pieces of information. Critical information is then only partially shared with friends or aligned agencies. One of the incentives for this information hoarding is to not reveal one's own miss-steps and miscalculations.

The lack of open sharing fragments and complicates DR teams' interactions on the ground. Fragmentation of critical information distribution reduces response quality and unintentionally injects anarchy into the system. Attempts to repair this fragmentation, selectively creates multiple information sharing solutions that confuse teams attempting to cooperate.[14] Multiple information sharing sources create a feeling of information overload, which could reduce the desire for the teams to work together in a synchronized manner.

The issues mentioned reflect the nature and relationships of interdependent components in today's DR system of systems. The

14. Larry Wentz, "Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010," Center for Technology and National Security (National Defense University, Washington, DC, 08 August 2010).

interdependencies work in concert to increase system-level anarchy.[15] Anarchy in the DR system is the ultimate state of disorder, uncertainty, instability, insecurity, and identification of leadership. A fragmented and disjointed response along with increased anarchy, results in avoidable post-disaster injuries and deaths, especially within the first 72 hours. Figure 1 illustrates some system-level variables that have a significant impact on the current DR system.

Looking at the social challenges within international disaster relief (DR) missions, some organizations' agendas and aspirations take precedence over providing relief to the victims.[16] Eyewitness testimony identifies this behavior occurring during Hurricane Katrina in 2005 and again in the 2012 Philippine mission.[17] The victims and their governments do not want mission teams to take over and impose foreign value systems, but they do desire assistance with locating lost family members and recovering from the disaster.[18] The victims are simply trying to survive in the aftermath of the disaster and do not care about organizational agendas and objectives.[19] Disaster relief is about working together as a community to provide life-saving efforts, support, and aid to the victims of a disaster.[20]

In order for the international community to successfully provide this service, responders should present a synchronized, unified front. The international community should develop ways to encourage open and transparent information sharing. The international community should work together to develop a functional communications strategy for DR. For a

15. Nancy Roberts, "Coping with Wicked Problems" Classroom Instruction (Monterey, CA, 22 September–18 December 2014).

16. Brian Steckler, "Hastily Formed Networks for HA/DR," Classroom Instruction (Naval Postgraduate School, Monterey, CA, 22 June–16 September 2014).

17. Ibid.

18. Ibid.

19. Victoria Richards, "Cyclone Pam: Vanuatu will run out of food "in a week" as officials slam aid agencies for wanting 'publicity,'" 19 March 2015, http://www.independent.co.uk/news/world/australasia/cyclone-pam-vanuatu-will-run-out-of-food-in-a-week-as-officials-slam-aid-agencies-for-wanting-publicity-10119369.html.

20. Ibid.

communications strategy to change DR at the system level, the international community must embrace a communications strategy that increases communication,[21] coordination,[22] cooperation,[23] and collaboration[24] (4C) between disaster relief mission teams. This is the 4C approach or framework.

The 4C approach involves setting up the conditions that: (1) encourage **free flow of communication** among diverse holders of information; (2) provide the capability to identify and share the critical information needed for individual, independent or semi-independent actors to know more about the "big picture" of events, problems, needs, and activities so they can **coordinate their actions and activities with other actors;** (3) assist actors in the system to identify gaps and issues that require **cooperation among actors**; and (4) encourage **collaboration** by promoting limited, contextualized trust among actors who might, in other situations, see one another as rivals, competitors or even adversaries.

Based on systems-level research, the author developed the 4C framework to address key variables within the DR system. Reduced 4C during disaster relief missions diminishes the quality of the relief, increases the duration of the mission, and presents an unsynchronized, non-unified front. The lack of a non-unified front for disaster relief missions increases a kind of anarchy that can result in preventable post-disaster damage, injuries, and loss of life.

This thesis analyzes the DR system and its social complexities. It frames the system-level problem, and identifies the system-level solution entry point.

---

21. MR3 Inc. and Black Swan Solutions, "Communicating in a Crisis," MR3 and Black Swan Solutions Joint Webinar, 20 January 2015. http://www.mir3.com/mir3-inc-and-black-swan-solutions-present-joint-webinar-on-communicating-in-a-crisis/.

22. Nancy Roberts, "Coping with Wicked Problems" Classroom Instruction (Monterey, CA, 22 September–18 December 2014).

23. Ibid.

24. Defense Advanced Research Projects Agency, "Request for Information (RFI): Strategic Collaboration," DARPA White Paper Request (FedBizOpps.gov. 2 April 2007), https://www.fbo.gov/index?s=opportunity&mode=form&id=c705f867a67b945de03592276252b605&tab=core&_cview=0.

Based on the findings, this thesis proposes a communications strategy concepts designed to reduce the overall anarchy within the system. A reduction in anarchy within the DR system could potentially reduce post-disaster damage, injuries, and loss of life.

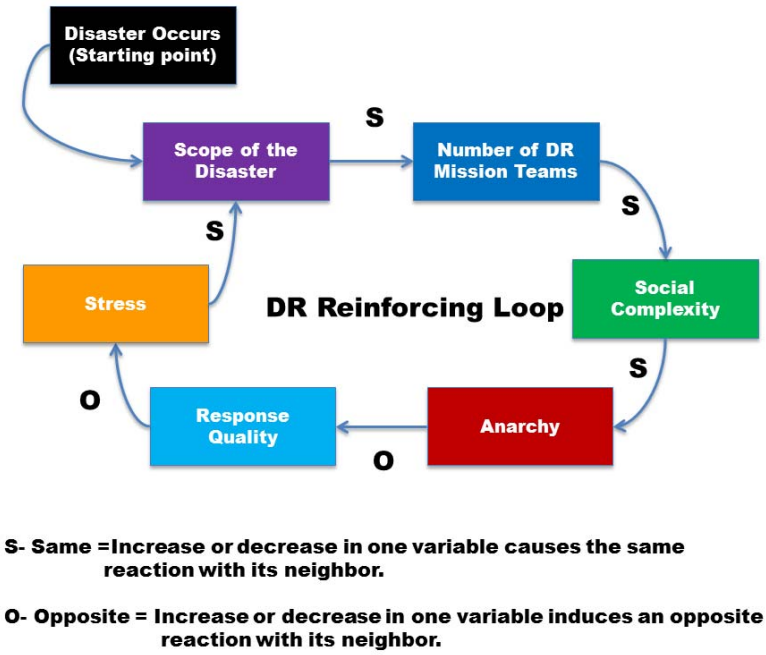


Figure 1. Disaster Relief Vicious Cycle.[25]

C. STRUCTURE AND SCOPE

In Chapter II, this thesis discusses solutions implemented to address specific problems of communication within DR. It continues with an introduction to current information and communications technology (ICT) example and explores significant issues identified from DR missions. Chapter II further provides a brief summary of past and present implementations, elucidating and justifying how previous solutions have failed to reduce information anarchy within

25. Anderson, Virginia and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loop* (Waltham, MA: Pegasus Communications, 1997).

the DR system.[26] Information anarchy is the problem of disjointed, ad hoc information sharing and the poor situation awareness that results from a system that fails to promote or encourage the free flow of communications, impeding coordination, discouraging cooperative behavior, and providing very limited incentives for collaboration (i.e., “reduced 4C”).

Chapter III introduces the concept of wicked problems. It then compares the issues in DR with known characteristics of wicked problems to formally identify it as a wicked problem with system-level issues. The chapter then explores the DR system using the Systems Thinking process. The Systems Thinking process allows a better understanding of the physical characteristics and social implications of the problem space. The chapter continues with an introduction to injection points and balancing mechanisms.[27] Injection points and balancing mechanisms depict a section within the system where a solution may reduce the anarchy within the DR system.[28]

Chapter IV begins with an introduction to a communication strategy for DR missions. The communications strategy combines an ICT capability with a cloud based, decentralized, integrated 4C interface concept. This chapter continues with a design structure proposal for the integration interface concept. The discussion concludes with a brief overview of security implications for the proposed concept model and a short summary of the combined communication strategy.

Chapter V introduces some general security considerations. The chapter addresses security of data-at-rest and data-in-transit. The chapter approaches security considerations of critical components of the security strategy.

---

26. Rebecca Goolsby, telephone call with author, 5 March 2015.

27. Anderson, Virginia and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loop* (Waltham, MA: Pegasus Communications, 1997), 2–21.

28. Ibid.

The thesis conclusion provides a summary of the concepts discussed in the thesis. Conceptually, creating an internationally accepted communication strategy reduces DR system-level anarchy.

D. BENEFITS OF THE THESIS

The 2014 U.S. Quadrennial Defense Review (QDR) states the following: "Protect the homeland, to deter and defeat attacks on the United States and to support civil authorities in mitigating the effects of potential attacks and natural disasters."[29] Another key goal in the QDR is to "Project power and win decisively, to defeat aggression, disrupt and destroy terrorist networks, and provide humanitarian assistance and disaster relief."[30]

To maintain compliance with this mandate, the Department of Defense (DOD) and the U.S. government must work with the international community to support disaster relief (DR) missions. This thesis investigates potential solutions that support compliance with the 2014 QDR.[31]

From an international DR stakeholder perspective, this document represents a preliminary model of framing the problem space within the DR system. By analyzing the broader system-level problems within the DR system, mission stakeholders can refine this concept to design solutions that reduce anarchy within the system. Furthermore, the implementation of a communications strategy has the potential to encourage open and transparent communication, coordination, cooperation, and collaboration (4C) within the international community.

29. U.S. Department of Defense, *Quadrennial Defense Review* 2014 (Washington, DC: Office of the Secretary of Defense, March 2014), V

30. Ibid.

31. U.S. Department of Defense, *Quadrennial Defense Review* 2014 (Washington, DC: Office of the Secretary of Defense, March 2014), 22, 25, 33.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. PREVIOUS AND CURRENT SOLUTIONS

Over the last 60 years, many different concepts have been independently introduced to correct known DR shortfalls. The implemented solutions added organization and enabled communications, but lacked the impact and support to encourage international open 4C participation for DR missions. These solutions succeeded in treating the symptoms of the problem but failed to address the system-level problem. Solutions that treat symptoms of system-level problems will likely result in adding new unanticipated problems.

The sections that follow briefly introduce previous and current solutions for DR:

- Organization solutions
- Collaborative solutions
- Communication enabling solutions

1. Organization Solutions

In 1942, the United Nations (UN) was established to promote international cooperation and to combat Axis powers.[32] In 1945, the United Nations Charter was ratified bringing 50 nation states into an allegiance to promote peace.[33] Over several decades, the United Nations added members and changed through collaborative planning.[34]

In 1991, the UN convened and passed the General Assembly Resolution 46/182, which set the foundation for UN DR missions.[35] In 2005, the

32. United Nations, “History of the United Nations,” UN Online, assessed 01 October 2014, http://www.un.org/en/aboutun/history/

33. Ibid.

34. Ibid.

35. United Nations, “About,” Office for Coordination of Humanitarian Affairs, accessed 23 September 2014, http://www.humanitarianresponse.info/about.

Humanitarian Reform Agenda introduced several changes within the UN to address identified issues with predictability, accountability, and partnership.[36] The Reform Agenda passed legislation to reorganize the UN into clusters.[37] A cluster is a group of organizations or stakeholders, with a designated leader, working in a specified area designed to fill existing capability gaps.[38] Figure 2 represents the UN organizational cluster system. Despite the organizational cluster system of the United Nations, information anarchy remains a constant problem throughout the DR system.[39]

36. United Nations, "What is the Cluster Approach?" Office for the Coordination of Humanitarian Affairs, assessed 26 October 2014, http://www.humanitarianresponse.info/clusters/space/page/what-cluster-approach.

37. Ibid.

38. United Nations, *UN Humanitarian Civil-Military Coordination Officer Field Handbook*, Office for the Coordination of Humanitarian Affairs, Emergency Services Branch, Geneva, 2008, p.124.

39. Brian Steckler, "Hastily Formed Networks for HA/DR." Classroom Instruction (Naval Postgraduate School, Monterey, CA. 22 June–16 September 2014).

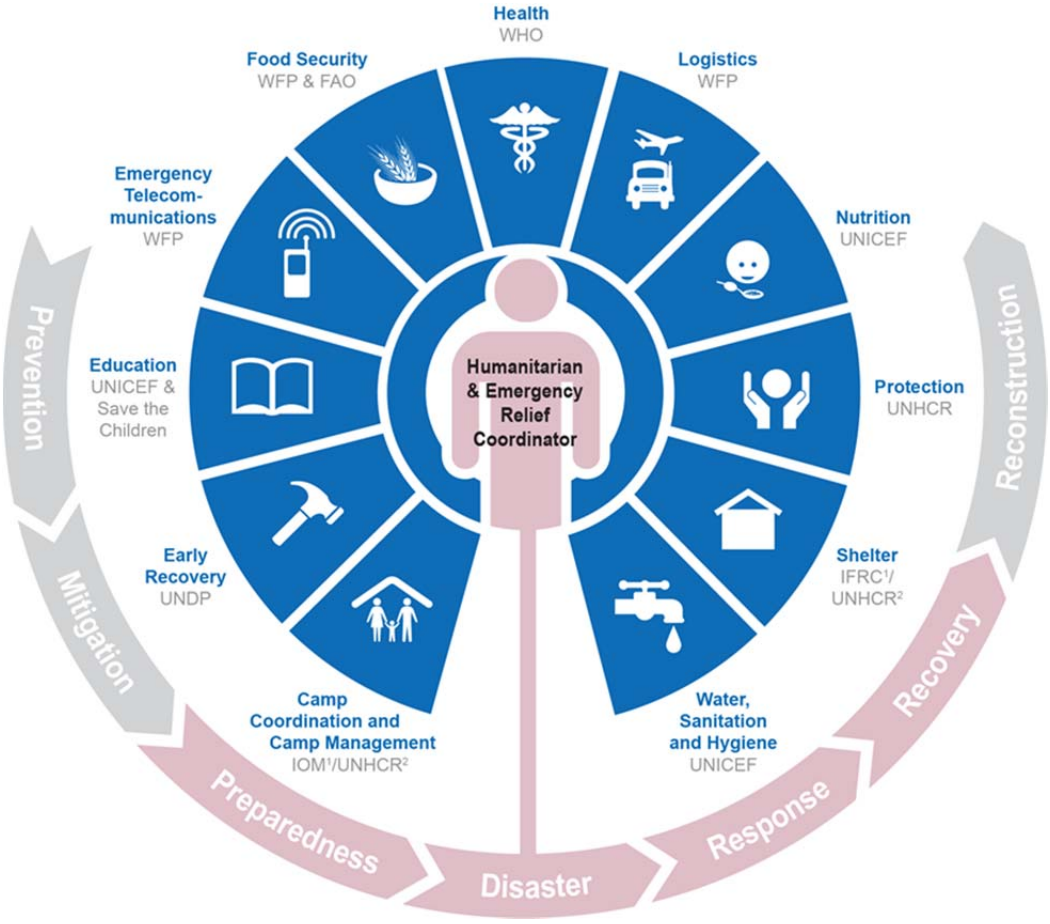


Figure 2. United Nations Cluster System.[40]

One of the main issues with an organization restructuring solution is that it is internal to the organization and is not applied or accepted globally. There is no official legislation appointing an organization as a recognized international body for DR. The design of the UN Cluster System is not the reason that the organizational restructuring solution continues to fail. The lack of international trust and social complexity of an international DR mission simply does not support a centralized command structure. This could be an advantage, as a flatter organization structure can be more agile in disasters. Actors with limited trust among themselves have more freedom to act individually or in concert with

40. United Nations, "What is the Cluster Approach?" Office for the Coordination of Humanitarian Affairs, assessed 26 October 2014, http://www.humanitarianresponse.info/clusters/space/page/what-cluster-approach.

only highly trusted partners; further, they are weighed down with fewer obstacles to acting. However, the cluster system provides problems for information flow that lead to situations of reduced 4C (lack of communication, coordination, cooperation, and collaboration) so that even information flow among trusted partners is fragmented, disjointed, and partial. This has long been a recognized problem, with a number of attempts to solve it in the last two decades.

2. Collaborative Solutions

Over the last decade, many different vendors developed solutions to provide a medium for international DR collaboration. These collaborative solutions provided vital capabilities to the international community and DR stakeholders. Many of the collaborative solutions are still in use today. One of the solutions currently in use is the All Partner Access Network (APAN) website.

APAN was originally developed and implemented in 1997 for the United States Pacific Command (PACOM).[41] The portal provides a community space for collaboration between international mission teams.[42] There are several reasons APAN is not widely embraced internationally. Wentz's observation report describes these barriers. First, the U.S. Armed Forces developed and currently manages APAN. Second, creating an APAN user account requires the user to provide a good deal of personal information. The international community as a whole does not maintain a mutual transparent trust relationship with the U.S. Armed Forces. The lack of transparency and compartmentalization practices, used within the U.S. Armed Forces, discourages open sharing across the international DR community. Furthermore, in some countries, cooperation with the U.S. military may put the lives of participants and their families in danger. The distrust between DR entities ultimately inspired the international community to develop and rely on its own collaborative solutions.

41. All Partners Access Network, "About page," accessed 26 October 2014, https://community.apan.org/p/about.aspx.

42. Ibid.

Other problems with APAN acceptance include the problem of getting all players to accept the centralized access model for distributing information and inefficiencies within the platform itself.[43] AARs from the international community also identify issues with the centralized access control model and platform inefficiencies. To access resources on APAN, individuals must request permission to a specific resource or group, justify their request to a higher authority, and wait for access. A centralized model that introduces layers of bureaucracy into a collaboration system will likely foster distrust and discourage open sharing.

Most of the collaborative solutions developed over the years support a hierarchical and centralized model. Instead of allowing the governing body affected by the disaster to lead collaboration efforts, previous models rely on the solution provider as collaboration lead for DR events. The social complexities of DR, combined with the centralized models of collaboration, do not support an open and transparent relationship. International distrust between teams and distributed information increases confusion and anarchy in the DR system.[44]

As was the case in 2011 and still today, no singularly recognized international platform successfully encourages open and transparent collaboration.[45] For a collaborative solution to be internationally accepted, the model used must inspire open and transparent sharing of information.

3. Information and Communications Technology Solutions

In today's world of crisis response, reliable global communications is the essential foundation for success for DR efforts. Search and rescue operations, the establishment of aid stations, and the coordination of lift and drop of essential

43. Larry Wentz, "Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010," Center for Technology and National Security (National Defense University, Washington, DC, 08 August 2010).

44. Ibid.

45. Naim Kapucu Ph.D., "Collaborative governance in international disasters: Nargis Cyclone in Myanmar and Sichuan Earthquake in China cases," *International Journal of Emergency Management*, 8(1). 2011, 1–25.

supplies and resource—every essential element of the response needs communication (and power). Communications, coordination, cooperation, and collaboration (4C) for disaster relief missions require a network connection. Implementing a mobile contingency communications package or information communications and technology (ICT) constitutes another solution developed to enable 4C for mission teams. ICT is a communications enabler and provides a required connection capability for the responder teams. The ability of teams to communicate when normal communication infrastructure goes down is an invaluable asset to international DR. With the demand for DR ICT solutions high, many ICT providers saw a need to fill the gap. As a result, there are hundreds of communications enabling solutions available.

With all of these solutions available, users are bound to encounter some interoperability issues. Interoperability issues can ultimately affect the ability of a DR team to successfully communicate. If the mission teams are incapable of effectively coordinating with participating teams, they may inadvertently become centrally located. Satellite bandwidth saturation can quickly become an issue when a significant number of satellite based ICTs, operating on the same frequency band, deploy to a small geographical area.[46]

ICT packages are comprised of computer and network equipment. ICT packages equip small to large teams with network connection capability in areas that have limited power and communications resources. ICT packages are critical components for participating in communication, coordination, cooperation, and collaboration (4C) during disaster relief missions. 4C activities provide a means to increase relief effort response quality, ultimately resulting in saving lives. When used effectively, an ICT capability enables communication and facilitates coordination between mission teams on the ground. One such example of an effective ICT is Hastily Formed Networks.

46. Brian Steckler, “Hastily Formed Networks in Haiti. Haiti Earthquake After Action Report and Lessons Learned (AAR/LL)” (Naval Postgraduate School, Monterey, CA. 8 September 2010).

In 2004, Dr. Peter Denning coined the term “Hastily Formed Networks” (HFN) and enlisted Brian Steckler to establish a lab at the Naval Postgraduate School (NPS).[47] The HFN concept enables a small team of communications experts with an ICT capability to provide an operations command and control center in support of global DR efforts.[48] The NPS HFN team is a two to seven person team, capable of rapidly deploying a mobile command and control communications capability in support of minimal notice Humanitarian Assistance and Disaster Relief (HA/DR) missions. To date, the NPS HFN team has supported four major international DR deployments and participated in numerous international military and state sponsored training exercises. Through deployments and training exercises, the NPS HFN team constantly transforms its deployment packages to resolve issues discovered.

B. HASTILY FORMED NETWORKS DEPLOYMENT REVIEW

1. Southeast Asia Tsunami Deployment

The first official test of the HFN concept occurred during the deployment to Southeast Asia.[49] On December 26, 2004, as a result of a massive 9.0-9.3 earthquake in Indonesia, tsunamis were generated, affecting eleven countries.[50] As a relatively newly formed DR mission concept, the NPS HFN team was tasked to establish two broadband networks. In its early phases, HFN did not possess the scalability or capacity required to support the event without commercial partner assistance.[51] In order to address the shortcomings, ad-hoc partnerships were formed to provide support, technical expertise, and additional

47. Peter J. Denning Ph.D., “Hastily Formed Networks,” Communications of the ACM 49, No. 4. April 2006, accessed 15 May 2014. http://faculty.nps.edu/dl/HFN/documents/HastilyFormedNetworks_Denning.pdf.

48. Ibid.

49. Brian Steckler, “Hastily Formed Networks: A report on Naval Postgraduate School Response to the 2004 Southeast Asia Tsunami” (Naval Postgraduate School, Monterey, CA. 25 July 2005).

50. Ibid.

51. Ibid.

equipment. Partnerships were formed with Redline Communications (802.16 WiMAX), Rajant Corporation (802.11 Wi-Fi), and Cisco Corporation (Network Router, VoIP).[52]

On January 4, 2004, Brian Steckler, the HFN communications expert, and his team arrived in Bangkok, Thailand.[53] The first steps of the mission required coordinating local government and the Royal Thai Armed Forces support. On January 8, 2005, the team began to establish its first hasty network connection at the Yang Yao Grave Registration Center and Morgue.[54] The team's secondary site was located at the nearby Bang Muang indigenously displaced persons (IDP) camp. Each site established a meshed 802.11 Wi-Fi cloud and was bridged using Redline 802.16 WiMAX technology.[55] By harnessing the power of WiMAX and meshed Wi-Fi, each site's responders were able to connect to the Internet and collaborate with other DR teams. The HFN implementation allowed for 4,000 survivors and 1,000 relief support personnel to communicate with colleagues, friends, and family members using the Internet connection at each site.[56]

52. Brian Steckler, "Hastily Formed Networks: A report on Naval Postgraduate School Response to the 2004 Southeast Asia Tsunami" (Naval Postgraduate School, Monterey, CA. 25 July 2005).

53. Ibid.

54. Ibid.

55. Ibid.

56. Ibid.

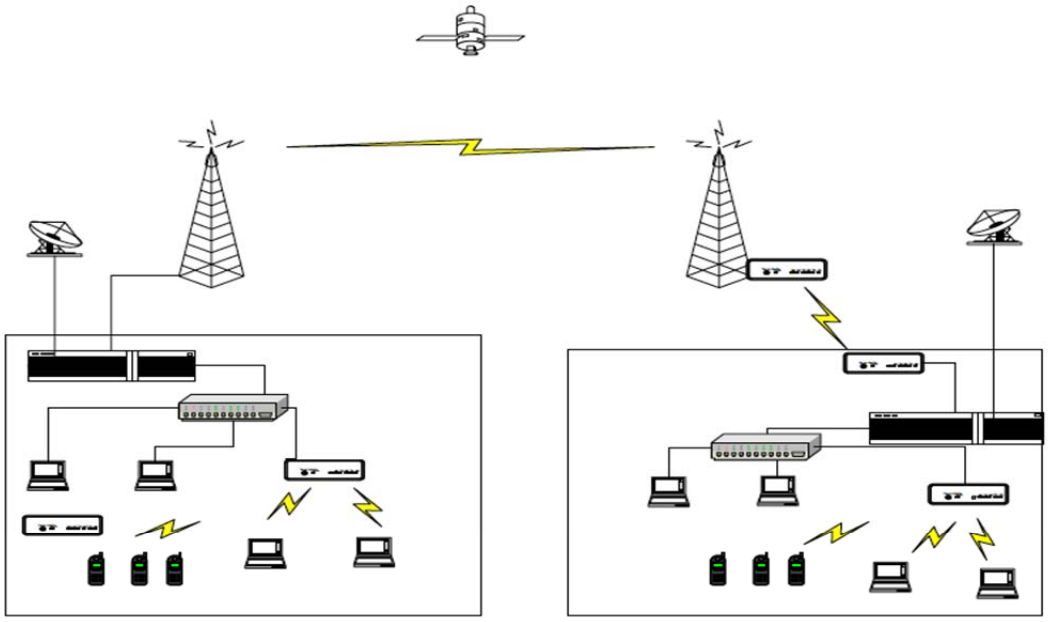


Figure 3 - Thailand Tsunami Wireless Network Topology (Wat Yang Yao and Bang Muang Camp)

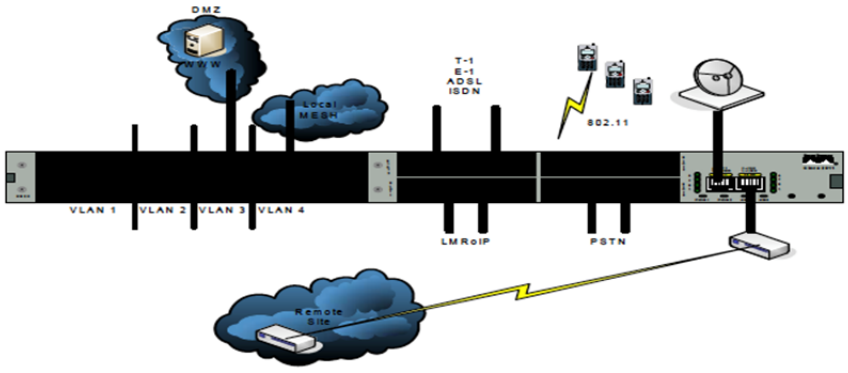


Figure 3. NPS HFN Team's Southeast Asia Network Diagram.[57]

Many issues surfaced during the first real world implementation of the NPS HFN team. Some of the significant issues identified from the deployment were as follows:

- Functionality and durability issues
- Cost of maintaining network equipment
- HFN Fly Away Kit (FLAK) standard was not established or defined

57. Brian Steckler, "Hastily Formed Networks: A report on Naval Postgraduate School Response to the 2004 Southeast Asia Tsunami" (Naval Postgraduate School, Monterey, CA. 25 July 2005).

The functionality and durability of ICT equipment was a pervasive issue.[58] The Breadcrumb devices continuously failed during the deployment and required the procurement of replacement network components.[59] Rajant Breadcrumb devices transform disparate wireless access points into a fully meshed Wi-Fi network.[60] A meshed network allows mobile users to seamlessly shift to the nearest access point.[61]

The cost of maintaining the equipment and providing service for the network was significant. BGAN is expensive and will not support many users concurrently.[62] Very small aperture terminal (Vsat) will support more users sufficiently; however, setup and operation requires specific technical expertise and can be significantly more expensive depending on the service plan.[63]

There is no existing definition of what needs to be in the FLAK.[64] Equipment requirements for each deployment differ. Steadily changing requirements complicate defining capabilities needed to support all deployment scenarios.

58. Brian Steckler, "Hastily Formed Networks: A report on Naval Postgraduate School Response to the 2004 Southeast Asia Tsunami" (Naval Postgraduate School, Monterey, CA. 25 July 2005).

59. Brian Steckler, "Hastily Formed Networks for HA/DR." Classroom Instruction (Naval Postgraduate School, Monterey, CA. 22 June–16 September 2014).

60. Brian Steckler, "Hastily Formed Networks: A report on Naval Postgraduate School Response to the 2004 Southeast Asia Tsunami" (Naval Postgraduate School, Monterey, CA. 25 July 2005).

61. Brian Steckler, "Hastily Formed Networks for HA/DR" (Classroom instruction, Naval Postgraduate School, Monterey, CA. 22 June–16 September 2014).

62. Ibid.

63. Ibid.

64. Ibid.

2. Hurricane Katrina Deployment

On September 6, 2005, the NPS HFN team deployed to Hancock Medical Center in Bay Saint Louis, Mississippi, in support of U.S. DOD DR efforts for Hurricane Katrina.[65]

Because Katrina occurred in the United States, many technology companies saw the disaster as an opportunity to sell their products and services. As such, there was a constant flood of companies offering their services directly to the NPS team leadership. These companies actually caused problems with the participation of the NPS HFN team in the mission. When Brian Steckler arrived with his HFN team, the incident commander of Hancock County Emergency Operations Center turned the U.S. Navy sponsored HFN team away, assuming they were another vendor trying to sell their products and services. Since HFN was a new concept, different levels of incident command denied the NPS HFN team's offer to provide support. Due to the additional confusion from information technology companies, the incident commander did not understand the role of the NPS HFN team and their capabilities for the DR mission set.[66] However, due to Mr. Steckler's diligence and patience, the NPS HFN team finally participated.

HFN's layout for this deployment consisted of a wide area network connection and a local area connection. Satellite communications using a VSAT terminal established the connection to the Internet. The use of Wi-Fi (802.11) access points, WiMAX (802.16) bridge, and mobile command vehicles enabled 4C for the mission.[67] By increasing the capabilities of HFN in this deployment, the HFN team was able to concurrently push out services to multiple areas. Improving HFN's FLAK prior to deployment enabled critical 4C participation for

65. Bryan L. Bradford, Steve Urrea, and Brian Steckler, "After Action Report and Lessons Learned from The Naval Postgraduate School's Response to Hurricane Katrina" (master's thesis, Naval Postgraduate School, September 2005).

66. Ibid.

67. Ibid.

key first responders and provided a way for the victims to reestablish contact with family members.

The impact of Katrina on coastal Mississippi has been described as "staggering" with many communities and towns destroyed in a single night.[68] This massive storm spawned 11 tornados in Mississippi with hurricane winds smashing the coast for seventeen hours.[69] Over one million people were affected in rural areas and had limited means for assistance.[70] This area had far less visibility than New Orleans, but the victims were in equally dire situations with fewer law enforcement, medical and relief resources, and transportation routes to support these populations.

The HFN deployment connected high critical nodes that had a direct impact on human security in the areas affected most by this disaster (see Figure 4). This deployment connected the police and law enforcement in the hardest hit areas in Bay St. Louis and Waveland, Mississippi, as well as the relief distribution center and the Hancock Medical Center. In these ways, the deployments in Thailand and Mississippi were highly similar—they occurred in rural areas, with serious impact, limited infrastructure, and a high population of victims in desperate situations.

68. *Washington* Post, "Katrina's Staggering Blow," Washington Post Editorials, 31 August 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/30/AR2005083001554.html.

69. Jacob Wycoff, "Flashback to Hurricane Katrina…8 Years Ago Today," WeatherBug, 29 August 2013, http://knowbefore.weatherbug.com/2013/08/29/flashback-to-hurricane-katrina-8-years-ago-today/.

70. Ibid.

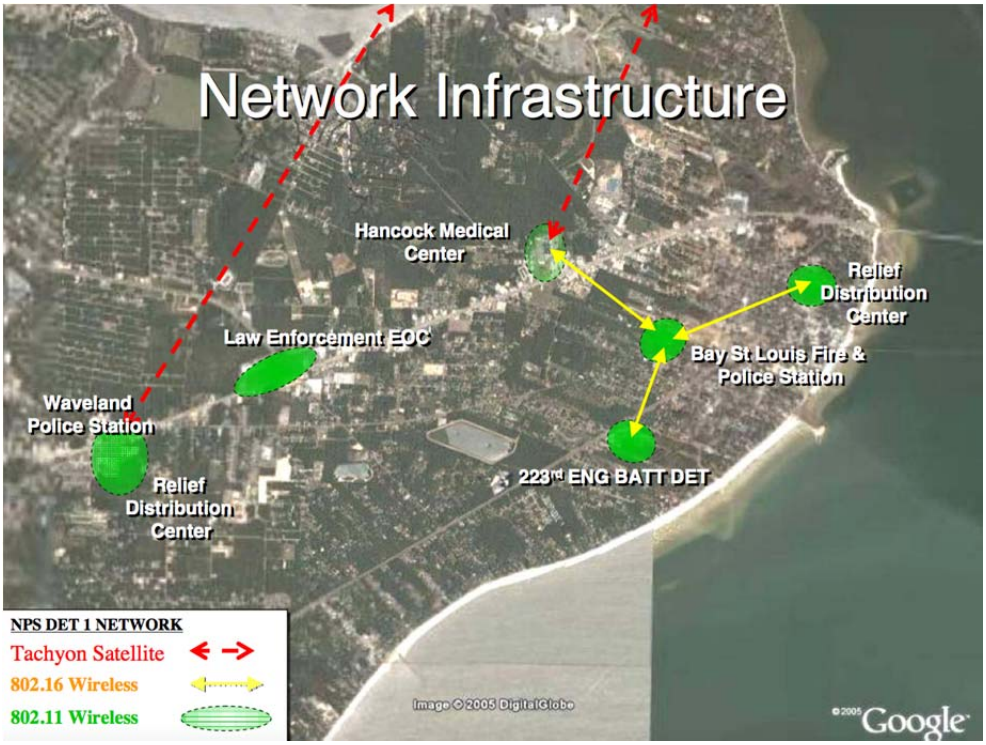


Figure 4. NPS HFN Team's Katrina Network Infrastructure.[71]

Due to the limited timeline between Thailand and Katrina missions (7 months), only some of the issues previously discovered were addressed. During the Katrina deployment, the team experienced some of the same challenges they did in Thailand. The primary issue that resurfaced during this deployment was equipment interoperability and durability issues. In addition, the changes and upgrades to the FLAKs brought issues to the surface.

The significant issues identified during the Katrina were as follows:

- Equipment durability, accountability, and interoperability issues
- Access to satellite communications was limited
- Network security policies were not in place
- Power generation issues

71. Brian Steckler, "Hastily Formed Network Information Brief," FCC Data Workshop, 4 October 2011, http://transition.fcc.gov/pshs/docs/summits/DACA/Steckler%20-%20FCC%20DACA%20Workshop.pdf.

Donated equipment experienced functionality and durability issues.[72] Some of the equipment did not perform for the duration of the mission. After the replacements arrived, there was no designated method for maintaining accountability of the network equipment.[73] Finally, some of the equipment donated suffered from significant interoperability issues when used in concert with products from other vendors.[74]

Throughout the Katrina deployment, access to government and commercial satellites was limited. Because of the limited access to the satellite connection points and shared frequency bands, saturation of bandwidth was a constant problem.[75] The absence of quality control mechanisms resulted in communications degradation during peak times.[76]

Another significant issue with the NPS HFN team was the lack of a multi-layered network security plan. Improper security procedures and lack of policies negated the ability of the NPS HFN team to manage the users that were connected. The lack of intrusion detection and prevention solutions denied the ability to monitor traffic on HFN.[77]

During the deployment, the NPS HFN team was vulnerable to cyber-attack because the team did not implement and enforce a multi-layered security solution. The NPS HFN team experienced an unexplained degradation of service. Due to the partner relations, Mr. Steckler was able to identify that the service degradation was coming from an IP range outside of the internal network. A few days prior to being relieved, an access list solution provided the means to

72. Bryan L. Bradford, Steve Urrea, and Brian Steckler, “After Action Report and Lessons Learned from The Naval Postgraduate School’s Response to Hurricane Katrina” (master’s thesis, Naval Postgraduate School, September 2005).

73. Ibid.

74. Ibid.

75. Ibid.

76. Ibid.

77. Ibid.

thwart further DOS attacks.[78] Due to the lack of a multi-layered security solution, the NPS HFN experienced a suspected denial of service (DOS) attack.[79]

During natural disasters, the power grid usually fails in affected areas.[80] It is problematic to transport power generation equipment and the supporting materials required to operate them to the disaster area.[81] There is an immediate need for self-sustaining power generation capabilities.[82]

3. Haiti Earthquake Deployment

On January 12, 2010, a 7.3 magnitude earthquake caused catastrophic damage to the country of Haiti, on the island of Hispaniola (Shared with the Dominican Republic).[83] The devastation that occurred resulted in over 220,000 deaths.[84] The damage was so extensive that it incapacitated a significant amount of the island's disaster response capability and critical infrastructure. Larry Wentz, an observer for the National Defense University, published a trip report detailing his observation of the ICT situation during the mission. In his report, Wentz indicated that over 40 percent of the government buildings experienced catastrophic damage.[85] He also mentioned that the earthquake destroyed the UN headquarters and the UN command and communication facilities, killing approximately 150 peacekeeping mission members of the United Nations.[86]

---

78. Bryan L. Bradford, Steve Urrea, and Brian Steckler, "After Action Report and Lessons Learned from The Naval Postgraduate School's Response to Hurricane Katrina" (master's thesis, Naval Postgraduate School, September 2005).

79. Ibid.

80. Brian Steckler, "HFN-USNS Mercy Mission Report AAR" (Naval Postgraduate School. Monterey, CA., 11 July 2006).

81. Ibid.

82. Ibid.

83. OXFAM, "Haiti Earthquake – our response," *OXFAM International*, accessed 30 October 2014, http://www.oxfam.org/en/haiti-earthquake-our-response.

84. Ibid.

85. Larry Wentz, "Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010," Center for Technology and National Security (National Defense University, Washington, DC, 08 August 2010).

86. Ibid.

Despite the significant damages, some of the cellular and network infrastructure remained intact.[87]

On January 18, 2010, the NPS HFN team deployed in support of DR operations in Haiti.[88] The team provided advice and employed their ICT platform in support of the relief effort.[89] The initial assignment of the team provided additional ICT capability for the United States Naval Ship (USNS) Comfort mission.[9091] The team was able to provide network connectivity to the locations in Figure 6 using its Redline WiMAX links and Wi-Fi Mesh capability. A few weeks later, the NPS HFN team provided support for Joint Task Force (JTF) Haiti. The new mission of the team provided communications for a variety of early responders including NGOs, UN personnel, U.S. government, and military entities.[92] The NPS HFN team's mission ended approximately thirty days after their initial deployment.

87. Larry Wentz, "Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010," Center for Technology and National Security (National Defense University, Washington, DC, 08 August 2010).

88. Brian Steckler, Hastily Formed Networks in Haiti, "Haiti Earthquake After Action Report and Lessons Learned (AAR/LL)" (Naval Postgraduate School, Monterey, CA., 8 September 2010).

89. Ibid.

90. Ibid.

91. Jennifer Ashton, "Aboard the USNS Comfort in Haiti," *CBS News*, 20 January 2010, accessed 13 September 2014, http://www.cbsnews.com/news/aboard-the-usns-comfort-in-haiti/.

92. Ibid.

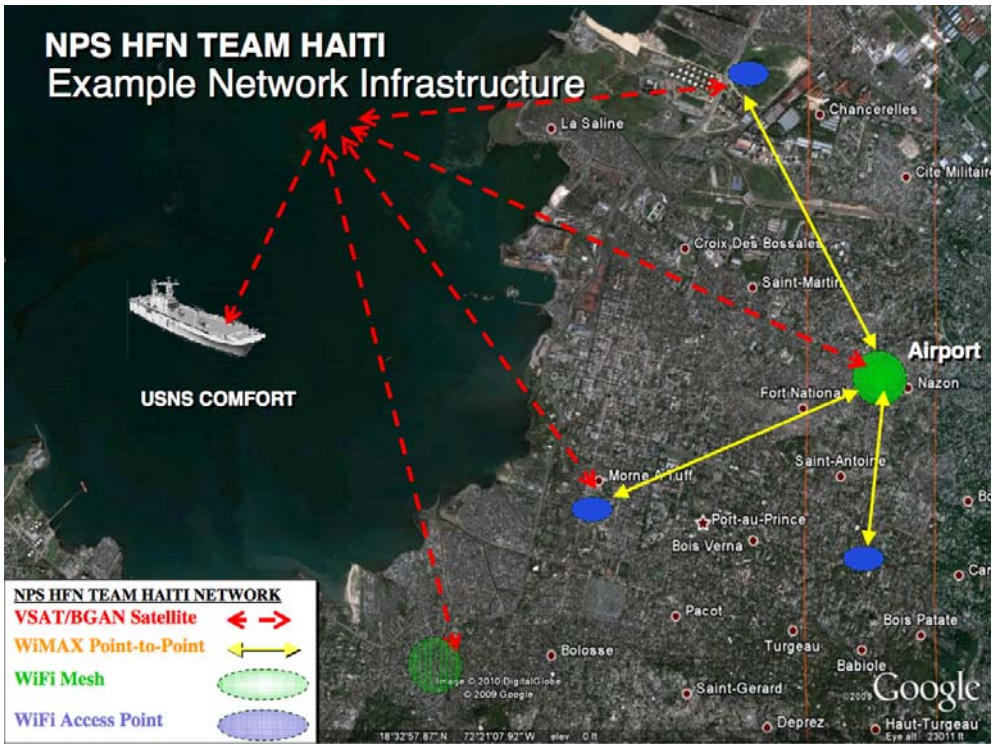


Figure 5. NPS HFN Team's Haiti Network Infrastructure.[93]

For the Haiti mission, the HFN team was able to address issues presented in previous AARs. With some help from NPS students, the HFN team developed an improved technical solution for the FLAKs.[94] The HFN contribution to the Haiti DR mission and international participation resulted in a slightly larger scale relief effort. With a much larger relief effort came a multitude of different international bodies and NGOs. The impact of more organized, international DR resulted in a completely different set of issues. The significant lessons learned from this event are as follows:

- Information overload
- Bandwidth over-utilization and frequency management issues
- International distrust and collaboration issues

93. Brian Steckler, "Hastily Formed Network Information Brief," FCC Data Workshop, 4 October 2011, http://transition.fcc.gov/pshs/docs/summits/DACA/Steckler%20-%20FCC%20DACA%20Workshop.pdf.

94. David D. Lancaster, "Developing a Fly Away Kit to Support Hastily Formed Networks for Humanitarian Assistance and Disaster Relief (HA/DR)" (Master's thesis, Naval Postgraduate School, 2005).

Due to the losses sustained directly to its facilities and workforce, the UN did not have the capability to lead disaster relief efforts.[95] The lack of a contingency disaster mission command and control element caused significant confusion and fostered a feeling of anarchy.

The lack of command and control (C2) empowered individual mission teams, using disparate collaboration solutions, to assume C2 of the mission in their respective areas. The use of disparate collaboration solutions created additional confusion and increased anarchy within the system.[96] Based on Wentz's report, there seemed to be a distinct feeling of information overload due to the using disparate collaboration solutions.

Throughout the deployment, the U.S. Navy had the capability to provide a shared common operational picture (COP). Compartmentalization practices, complex interfaces, large bandwidth requirements, lack of vender-to-vendor data normalization, and social complexity rendered international access to the U.S. Navy COP unattainable. As such, the notion of a unified front for the DR was not possible during the initial phases of the mission.[97]

The absence of frequency management during the mission affected communications between participating teams.[98] The extraordinary quantity of satellite phones, BGANs, and VSAT terminals in close proximity created serious bandwidth and communications interference issues.[99] The lack of a coordinated frequency management plan resulted saturated bandwidth and degraded service capabilities.[100] Social media and interfaces were great assets, but the mission

95. Larry Wentz, "Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010," Center for Technology and National Security (National Defense University, Washington, DC, 08 August 2010).

96. Ibid.

97. Ibid.

98. Ibid.

99. Ibid.

100. Ibid.

teams lacked the capability to fully analyze and mine the data.[101] Twitter, Facebook, Skype, and other social media tools and applications facilitated an unprecedented amount of information flow. The social media interfaces proved the most flexible and useful information tools for the victims due to flexibility, user familiarity, and ease of use.[102]

The use of Short Message Service (SMS)[103] numbers to locate people trapped inside buildings was an irreplaceable asset to search and rescue and resulted in numerous life-saving rescues.[104] The SMS capability is heavily reliant on the availability of existing critical communications infrastructure, which in some cases is not available in the aftermath of a disaster. Fortunately, during the Haiti relief effort there were "pockets" of cellular coverage in the immediate aftermath of the earthquake, thus enabling some critical life-saving SMS traffic.[105]

4. Typhoon Haiyan Deployment

On November 8, 2013, Super Typhoon Haiyan made landfall in the Philippines.[106] Super Typhoon Haiyan was the strongest tropical cyclone to hit land in history, with sustained winds of over 195 miles per hour.[107] As of

101. Larry Wentz, "Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010," Center for Technology and National Security (National Defense University, Washington, DC, 08 August 2010).

102. Brian Steckler, Hastily Formed Networks in Haiti, "Haiti Earthquake After Action Report and Lessons Learned (AAR/LL)" (Naval Postgraduate School, Monterey, CA., 8 September 2010).

103. Margret Rouse, "Short Message Service (SMS)," *techtarget*, July 2007, accessed 7 January 2015. http://searchmobilecomputing.techtarget.com/definition/Short-Message-Service.

104. Brian Steckler, Hastily Formed Networks in Haiti, "Haiti Earthquake After Action Report and Lessons Learned (AAR/LL)" (Naval Postgraduate School, Monterey, CA., 8 September 2010).

105. Brian Steckler, "Hastily Formed Networks for HA/DR." Classroom Instruction (Naval Postgraduate School, Monterey, CA. 22 June–16 September 2014).

106. Jethro Mullen, "Super Typhoon Haiyan, one of the strongest storms ever, hits central Philippines," *CNN World News*, updated 08 November 2013, assessed 23 November 2014, http://www.cnn.com/2013/11/07/world/asia/philippines-typhoon-haiyan/.

107. Ibid.

November 22, 2013, the storm claimed the lives of over 5,000 people, was responsible for over 24,000 injuries, and displaced millions of Filipinos.

The NPS HFN team deployed once again to provide communications infrastructure for disaster relief operations. For the Typhoon Haiyan relief effort, the NPS HFN team deployed to Tacloban, Philippines. The NPS HFN team served as ICT advisors to the 3rd Marine Expeditionary Brigade by conducting Rapid Information and Communication Technology Assessment Team (RTAT).[108] During this deployment, significant capability improvements in social media assessment, reporting procedures, and situational awareness solutions facilitated a more organized and succinct mission.

Figure 6. NPS HFN Team's ICT Training During Typhoon Haiyan Mission.[109]

Despite the added capabilities and functionality, the operation still suffered from technology and policy-based communications shortfalls.

108. Waddell, Joshua and Brian Steckler. "Marine C2 in support of HA/DR: Observations and Critical Assessments Following Super-Typhoon Haiyan." *19th International Command and Control Research and Technology Symposium*, 2013, http://dodccrp.org/events/19th_iccrts_2014/track_chair/papers/120.pdf.

109. Brian Steckler, "HFN Support Briefing on Typhoon Haiyan/Yolanda" (Naval Postgraduate School, Monterey, CA. January 2014).

The initial procedures for RTAT reporting were manual and the capability suffered from severe compartmentalization. When filling in the information for the RTAT Emergency Operations (EMOPS) report, users were required to assess seven primary communications infrastructure criteria. The seven communications criteria are electricity, land lines/fiber, cellular, satellite, Wi-Fi (voice and data), broadcasting (TV/radio), and radio (tactical and commercial bands). By restricting participation to only authorized personnel, the effectiveness of the reporting procedure was limited. Enabling trusted members of the local government would have facilitated faster damage assessments.

The lack of an automated solution for RTAT reporting resulted in manual submission of reports. Major Travis Beason, a 2014 NPS graduate, worked with Lighthouse software to develop an android mobile application to streamline the RTAT reporting process.[110] Appendix B provides additional details on the RTAT project.

Figure 7. Lighthouse RTAT Application and PDC EMOPS Integration.[111]

110. Brian Steckler, "Hastily Formed Networks for HA/DR," Classroom Instruction (Naval Postgraduate School, Monterey, CA. 22 June–16 September 2014).

111. Brian Steckler, "HFN Support Briefing on Typhoon Haiyan/Yolanda" (Naval Postgraduate School, Monterey, CA. January 2014); Travis Beason, "RTAT Survey v6," PowerPoint presentation (Naval Postgraduate School, Monterey, California, n.d.)

COP information overflow is still a challenge. Pacific Disaster Center Emergency Operations Center (PDC EMOPS) provides a free a web based secure map interface (DisasterAware) for sharing situational information.[112] Figure 7 illustrates the integration of the Lighthouse application into the map interface of PDC EMOPS DisasterAware. This tool facilitated RTAT report information sharing in a map-based interface during the Hayian DR mission.[113] Although PDC EMOPS DisasterAware web interface has the capability to provide COP, no legislation appointed DisasterAware as the designated COP provider. This was similar to previous deployments, in which multiple organizations provided their own collaborative solutions.

The relief effort continued to suffer from bandwidth degradation due to oversaturation of satellite communication links. As in the Haiti, the international DR mission teams each provided ICTs, which resulted in additional congestion within the network. Network security was still a challenge for the NPS HFN team and others setting up HFNs. In 2004, the Institute of Electrical and Electronic Engineers (IEEE), a body of standards for communications, deemed the WEP standard obsolete and replaced the standard with Wi-Fi Protected Access (WPA).[114][115] At the time of the deployment, the NPS provided BGANs only supported the outdated and overly unsecured Wired Equivalent Privacy (WEP) standard for encrypting wireless data and traffic.[116]

112. Pacific Disaster Center, “DisasterAware Powered Emergency Operations,” http://www.pdc.org/solutions/products/disasteraware-emops/.

113. Pacific Disaster Center, “Haiyan Response Efforts in the Philippines Transitioning to Recovery Phase,” published 29 November 2013, accessed 30 October 2014, http://www.pdc.org/news-n-media/pdc-updates/Haiyan_Response_Efforts_in_the_Philippines_Transitioning_to_Recovery_Phase/.

114. Scott M. Miller, Terry Ogletree, and Mark Soper, *Upgrading and Repairing Networks*, 5th ed (QUE publishing, 11 May 2006).

115. Guillaume Lehembre, “Wi-Fi Security WEP, WPA and WPA 2,” *Hakin9.org*, vol. 6, June 2005, accessed 19 January 2014, http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf.

116. Hughes and Inmarsat, *BGAN 9201 User Manual*, ver. 4.0, Hughes Network Systems LLC (Germantown, MD. 2009).

In principle to use encryption on a network, all devices must use the same encryption standard. Since the team's Hughes 9201 BGAN only supported WEP encryption standard, to interoperate with the other wireless access points, the legacy standard was required. Use of obsolete encryption standards allows the traffic to be accessible to potential adversaries.

Adding to the use of obsolete standards, the NPS HFN team did not have a plan to implement a layered security plan for its network. There was no way to monitor the network or prevent outside intrusions. In addition, system security, network securities, and acceptable use policies were undefined or did not exist. The lack of a multi-layered security solution for the NPS HFN team left the network in the same security posture as it was in 2004. Without the capability to monitor traffic, identification of an attack was not possible.

Using social media, such as Twitter and Facebook, has proven to be a valuable means of DR communication.[117] Whether we continue to use the available commercial social media tools or develop a DR specific social media tool, we have yet to fully address the risks, benefits, and capabilities of this venue.

C. SOLUTIONS SUMMARY

This chapter provided examples of restructuring, collaborative, and ICT solutions implemented to improve disaster relief efforts. These solutions help to reduce the anarchy within the DR system. Compartmentalization, social complexity, and the lack of international trust form barriers to open communication. These barriers work in concert with each other to increase the anarchy within the DR system.

In addition, it highlighted issues experienced by the NPS HFN team during disaster relief deployments. The issues identified during the NPS HFN team's deployments are as follows:

117. Brian Steckler, "HFN Support Briefing on Typhoon Haiyan/Yolanda" (Naval Postgraduate School, Monterey, CA. January 2014).

- Functionality and durability issues
- Cost of maintaining network equipment
- HFN fly away kit (FLAK) standard was not established or defined
- Equipment durability, accountability, and interoperability issues
- Access to satellite communications was limited
- Network security policies were not in place
- Power generation issues
- Information overload
- Bandwidth over-utilization and frequency management issues
- International distrust and collaboration issues
- Lack of automated reporting (manual RTAT reports)
- Lack of social media integration and usage

Regardless of the solution category, all items presented applied solutions to symptoms rather than addressing the system-level problem. Before providing a solution to this problem, planners must explore the context of the system-level problem within DR.

III. WICKED PROBLEMS AND SYSTEMS THINKING

A. DISASTER RELIEF AS A WICKED PROBLEM

From global warming to refuse disposal, the international community is flooded with complex problems that exhibit wicked characteristics.[118] Rittel and Webber define a wicked problem as "complex, ill-defined, constantly changing, involve lots of stakeholders with conflicting views, and cannot be solved using linear 'system' processes."[119]

A more recent definition of a wicked problem comes from the book *Wicked Problems: Problems Worth Solving*, from the Austin Center for Design (Ac4d). Ac4d defines a wicked problem as "a social or cultural problem that is difficult or impossible to solve for as many as four reasons: incomplete or contradictory knowledge, the number of people and opinions involved, the large economic burden, and the interconnected nature of these problems with other problems."[120]

Another advocate of Horst Rittel's work on wicked problems was Dr. Jeff Conklin. Dr. Conklin's book on dialog mapping for wicked problems proposed a framework for identifying wicked problem characteristics. Dr. Conklin summarized Horst Rittel's description of wicked problem characteristics as the following:

- "You don't understand the problem until you have developed a solution.
- Wicked problems have no stopping rule.
- Solutions to wicked problems are not right or wrong.
- Every wicked problem is essentially unique and novel.

118. Nancy Roberts, Naval Postgraduate School, "Coping with Wicked Problems" (Classroom Instruction, Monterey, CA, 22 September – 18 December 2014).

119. Horst W. J. Rittel and Melvin M. Webber*, Dilemmas in a General Theory of Planning* (Policy Sciences 4, 1973), 155–173.

120. Austin Center for Design (ac4d), "Wicked Problems: Problems worth Solving" (ac4d, n.d.) https://www.wickedproblems.com/1_wicked_problems.php

- Every solution to a wicked problem is a one shot operation.
- Wicked problems have no given alternative solutions."[121][122]

It is difficult to identify whether a problem exhibits wicked characteristics without understanding the problem context or problem space. Dr. Conklin introduced dialog mapping as a process to understand context and identify complex problems that possess wicked characteristics.[123] The dialog mapping process starts with a question or problem statement, and explores all possible ideas and solutions. When combined with Dr. Conklin's dialog mapping process, Rittel's definition allows planners to determine if the problem exhibits characteristics of wickedness.

The following DR question proposes a potential solution for evaluation against Rittel's definition and Dr. Conklin's process, determining if wicked problem characteristics are present in the system: Which country or organization should be ultimately responsible for all global disasters and humanitarian crisis response?

1. "You Don't Understand a Problem Until You Have a Solution"[124]

Using Conklin's process, as ideas evolve from the original problem question additional supporting questions arise. These ideas spawn additional questions, indicated by the icon's number in Figure 8. Many times the additional questions become so complex that they require their own dialog map. The number of additional dialog maps created quickly becomes unruly. For the

121. Jeff Conklin, Ph.D., Dialogue Mapping: Building Shared Understanding of Wicked Problems (John Wiley & Sons. 2005), 7–10.

122. Horst W. J. Rittel and Melvin M. Webber, *Dilemmas in a General Theory of Planning* (Policy Sciences 4, 1973), 155–169.

123. Jeff Conklin, Ph.D., Dialogue Mapping: Building Shared Understanding of Wicked Problems (John Wiley & Sons. 2005).

124. Ibid., 7–10.

proposed question, any idea, results in an inconceivable number of additional problems that require consideration.[125]

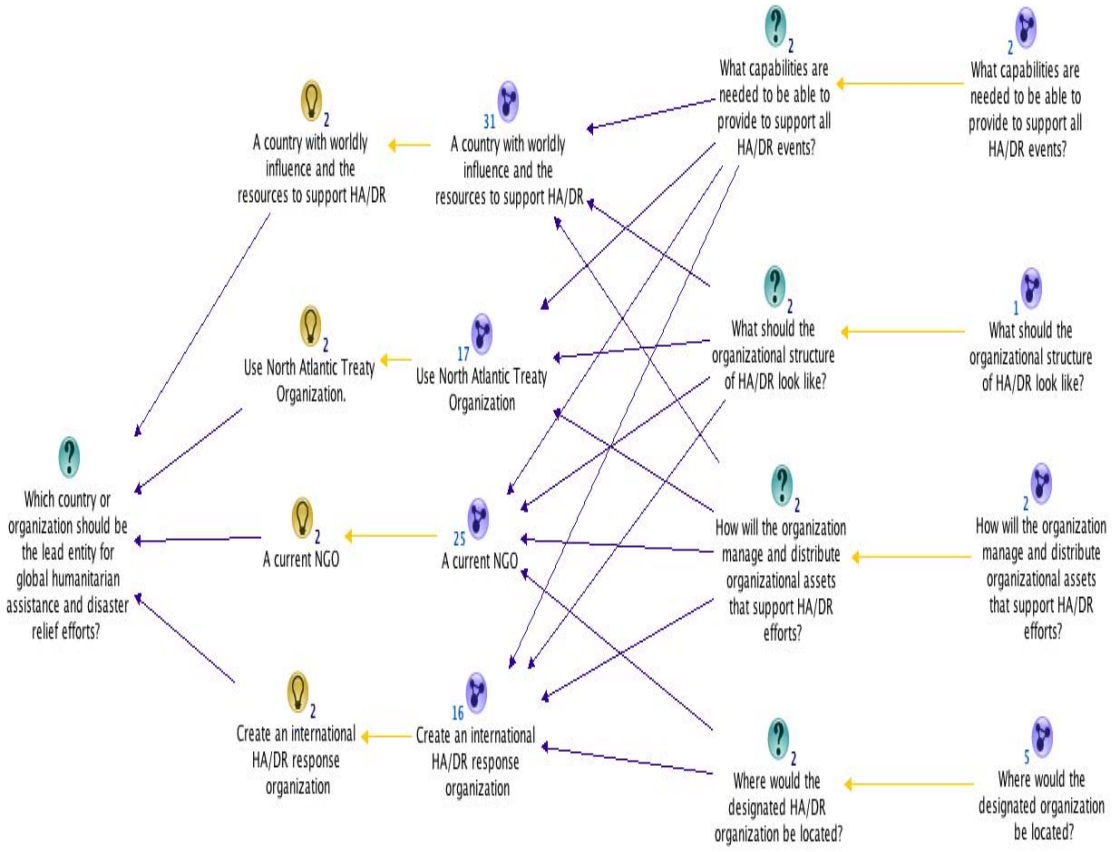


Figure 8. Dialog Map of the Proposed Question.

To understand the complexity in Figure 8, consider that there are currently 192 countries and over a thousand DR organizations that have a stake in the question. Each countries' and organizations' values, morals, desires, and experiences differ. These differences result in organizations providing different solutions, as it is from their own perspectives. The exploration of ideas for solving this problem identifies additional complexities within the problem space.

125. Ibid.

Furthermore, the complexities identified render the selection of a viable solution improbable.

2. "Wicked Problems Have No Stopping Rule"[126]

By looking at Figure 2 and the previous characteristic, it is difficult to identify a distinct stopping point. Shareholders play a big role in organizational decisions, especially in situations such as the proposed question. To appoint an authoritative organization, all of the stakeholders must agree and accept the group's decision. Due to the quantity of stakeholders, attaining a unanimous solution is unlikely. Without unanimous approval, an authoritative figure will not solve the problem. If an authoritative figure is appointed, the social complexity of the stakeholders will act as barriers to conformity. Because of this, there are no methods or indicators to determine when the solution presented solves the problem.

3. "Solutions to Wicked Problems Are Not Right or Wrong"[127]

According to Dr. Conklin, problems are contextual and cannot be identified using simple or complex mathematical equations.[128] Nominating a country or organization as the responsible entity for DR will differ for each country or organization due to many different factors: bureaucratic procedures, legal constraints on scope or authority, or local practice, for example. Stakeholders prefer their own nominations, while strongly expressing reservations against other potential nominees. There is no right or wrong solution; there are only differences in personal preferences and individual biases.

126. Jeff Conklin, Ph.D., Dialogue Mapping: Building Shared Understanding of Wicked Problems (John Wiley & Sons. 2005), 7–10.

127. Ibid.

128. Ibid.

4. "Every Wicked Problem is Essentially Unique and Novel"[129]

Disasters are complex events. Even a disaster that is predictable, such as the typhoons in the Philippines, will impact different stakeholders, different systems, and have different outcomes. During the 2010 earthquake in Haiti, the local government and the United Nations, infrastructure and personnel were destroyed or killed as a result. This situation was unique because the command structure for the response was completely obliterated. Almost every disaster on record presents its own unique challenges physically, socially, and logistically.

5. "Every Solution to a Wicked Problem is a One-Shot Operation"[130]

In a wicked problem, there is no way to test a solution because every solution can have lasting second-order effects, which can create additional problems.[131] In July 2004, the state of Louisiana hosted a disaster preparedness exercise known as Hurricane Pam.[132] Despite the planning and coordination efforts during the exercise, things did not go as planned during the response to Katrina.[133] The plans and processes produced from Hurricane Pam exercise can serve as a baseline for future events. However, exercises assume specific conditions, which may or may not support the reality during actual relief efforts. The expectation that disasters and the relief effort will occur according to plan is unrealistic. As such, every disaster is a one shot operation.

---

129. Horst W. J. Rittel and Melvin M. Webber*, Dilemmas in a General Theory of Planning* (Policy Sciences 4, 1973), 155–169.

130. Ibid.

131. Ibid.

132. U.S. Senate, Preparing for a Catastrophe: The Hurricane Pam Exercise, U.S. Senate Committee on Homeland Security and Governmental Affairs, Senate Hearing 109–403, Washington, DC, 24 January 2006.

133. Ibid.

6. "Wicked Problems Have No Given Alternative Solutions"[134]

After action reports (AARs), from DR events over the last decade exemplify that the lack of centralized responsibility for DR operations directly contributes to the anarchy within the system. There are no given alternative solutions to appointing a responsible entity for DR missions. The question proposed is improperly framed and does not allow for the exploration of alternate solutions.[135] The question proposed addresses one of the symptoms of a system-level problem within the DR system.

Based on the above comparison, there should be no doubt that disaster relief is a wicked problem. In addition to being a wicked problem, the complexity of DR and its international impact warrants classification as a system. Rather than classifying DR as a singular system, other systems such as governments, militaries, nongovernmental organizations, and commercial organizations working in concert towards a common goal constitute a system of systems. As such, it would be premature to propose a solution without an understanding of the interdependencies of the system. To further evaluate the interdependencies in the DR system, planners must identify all relational dependencies within the DR system.

B. DISASTER RELIEF AS A SYSTEM

According to Dr. Derek Anthony Cabrera, systems concepts date back 2600 years, to Lao Tzu's explanation of yin and yang.[136] Systems Thinking is not an equation to solving wicked problems; it is a conceptual framework accessed to understand the system in its related components.[137] The Systems Thinking

134. Jeff Conklin, Ph.D., Dialogue Mapping: Building Shared Understanding of Wicked Problems (John Wiley & Sons. 2005), 7–10.

135. Virginia Anderson and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loops* (Waltham, MA: Pegasus Communications, 1997).

136. Derek Anthony Cabrera, "Systems Thinking" (dissertation, Cornell University, Ithaca, NY, May 2006), http://www.ecommons.cornell.edu/bitstream /1813/2860/1/DerekCabreraDissertation.pdf._May 2006.

137. Ibid., 18.

process defines and explores the entire problem space, properly frames the problem within the problem space, and enables planners to deal with wicked problems. Properly framing the problem within the problem space enables identification of the system-level problem. With the system-level problem identified, stakeholders can develop solutions that can have an impact on the entire system. Many of the symptoms identified will be resolved through implementing the system-level solution.

A system is a group of independent items or objects working in concert towards a common goal or performing individual actions to provide a singular function.[138] The Systems Thinking process relies on the following principles:

- Analyzing the target problem using a big picture perspective[139]
- Identifying and understanding the balancing mechanisms within the system[140]
- Accounting for the complexities of dynamic, interdependent systems[141]
- Understanding the nature and differences between measurable and non-measurable entities within the system[142]
- Account for the socially complex nature of human behavior and identifying its effect on the system[143]

C. A SYSTEMS PERSPECTIVE FOR DISASTER RELIEF

The first step of a Systems Thinking process is to define the problem using a succinct narrative.[144] The narrative provides a short, succinct definition of the problem space.

138. Virginia Anderson and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loops* (Waltham, MA: Pegasus Communications, 1997), 2–21.

139. Ibid.

140. Ibid.

141. Ibid.

142. Ibid.

143. Ibid.

144. Nancy Roberts, Naval Postgraduate School, "Coping with Wicked Problems" Classroom Instruction (Monterey, CA, 22 September–18 December 2014).

1. Narrative

The anarchy created in the aftermath of a natural disaster is uncompromising. The lack of international legislation and appointed authority results in increasing the level of anarchy associated with DR.[145] DR mission teams provide assistance and resources for disaster relief to local first responders, governments, and victims.[146] After DR mission teams arrive, the social complexity of the mission increases, reducing the desire and capability of the mission teams to participate in open 4C. This lack of international participation in open 4C results in a reduction of the overall quality of the response. A reduction in the overall response quality incites additional stress, thus resulting in a longer duration to the relief mission.

2. Identification of Stakeholders

The identification of stakeholders helps the planner conceptualize the social implications within a group. The scope of social impact is directly proportional to stakeholder diversity. An understanding of the diversity and social complexity helps to better identify the problem area. The primary stakeholders for DR are foreign countries, the UN, nongovernmental organizations (NGOs), local governments, and the victims.

D. VARIABLE IDENTIFICATION

The second step in the Systems Thinking process is to identify and name the primary measurable and non-measurable variables.[147] The book *Systems Thinking Basics: From Concepts to Causal Loops* defines variables as components of the problem that can vary over time. Table 1 illustrates the redefined variables for the disaster relief system. The steps for identification of

145. Ibid.

146. Brian Steckler, Hastily Formed Networks in Haiti, “Haiti Earthquake After Action Report and Lessons Learned (AAR/LL)” (Naval Postgraduate School, Monterey, CA., 8 September 2010).

147. Virginia Anderson and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loops* (Waltham, MA: Pegasus Communications, 1997), 41.

variables are identification, consolidate, eliminate, redefine, and verify.[148] Appendix A contains all steps in the Systems Thinking process.

Table 1. The Redefined Variables for Disaster Relief.

Variables	Redefining Variables
Scope of the Disaster	The degree of damage and level of impact that the physical and emotional damage have on the victims of the disaster. The actions of all stakeholders and victims affect the speed and efficiency of recovery operations.
Number of DR Mission Teams	Contingent upon severity of incident. The number of DR mission teams and capability required facilitating an efficient and effective relief.
Response Quality	The overall quality of service provided by the mission teams combined.
Anarchy	Ultimate state of disorder, uncertainty, instability, insecurity, and identification of leadership.
Social Complexity	Humans tend to react in a certain manner based on their individual experiences, beliefs, morals, and values. These reactions are also based upon the norms, values, and belief systems of their country, state, city, and origin.
Stress	Level of stress associated with DR. This includes all stakeholders.

E. PROPERLY DEPICT THE PROBLEM SPACE

The next step in the Systems Thinking process is to properly depict the problem space. In order to properly depict the problem space, three products must be generated and analyzed. These products are a timeline, a behavior over time (BoT) chart, and the initial causal loop diagram (CLD).[149] The results from AARs, academic research, narratives, and redefined variables facilitate creation of these products.

148. Ibid.

149. Virginia Anderson and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loops* (Waltham, MA: Pegasus Communications, 1997), 23–36.

1. Timeline Generation

The timeline bridges the gap between the narrative, the variables, and the products created later in the process.[150] The timeline encourages the planner to define the system processes. The processes discovered form a graphical depiction of DR efforts. An investigation into deployments and AARs indicate that the measurable baseline for a DR mission set is between zero and thirty days.

Prior to a disaster, some organizations participate in 4C activities with designated trusted parties. Most of the 4C activities are in the form of standard operating procedure development, disaster response planning, and pre-disaster exercises.[151] In some cases, there are no pre-disaster 4C interactions between stakeholders. The best scenario is to assume little to no international 4C has taken place prior to a DR event. Based on this assessment, the timeline covers the first thirty-one days of the event. Figure 9 illustrates an example timeline for DR mission set.

150. Nancy Roberts, Naval Postgraduate School, “Coping with Wicked Problems” Classroom Instruction (Monterey, CA, 22 September–18 December 2014).

151. U.S. House of Representatives, *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. 15 February 2006).

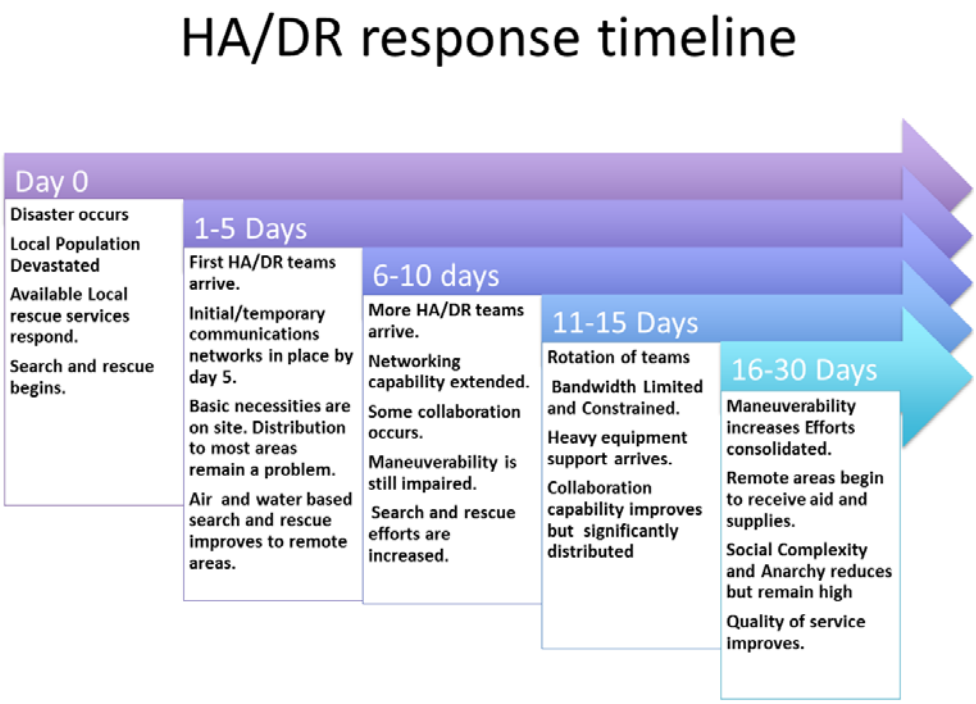


Figure 9. Timeline for Disaster Relief Mission Set.[152]

2. Behavior Over Time Chart

The behavior over time (BoT) chart provides the opportunity to examine each of the variables within the problem space and identify patterns.[153] Once patterns are established, the assessment of the BoT enables the creation of the initial causal loop diagram (CLD).[154] Figure 10 depicts the behavior over time (BoT) chart.

152. Virginia Anderson and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loops* (Waltham, MA: Pegasus Communications, 1997), 18–32.

153. Nancy Roberts, Naval Postgraduate School, "Coping with Wicked Problems" Classroom Instruction (Monterey, CA, 22 September–18 December 2014).

154. Ibid.

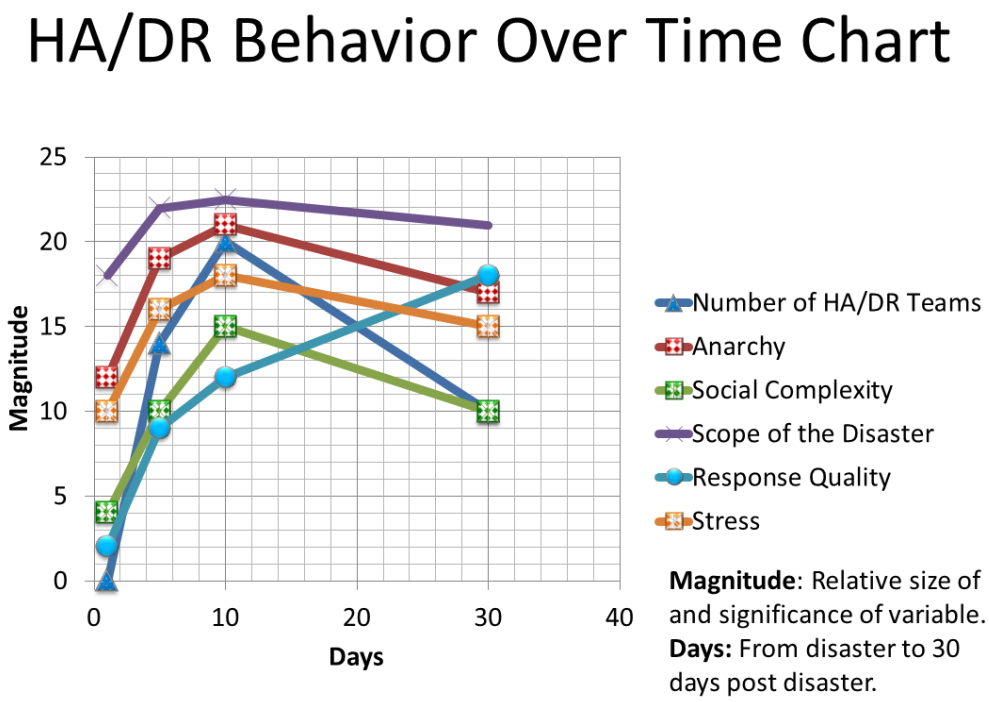


Figure 10. Disaster Relief Variable Relationship over Time.[155]

The initial assessment of Figure 10 shows that the variables of the number of DR mission teams, social complexity, and response quality exhibit an opposing relationship with the scope of disaster, stress, and anarchy. It appears that as the number of DR mission teams increase, response quality increases but not at the same rate as expected. By increasing the number of DR mission teams, anarchy and social complexity increase. Increases in anarchy and social complexity reduce response quality. Adding to the anarchy within the system, the increase of social complexity reduces the desire of the teams to participate in open 4C activities.

The final assessment of Figure 10 warrants a discussion of the impact of the variables on the system as a whole. Because of system interdependencies, applying a solution to one variable may not produce a significant change at the system level. However, if a proposed solution influences more than one variable

155. Virginia Anderson and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loops* (Waltham, MA: Pegasus Communications, 1997).

in the system, the outcome could potentially solve the problem. For instance, if the proposed solution reduces social complexity and anarchy within the system, the scope of the disaster and its duration could significantly reduce.

3. Initial Causal Loop Diagram

The causal loop diagram (CLD) graphically illustrates the problem area.[156] The CLD also defines the relationships between the variables. Figure 11 depicts the initial DR CLD.

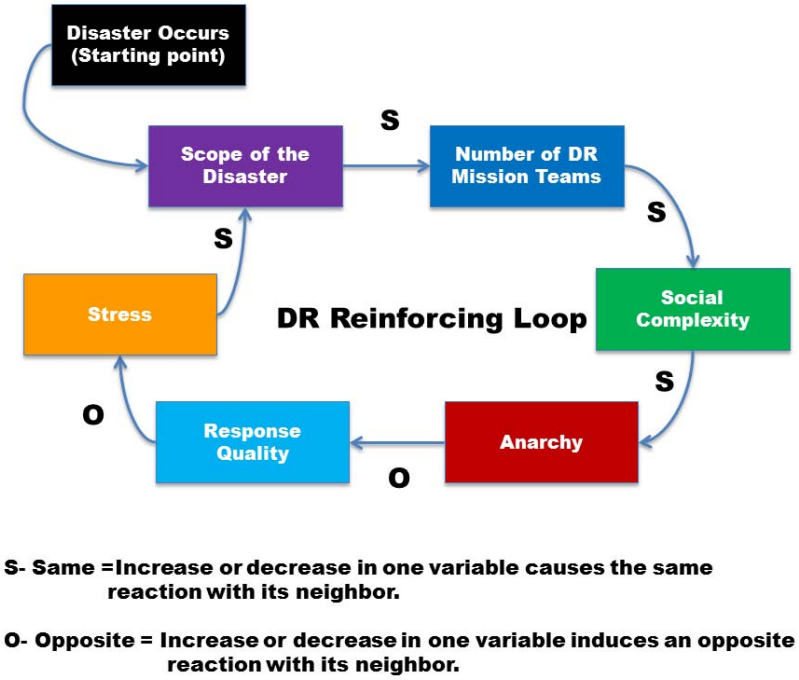


Figure 11. The Initial Disaster Relief Causal Loop Diagram.[157]

156. Nancy Roberts, Naval Postgraduate School, "Coping with Wicked Problems" Classroom Instruction (Monterey, CA, 22 September—18 December 2014).

157. Virginia Anderson and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loops* (Waltham, MA: Pegasus Communications, 1997).

a. Initial Disaster Relief Causal Loop Diagram Flow

The flow of the diagram moves in a clockwise motion. The diagram flow reads as follows:

1. A disaster occurs resulting in catastrophic damage to the affected area. The damage to the affected area determines the initial scope of the disaster.
2. As the initial scope of the disaster increases, the number of DR mission teams required increases.
3. As the number of DR mission teams required increases, the level of social complexity increases.
4. As the level of social complexity increases, level of information anarchy increases.
5. As the level of information anarchy increases, the level of response quality decreases.
6. As the level of response quality decreases, the level of overall stress increases.
7. As the level of overall stress increases, the scope of the disaster increases.
8. As the scope of the disaster increases, the number of DR mission teams required increases.
9. As the number of DR mission teams required increases, the level of social complexity increases.
10. As the level of social complexity increases, the level of anarchy increases.

The relationships between each of the variables within the CLD determine the system model assigned to the causal loop and the problem space.[158] The CLD system model is one of the best indicators of determining when a system-level problem exists. In some cases, assessing the CLD will change the planner's perception of the problem.

Examining the system model facilitates a more thorough understanding of the entire system. This enables the planner to properly frame the problem statement within the problem space.[159]

158. Ibid., 52–73.

159. Nancy Roberts, Naval Postgraduate School, "Coping with Wicked Problems" Classroom Instruction (Monterey, CA, 22 September–18 December 2014).

The system model can be determined by counting the number of opposite relationships in the CLD.[160] An even number of opposite relationships identify the loop as reinforcing, and an odd number of opposite relationships indicate a balancing loop.[161] Reinforcing loops represent systems that remain in a vicious, unrelenting cycle;[162] whereas, balancing loops inject measures to tame vicious uncompromising system cycles.[163]

An assessment of the CLD for DR represents a reinforcing loop and is destined to remain in an uncompromising cycle.[164] The results of the CLD confirm that a system-level problem within DR exists. Reinforcing loops require a balancing mechanism to break the cycle. To apply a balancing mechanism, the planner must identify the system-level problem variable. The system-level problem variable will serve as the balancing solution injection point.

b. Determining the System Level Problem Variable

One way to determine the system-level problem variable is by identifying the negative variables of the system. These variables negatively impact the system and exhibit a distinct opposite relationship with their direct neighbors. Because system variables are interdependent, this process can indicate multiple system-level problem variables. The planner must establish a system for differentiating between potential system-level variables.

One method to differentiate between system-level problem variables is to modify the level of the opposing variables and renegotiate the CLD. Renegotiating the CLD reveals the nature (positive or negative) of each variable. If reducing the variable helps to improve the system, then it is representative of a likely system-level problem variable. If reducing the variable has a negative effect

160. Ibid.

161. Ibid.

162. Virginia Anderson and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loops* (Waltham, MA: Pegasus Communications, 1997), 54.

163. Ibid., 56.

164. Ibid., 22–64.

on the system, then it is not the system-level problem variable. The variable that imposes the greatest negative impact on the system is the system-level problem variable.

Within the DR CLD, there are six variables. Three of the variables have opposing (O) relationships with their immediate neighbors. These variables are response quality, stress, and information anarchy.

1. A reduction of response quality reflects negatively on the system. Response quality is not the system-level problem variable.
2. A reduction in system-level stress would have a positive effect on the system. An increase in system-level stress has a negative effect on the system. Stress is a candidate for the system-level problem variable.
3. A reduction in information anarchy would have a positive effect on the system. An increase in information anarchy has a negative effect on the system. Information anarchy is also a candidate for the system-level problem variable.

To distinguish the system-level problem variable from the remaining variables, a system impact assessment is required. If the stress within the system is reduced, the scope of the disaster is reduced, but not to such a point that it would take away from the physical attributes of the disaster. By the definition in Table 2, a reduction in anarchy would increase the order and organization for the DR mission. Furthermore, a reduction of information anarchy increases the response quality and reduces the stress that occurs because of the catastrophe. When actors have equal access to critical information and share information appropriately, this leads to better coordination, cooperation, and collaboration, thus reducing the anarchic aspects of the on-the-ground response among parties with similar goals and objectives.

4. Properly Frame the Problem

With the system-level problem variable identified, the planner can develop a problem statement that accurately reflects the problem space. The system-level problem statement is as follows:

The lack of information sharing, stress, and social complexity present within the DR system breed chaos and severely reduce the mission teams' ability to effectively communicate, coordinate, cooperate, and collaborate (4C). This leads to anarchic tendencies and confusion among DR participants. Whatever central or leading authority may exist, this confusion and lack of communication are likely to further undermine it. Reduced 4C during DR missions diminishes the quality of the relief, increases the duration of the relief effort, and presents an unsynchronized, disjointed front. The lack of a unified front for DR missions increases the disjointedness and confusion in response, leading to anarchic situations that can result in preventable post-disaster damage, injuries, and loss of life.

5. Injection Point and Validation

Injection points are created to show a vector within a systems model where a balancing solution could break the vicious cycle.[165] From a DR perspective, it would be difficult to implement a solution directly to negative system-level variables. A significant increase in response quality would be difficult without added capabilities from DR mission teams.

Some of the previously discussed solutions focus on establishing a network connection to facilitate 4C activities. For the DR system model, previous solution attributes reside within the variable number of mission teams. As such, the number of mission teams represents the preliminary injection point.

ICT solutions provide responders with a means to participate in 4C. ICT solutions provide additional capability for their individual areas. If a communication strategy combines ICT capability with open 4C interface, the impact produced by the variable number of mission teams may potentially add a balancing structure to the existing reinforcing loop. As such, the number of mission teams represents a valid injection point into the system.

165. Ibid., 65–73.

The next step identifies and defines the balancing loop variables.[166] The author's research shows that organizational restructuring, ICT solutions, and collaboration platforms introduce mechanisms to facilitate 4C and reduce anarchy within the DR system. A reduction in information anarchy may be possible if a solution was to incorporate organizational structure, a communication enabler, and an internationally accepted 4C interface. By definition, the communication, coordination, cooperation, and collaboration variables synchronize relief efforts and help to present a unified front for DR missions. Thus, the variables that make up 4C represent likely variables for a balancing function. Table 2 defines the balancing loop variables.

Table 2. The Balancing Loop Variables for Disaster Relief.

Balancing Variables	Definitions
Communications	The communications variable encompasses all forms of communication. This includes verbal, written, signaled, and electronic communication methods.
Coordination	The coordination variable encompasses, organizing efforts between disparate groups, in preparation for participation in an activity. Coordination works to prevent individual or group actions from interfering with the actions of other individuals and groups.
Cooperation	Cooperation encompasses coordination on a larger scale and occurs when organizations work together for a common beneficial outcome.
Collaboration	Collaboration encompasses the act of organizations working together and sharing information in order to generate a product or system. The product or system modifies, improves, or changes an existing system or process. Collaboration can also facilitate the creation of a new system.

166. Ibid., 58–73.

With defined variables, the balancing loop is ready for insertion into the final CLD.[167] Due to the changes in the DR CLD, it is necessary to reassess the flow and test the CLD diagram. Assessing the CLD flow, verifies whether the added variables maintain a balancing effect.[168] Figure 12 illustrates the final DR CLD.

F. FINAL DISASTER RELIEF CAUSAL LOOP DIAGRAM

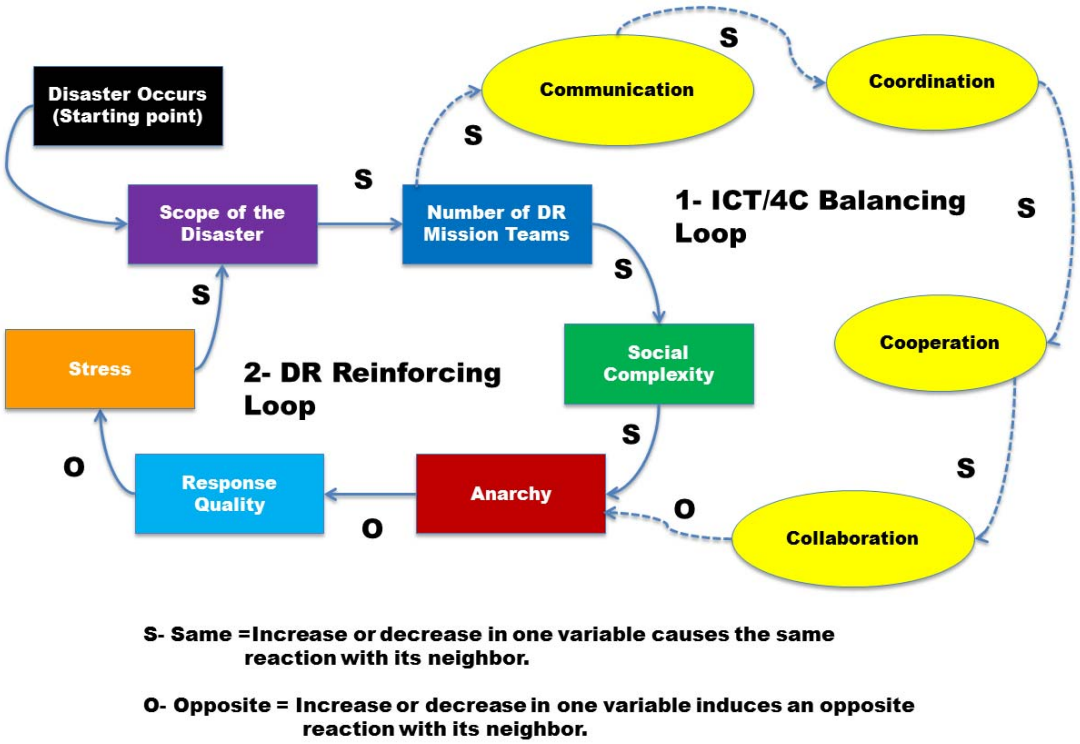


Figure 12. Final Disaster Relief Causal Loop Diagram.[169]

167. Nancy Roberts, Naval Postgraduate School, "Coping with Wicked Problems" Classroom Instruction (Monterey, CA, 22 September–18 December 2014).

168. Virginia Anderson and Lauren Johnson, *Systems Thinking Basics: From Concepts to Causal Loops* (Waltham, MA: Pegasus Communications, 1997), 58–73.

169. Ibid.

The final CLD flow is as follows:

1. A disaster occurs resulting in catastrophic damage to the affected area. The damage to the affected area determines the initial scope of the disaster.
2. As the initial scope of the disaster increases, the number of DR mission teams required increases.
3. As the number of DR mission teams required increases, the communication capability level increases.
4. As the communication capability level increases, the level of coordination increases.
5. As the level of coordination increases, the level of cooperation increases.
6. As the level of cooperation increases, the level of collaboration increases.
7. As the level of collaboration increases, the level of information anarchy deceases.
8. As the level of information anarchy decreases, the level of response quality increases.
9. As the level of response quality increases, overall stress decreases.
10. As overall stress decreases, the scope of the disaster decreases.
11. As the scope of the disaster decreases, the number of DR mission teams required decreases.
12. As the number of DR mission teams required decreases, the level of social complexity decreases.
13. As the social complexity decreases, the level of general anarchy decreases.

Individually, any of the 4C variables could maintain an opposing relationship with social complexity and anarchy. However, combining the 4C variables adds structure and organization to the system. Combining the variables could potentially facilitate establishing a unified front for DR missions. An internationally embraced communications strategy, combining a connection capability with an interface for 4C, could potentially decrease anarchy and tame the vicious cycle within the DR system.

IV. A COMMUNICATION STRATEGY FOR DISASTER RELIEF

The purpose of this chapter is to provide design suggestions and concept prototypes that specifically address the issues within DR from a systems perspective. Previously implemented collaboration solutions have failed to obtain international acceptance because business models or implementation methods did not address social complexity challenges within the DR system. The ideas and concepts from previous solutions are decent; however, the traditional models of ownership, management, and administration do not fit into the DR system. Why do collaborative solution providers continuously embrace traditional (hierarchically-oriented) models of implementation, given the resistance of many critical actors?

Instead of working together to develop a single communications strategy concept, vendors create competing solutions, further adding to information fragmentation. As an international body, DR responders and their respective vendors may need to reassess their priorities.

As identified in Chapter III, DR is a wicked problem. No singular solution, developed independently, will solve a system-level wicked problem. An internationally accepted communications strategy can only provide some measure of reprieve to the system. The concepts in this chapter provide a foundation for addressing the problems within DR from a systems-level approach. These concepts represent a means to inspire the international DR community to begin the development of a common 4C interface. To overcome the anarchy and social complexity impact on DR missions, the international community should consider the design suggestions and prototype concepts in this chapter.

A. TRUSTED ORGANIZATION FOR INTEGRATION MANAGEMENT

As discussed, social complexity leads to a vicious cycle where actors do not communicate effectively, cannot get a full understanding of the situation, and

thus, they cannot coordinate or collaborate effectively.[170] This means they are less likely to cooperate with one another, because cooperation involves exposing their operations to greater risks—risks of blame for failure and errors, risks of having their productivity and success attributed to others, and other problems.[171] Developing a concept that does not address social implications of the system would be counterproductive to effective 4C and would likely fail.

DR stakeholders have their own agendas, biases, and social complexity issues. As such, designating an existing DR entity or 4C solution provider as manager and service provider for the integration interface may prove difficult. To alleviate preconceived biases and social issues between DR mission entities, the creation of a trusted third-party organization may present a viable alternative solution for inspiring open and transparent 4C for DR.

In concert with the previous statement, a fundamental step for developing this communication strategy is appointing or establishing a trusted organization. The trusted organization would provide the following three functions: 1) Integration application development and testing; 2) Interface development, management, and administration; and 3) Community development and international relations. In addition, the new organization can assist with partner-to-partner negotiations. The new organization addresses some of the social issues within DR using modular measures.

Modular measures for this strategy involve the development of custom packaged interfaces for individual DR stakeholder organizations. These interface modules create a stakeholder-specific private community for its organizations. Private community design enables regional governments and organizations to have their own personal space for 4C within their respective countries or organizations. Information, resident and shared within the private communities, is restricted to the community and specified community partners. The custom

170. Rebecca Goolsby, telephone call with author, 5 March 2015.

171. Ibid.

packaged interface design enables pre-disaster partnerships between stakeholders through custom memorandums of understanding (MOUs) and service level agreements (SLAs).

MOUs establish the informal terms of understanding between two private communities. The SLA is a document created by the trusted third-party organization; it contains an overview and implementation specifications based on the MOU. A signed SLA allows a temporary merge of operational interfaces for the purposes of a single DR mission. This includes, but is not limited to, common interface tools, use of common DR information, and the creation of disaster response plans.

B. COMMUNICATION STRATEGY CONCEPTS

The DR communication strategy does not create new or novel technologies; rather, it is an integration of existing technology into a usable and functional solution. This approach uses ICT capability to provide a connection to an integration interface. The strategy creates or appoints a trusted organization to manage custom packaged interfaces. The custom packaged common interface is where the international community, local governments, NGOs, and commercial DR organizations can interact within their own organizational communities. Custom packaged interfaces also enable integration of existing DR tools and solutions such as Dropbox, Skype, APAN, Jabber, Inrelief, and DisasterAware.

In the event of a disaster, the communities could come together to share a common interface through integration and data normalization. Community integration allows the local government to maintain command and control (C2) while seamlessly presenting a unified front for International DR missions. Figure 13 presents the disaster relief conceptual model. Integration and data normalization occurs through application development. These applications provide translation services, so that common information converts appropriately into the private community interface format.

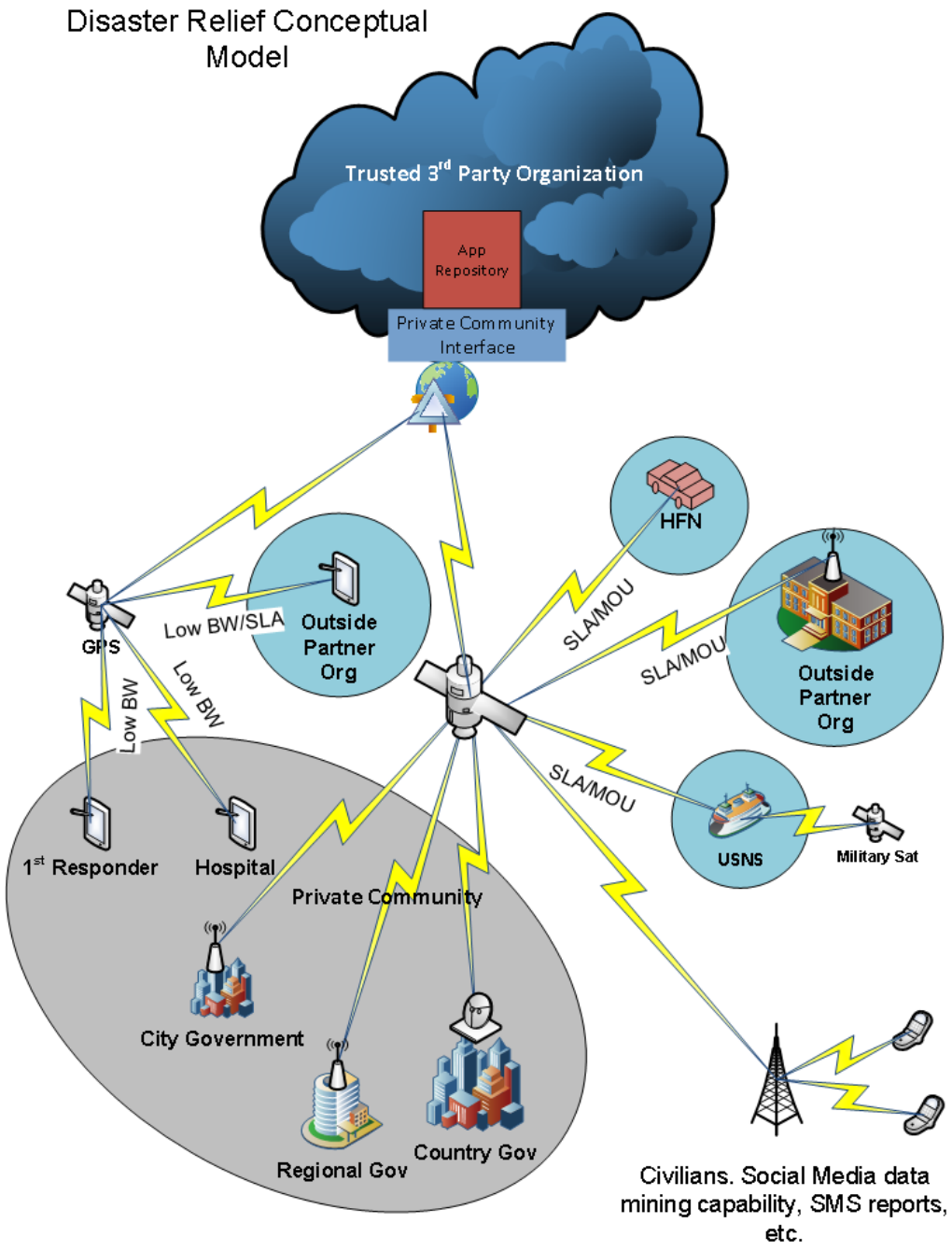


Figure 13. Disaster Relief Conceptual Model.

1. Providing a Connection

Communication in austere environments, with limited resources, requires the responder to have all necessary elements on hand when responding to a disaster. The selection of an ideal ICT system is contingent on many different

factors, but the most pertinent are finding a highly deployable, inexpensive, and secure communication system with scalable levels of service. Highly deployable indicates that ICT systems must be capable of deploying to the disaster area on very short notice. Inexpensive and affordable are acceptable goals. However, cost is relative to required bandwidth and user support requirements. The package examples below have varying levels of cost, based on purpose and bandwidth requirements. Although availability and integrity are the focus, the focus does not dismiss the need for security. A communications strategy should show a balance between information sharing and security.[172] The requirements for security increase in proportion to the size of the organization, functions, and ICT package chosen.

Organizations and mission teams vary throughout the DR community. As these teams refine their roles and desired capabilities, bandwidth requirements vary. To ensure scalable levels of service, the easiest approach is to introduce packages for varying organizational needs.

2. Information and Communications Technology Solution Concept

This section explores the capabilities of three median-level packages. The following characteristics of the three packages are as follows: deployability, cost, and security. Figure 14 provides a conceptual diagram of the three package categories.

172. Larry Wentz, "An ICT Primer: Information and Communication Technologies for Civil-Military Coordination in Disaster Relief and Stabilization and Reconstruction," Center for Technology and National Security Policy (National Defense University, Washington, DC. June 2006), p.51.

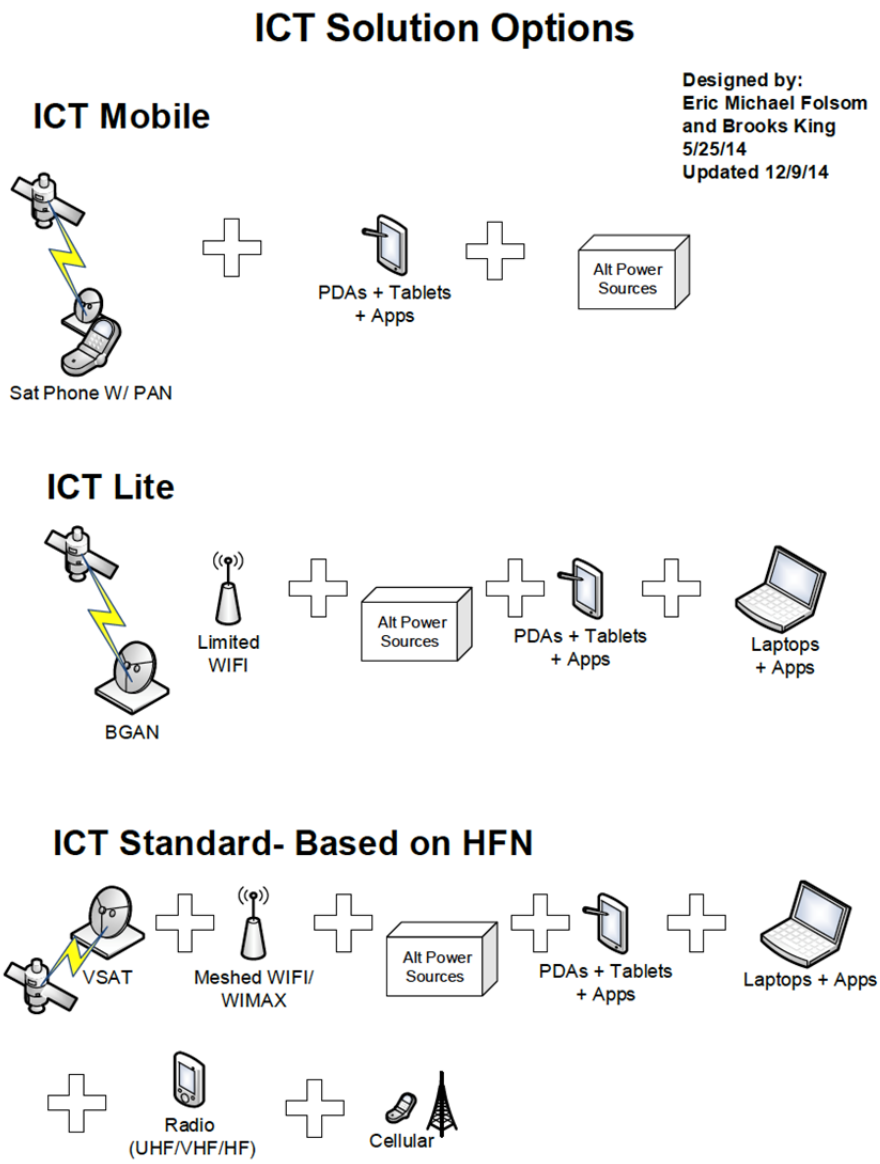


Figure 14. ICT Package Options.[173]

a. ICT Mobile

ICT Mobile packages provide the least amount of bandwidth, are highly deployable, and are inexpensive. Their size and cost make them an ideal choice for contingency communications. If ICT Mobile is the desired solution, teams

173. Folsom, Eric and Brooks King, ICT Packages Concept, HFN Class Project, June 2014.

should work with ICT providers to develop methods to encrypt data-in-transit and at rest.

A median solution identified for ICT Mobile is using a Delorme inReach Explorer Extreme.[174] The inReach has the capability to send text messages of up to 160 characters in each text. In the current configuration, the device sends a message to Delorme. If coordinated in advance, Delorme could forward all messages from specified devices to a designated phone number or individual. This allows for position reporting, status updates, and resource request.

Use of this system would be perfect for prepositioning in places like hospitals, fire departments, and police stations in countries or areas that are prone to a disaster. There is also the potential to develop an application that allows the device to access metadata from a map source; this potentially facilitates access to a common operational picture and serves as a guide to obtaining the assistance required.

The baseline package for Delorme inReach with unlimited text messaging is approximately $499.95 + shipping and $1200 per year for service.[175] Delorme inReach uses the GPS frequency bands (L1 and L2). The use of GPS communications reduces the impact on L Band (BGAN) devices. GPS accesses a different frequency range and uses different satellites for communications.[176] Figure 15 is a picture of the Delorme inReach Explorer.

174. Delorme, “Delorme inReach Explorer Extreme,” Delorme website, accessed 14 December 2014, http://www.inreachdelorme.com/product-info/inreach-explorer-extreme-communication-kit.php.

175. Ibid.

176. Lonnie Wilson, Ph.D., Naval Postgraduate School Professor, email message to author, 12 December 2014.

Figure 15. Delorme inReach Explorer Extreme.[177]

b. ICT Lite

ICT Lite packages deliver more bandwidth to the customer. The baseline package for ICT Lite consists of a Broadband Global Area Network (BGAN), an alternate power source, laptop computers, and mobile devices. This package allows for the implementation of an IEEE 802.11 wireless network and can concurrently support up to eleven users depending on their usage of the bandwidth. More than eleven users would require the purchase of a wireless router. BGAN is capable of speeds up to 490 Kbps.[178]

177. Delorme, "Delorme inReach Explorer Extreme," Delorme website, accessed 14 December 2014, http://www.inreachdelorme.com/product-info/inreach-explorer-extreme-communication-kit.php.

178. Network Innovations, "BGAN or VSAT Comparing Technologies," 26 April 2012. accessed 14 December 2014, http://www.networkinv.com/bgan-or-vsat-comparing-the-technologies/.

A BGAN system is still highly deployable. BGANs are airline transportable and are small enough to fit into carry-on bags. ICT Lite packages are much more expensive than ICT Mobile packages, but offer significantly more capability for DR mission teams. Most ICT Lite solutions come with embedded security features. DR mission teams should closely examine each providers BGAN solution to ensure that vendor default encryption and other security controls do not rely on obsolete security standards.

A median package for ICT Lite could be a Hughes 9201 BGAN Satellite Terminal for approximately $3000.[179] The annual service plan is based on price per megabyte. A median price range is 500 MB for approximately $3000 per year.[180] The estimate for the entire package is roughly $5,500 for the equipment and 1 year of service. Then for continued service, it is $2,499 per year. Figure 16 illustrates this package.

179. Ground Control Global Communications, “Inmarsat BGAN pricing,” accessed 14 December 2014, http://www.groundcontrol.com/Hughes_9201_BGAN.htm

180. Ground Control Global Communications, “Inmarsat Service Plan pricing,” accessed 14 December 2014, http://www.groundcontrol.com/BGAN_rate_plans.htm.

Figure 16. Hughes 9201 Broadband Global Area Network (BGAN).[181]

c. ICT Standard

ICT Standard packages have the potential to deliver maximum capability to the mission team. These packages may consist of a very small aperture terminal (VSAT) and a pair of Redline 802.16 WiMAX antennas. ICT Standard solutions provide sufficient capability for larger organizations with greater than

181. Hughes, "9201 BGAN terminal documentation," accessed 14 December 2014, http://www.hughes.com/technologies/mobilesat-systems/mobile-satellite-terminals/hughes-9201-bgan-inmarsat-terminal.

eleven concurrent users. HFN's current ICT Standard implementation fits into ten airline transportable tough boxes, making them highly deployable. An ICT Standard package represents the most costly and scalable solution. The VSAT terminal can range from $20,000–$200,000 for the dish itself. In addition, the monthly service plan ranges from $3,000–$20,000 depending on the data rate and the organizational requirements. For extra add-on capabilities, such as ruggedized Redline (or similar) WiMAX antennas, Persistent Systems (or similar) Wave Relay Wi-Fi, and RoIP interfaces, the cost would increase substantially. Annual cost estimate would be $36,000–$240,000 depending on the service plan.

As with ICT Lite, ICT Standard packages come with mechanisms to provide basic security. As bandwidth increases, the cost of service and the number of end devices increases. As end devices connect to the network, system and network vulnerabilities can increase exponentially. When possible, DR mission teams should ensure that end devices receive updates prior to responding to a disaster. Reducing existing vulnerabilities prior to a deployment can significantly reduce the chance of an adversary gaining unauthorized access. Figure 17 illustrates one of ViaSat's very small aperture terminals. Figure 18 displays a picture and some basic data on Redline's 802.16 WiMAX antennas. Figure 19, highlights the key components in Persistent System's WAVE Relay point-to-point network.

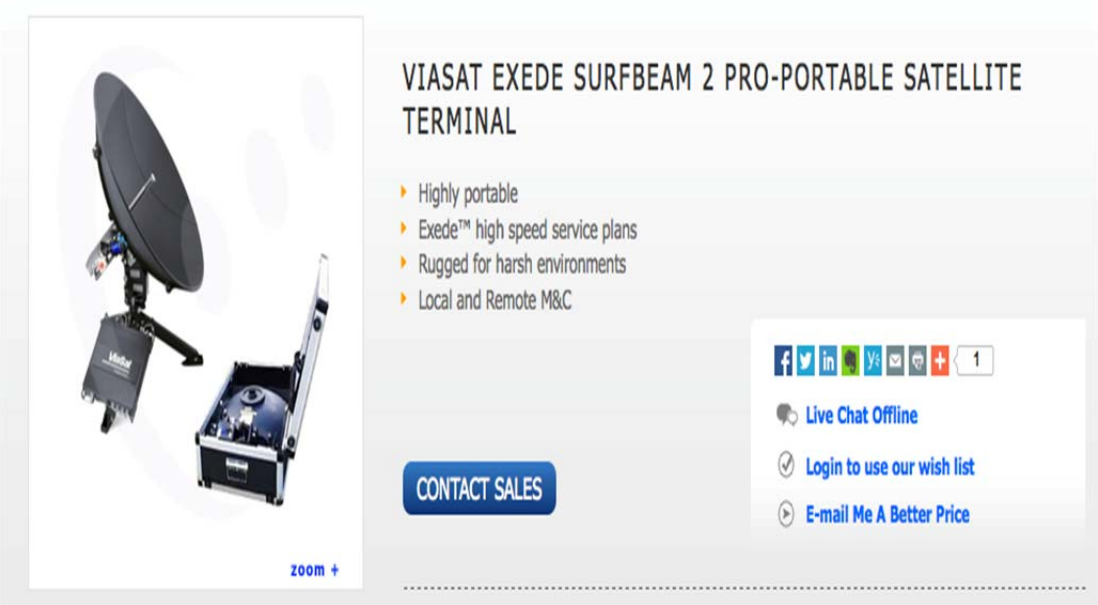


Figure 17. Very Small Aperture Terminal (Vsat).[182]

182. Satcom Resources, “Mobile VSAT terminal,” assessed 14 December 2014, http://www.satcomresources.com/Viasat-Exede-Pro-Portable-Satellite-Terminal?sc=8&category=7313.

Virtual Fiber™ Outdoor Wireless TCP/IP Transport

RAS-EXTEND

Full Motion Auto-Acquire Wireless TCP/IP Data Terminal

The RDL-3000 RAS-Extend series provides secure reliable wireless transport directly to land vehicles, marine vessels, and floating platforms in motion. Easily operated by non-technical personnel with no special training, the RAS-Extend automatically obtains and holds a reliable high-speed connection to the fixed Redline wireless network.

FEATURES AND BENEFITS

- The highly reliable touchless operation and self-aiming antenna with continuous signal and GPS tracking, requires no specialized (telecom) personnel for normal operation
- High throughput for concurrent transport of M2M telemetry and telecontrol, data, video and voice services
- Durable all-weather enclosure for reliable operation in a wide range of temperatures and environmental conditions
- Over-the-air monitoring, configuration and software keyed features enable upgrades without physical access
- Software-defined architecture enhances reliability and service lifetime

PRODUCT COMPLEMENTS

The RAS-Extend is fully compatible with all Redline RDL-3000 family base stations and wireless terminals. Redline provides a complete selection of peripherals and professional services for all your deployment needs.

UNIFIED GLOBAL SOLUTIONS

Redline's patented UWT™ technology provides a truly unified wireless networking solution—across the spectrum, across your company and across the globe—enabling secure, reliable, high-speed connectivity to people and smart devices everywhere.

SYSTEM AT A GLANCE

Outdoor auto-acquire software-defined wireless terminal

Extends high speed TCP/IP transport to moving land vehicles, marine vessels and floating platforms

Reliable fast transport of M2M, data, HD video and voice traffic

Auto-acquire with full-time tracking and automatic antenna alignment with built-in GPS

Wide selection of MIMO antennas

-15 to 55 °C operating range using dynamic and thermal dissipation (no moving parts)

High-grade cyber security features

Very low latency supports time-sensitive applications

Over-the-air monitoring, configuration, upgrades and software keyed speeds and features

Figure 18. Redline 802.16 WiMAX Line of Sight (LOS) Antenna.[183]

183. Redline Communications, "WiMAX Line of Sight Antenna," accessed 14 December 2014, http://rdlcom.com/products/ras-extend.

Figure 19. Persistent Systems WAVE Relay Wi-Fi and Point-to-Point (P2P) Network[184]

3. Power Generation for Solutions

Some ICT packages only work with the provider's alternate power sources; whereas, other ICT packages require the consumers to procure their own alternate power source solutions.

Due to natural occurrences, disasters can occur anywhere in the world, which makes it difficult to recommend a specific vendor for ICT alternate power generation capability. The massive numbers of ICT kits available with varying power requirements preclude specifying an ideal power solution. Alternate power generation requirements will vary depending on the size and functionality of the

184. Persistent Systems, "Wave Relay Manual - WR-01," ver. 1.1, issued 12 April 2012, accessed 14 December 2014.

mission team. The chart in Appendix D provides a comparison of alternate power generation technology.

C. A 4C INTEGRATION INTERFACE

APAN, Relief Web, and Inrelief all provide portals to assist in 4C planning and collaboration. Software solutions such as Jabber and Skype equip responders with the capability to coordinate on the ground via voice and chat. Organizations such as PDC EMOPS, ArcGis, Google, and OpenStreetmaps provide tools and capabilities to develop a common operational picture. There is currently no way to integrate these capabilities into a common interface and to allow maximum flexibility and user preference. Thus, these solutions are problematic. Based on Larry Wentz's research[185] and lessons learned, a solution that integrates existing technologies and 4C vendor solutions into a common DR mission interface could result in the desired system-level impact. The solution must provide coverage of the following issues and attributes:

- Ownership, implementation, administration, and hosting
- Cloud models of service and deployment
- Application interface
- Mobile application interface
- Security implications of the models

1. Ownership, Implementation, Administration, and Hosting

Development of the trusted third-party organization is the key to solving the issue with deciding ownership, management, and administration. Due to potential social implications, a single government, military, or existing DR organization cannot assume responsibility for ownership, management, and administration of the integration interface concept. As mentioned in the example question in Chapter III, appointing an outside entity as C2 for DR missions could result in irreversible second and third order effects.

185. Larry Wentz, "Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010," Center for Technology and National Security (National Defense University, Washington, DC, 08 August 2010).

Another factor to consider is hosting for the interface. Since disasters can occur worldwide, hosting the interface only in the United States or in another single country would not be effective. To provide open and continuous access to the interface, it has to be hosted in a distributed manner.

One possible solution is to use cloud-computing technology as a means to provide distributed access to the integration interface. The use of cloud technology allows the greatest flexibility by providing the essential characteristics of on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[186]

On-demand self-service allows the consumer to adjust resource requirements as needed, without additional human interaction.[187] *Broad Network Access* allows device agnostic connections to network assets and resources.[188] *Resource Pooling* provides a vast quantity of storage, processing, network bandwidth capability, and other resources for the consumer on-demand while maintaining ambiguity of where the resources are actually located.[189] The *Rapid Elasticity* component allows high availability models to succeed through the automatic variability of resource requirements based on consumer resource needs.[190] Finally, the *Measured Service* component ensures usage transparency through providing monitoring, controlling, and statistics to the consumer.[191] The essential characteristics of a cloud-based solution have the potential to grant the consumer access to a wealth of on-demand resources.[192]

186. Wayne Jansen and Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, National Institute of Standards and Technology Special Publication (NIST SP 800–144) (Gaithersburg, MD, December 2011), p.4.

187. Ibid.

188. Ibid.

189. Ibid.

190. Ibid.

191. Ibid.

192. Ibid.

Hosting cost is an additional consideration for moving services to the cloud. Building infrastructure to host an internationally distributed interface that uses a traditional data center model would require a significant amount of money to build. In addition, maintaining a large employee base for application development, information management, and information security on a distributed international scale is likely to be unattainable.

Traditional storage cost versus cloud-based storage cost is a key factor to consider. The cost of accessing cloud storage is much less than the cost of traditional hard drive cost. Table 3 provides a short comparison.

Table 3. Cloud Storage Versus Traditional.

Mode	Hard Drive1 [193]	Hard Drive2 [194]	Amazon Web Svc[195]	Microsoft Azure[196]
Brand/ Model	Seagate NAS SATA HDD	Western Digital NAS SATA	Amazon S3	Block Blobs
Capacity	2 Terabytes	2 Terabytes	2 Terabytes	2 Terabytes
$ per Unit	$119.99	$99.99	N/A	N/A
$ per TB	$59.95	$49.99	$20.48-$61.44	$40.96 - $122.88
$ per GB	$17.08	$50	$0.01 – $0.03	$0.02 - $0.06
$ per year	$0	$0	Usage Based	Usage Based

When disasters occur and DR mission teams deploy, resource requirements increase significantly; they decrease as the teams complete their

193. Tiger Direct, "Seagate Hard Drive Advertisement," accessed 29 January 2015. http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=9557692&CatId=4357.

194. Tiger Direct, "Western Digital Hard Drive Advertisement," accessed 29 January 2015, http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=3580091&csid=_61.

195. Amazon Web Service, "Storage Pricing," AWS EC2, accessed 20 January 2015, http://aws.amazon.com/ec2/pricing/.

196. Microsoft Azure, "Storage Pricing," MS Azure, accessed 20 January 2015, http://azure.microsoft.com/en-us/pricing/details/storage/.

missions and return home. Private community models for the international DR community have an undefined requirement for computing resources.

An enterprise system managed by an IT staff does not have the scalability that is present in a cloud-based deployment. In addition to scalability, the cost of maintaining staff to service an enterprise solution would be significant. Employing staff, leasing data centers, and paying the electric bill associated with operating the data center are factors that greatly outweigh the cost to procure cloud services.

2. Cloud Models of Service and Deployment

One of the key focuses for DR mission teams is allowing the local government to serve as primary command and control for the relief effort. Any technology solution for DR missions must consider ways to protect the integrity of that command structure. As such, the cloud service and deployment model design has to incorporate methods that facilitate a local government led effort.

The service model selected should provide an interface for the DR customers. The cloud model of service for a DR system-level solution would need to support the development, testing, and implementation of applications that facilitate integration of existing 4C solutions.

In accordance with the National Institute of Standards and Technology (NIST) special publication, there are three types of service models and four types of deployment models for cloud based solutions. Tables 4 and 5 identify the models for service and deployment.

Table 4. Cloud Service Models.[197]

Service Models	Access Granted
Software as a service (Saas)	Consumer can access and use provider software. Provider is responsible for all security.
Platform as a service (PaaS)	Consumer can create programs using provider-approved methods and deploy applications into the cloud. Consumer is responsible for application security.
Infrastructure as a service (IaaS)	Consumer has power to build, modify and maintain servers. Consumer is responsible for all privacy and security considerations.

Software as a service (SaaS) would allow use of specific software or interface. From a user's perspective, this model does not allow specific configuration. Interfaces would remain fixed. SaaS is a common model used for access to Electronic health records (EHR) and electronic medical records (EMR). Confidentiality, integrity, availability, and authentication (CIA-A)[198] of data and information are the responsibility of the vendor or SaaS service provider.

The platform as a service (PaaS) model facilitates more flexibility by allowing the user to create useful applications and interfaces. PaaS provides organizations and users with the capability to develop and test their own applications. Upon provider approval, they can integrate these applications into the interface. The negative aspect to the PaaS model is that only the provider can approve interface implementations.

Infrastructure as a service (IaaS) allows the maximum control of the servers, software development, and implementation. It still follows the distributed cloud based architecture. By increasing the flexibility to an IaaS, the consumer is now the provider. Now, the consumer is responsible for all aspects of security and privacy from the virtual servers and storage to application security. Although IaaS is the most powerful and flexible cloud-based model of service, it requires

197. Wayne Jansen and Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, National Institute of Standards and Technology Special Publication (NIST SP 800–144) (Gaithersburg, MD. December 2011), 4.

198. Shon Harris, *All-In-One CISSP Exam Guide*, ed.4 (New York, NY: McGraw-Hill, 2008).

the most overhead, administration, and cost to the consumer. Depending on their prescribed functions and operation, very large organizations with an existing enterprise network may benefit from moving some or all aspects of their network to an IaaS model.

Table 5. Cloud Deployment Models.[199]

Service Models	Access Granted
Private Cloud	**Use:** Single Organization **Management:** Internal or external organization. **Location:** Local or remote
Community Cloud	**Use:** Specific Community **Management:** Single organization, multiple organizations, or external organization. **Location:** Local or remote
Public Cloud	**Use:** Open to the public **Management:** Business, academy, government **Location:** Cloud provider premises
Hybrid Cloud	A combination of two or more deployment models which are typically unique.

3. Private Community Disaster Relief Plans and Partnerships

Regardless of proximate causation, the local government will always take the blame for a botched response to disaster relief. With this in mind, the custom interface designer must provide a means to share information with early responder organizations outside of their private communities while allowing the local government to remain in command and control (C2) of the relief effort. The example DR cloud model in Figure 20 provides community partnership capability to share information. Partnerships are typically specified using memorandums of understanding (MOUs) and service level agreements (SLAs).

199. Wayne Jansen and Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, National Institute of Standards and Technology Special Publication (NIST SP 800–144) (Gaithersburg, MD. December 2011), 3, 4.

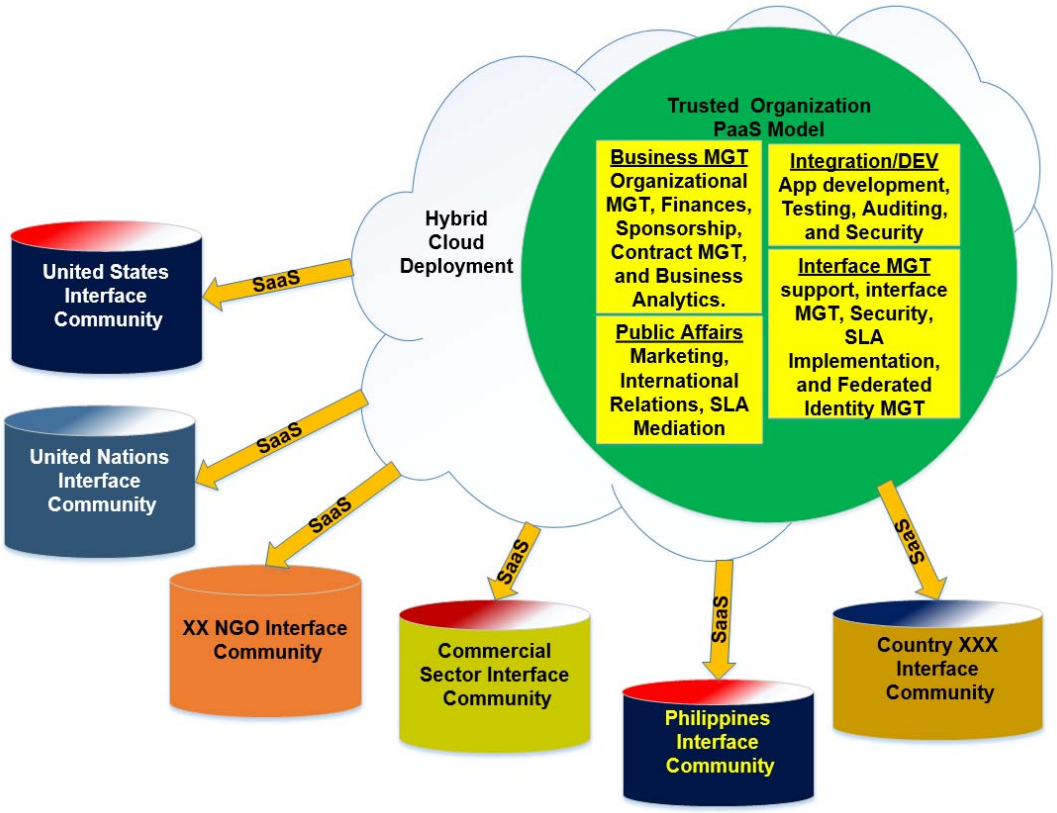


Figure 20. Disaster Relief Cloud Deployment Model Example.

Establishing disaster response plans will significantly reduce anarchy and chaos that occurs because of the disaster. Thus, it is important for organizations to develop a disaster response plan (DRP) and a contingency disaster response plan (CDRP). The DRP allows local governments to develop procedures that facilitate saving lives and expedite recovery within respective countries.[200]

DRPs consider all aspects that deal with emergency response for the country. In the case of a very large-scale disaster, the government may or may not have the capability to effectively implement its DRP. As was experienced in Haiti in 2012, the government and UN were incapable of leading an effective

200. Ready.gov, "Emergency Response Plan," 19 December 2012, accessed 10 January 2015, http://www.ready.gov/business/implementation/emergency.

relief effort.[201] In situations such as this, a CDRP could provide continuity when the local government is not able to respond effectively.

As most people understand, things do not always work as planned. However, having a countrywide DRP and CDRP would provide a framework by which local government and incident responders could modify or change the plan to meet the situation at hand. In line with General George S. Patton, “A good plan executed violently now, is better than a perfect plan executed next week.”[202] Having the framework in place could significantly reduce chaos, anarchy, and recovery time.

A DR communication strategy supports the development and implementation of DRPs and CDRPs. Furthermore, the concepts introduced in this chapter support and encourage development of community wide DRPs and CDRPs. DRPs within a private community or a country, enumerates the processes for the disaster response system within the country. The CDRP designates what occurs in the event that the country is unable to effectively respond to the crisis. The CDRP spells out which partner organizations will be involved in the relief effort. The CDRP replicates the DRP processes, but it also establishes temporary leadership roles when the local government is unable to maintain C2 of the response. The temporary mission leader follows the procedures spelled out in the DRPs of the private communities and only uses the collaboration and integration tools authorized by the local government.

Creation of the CDRP integrates partner organizations into the concept of operations before an incident occurs. When a disaster occurs, the DRP and CDRP guide the activities of participating mission teams. A clear understanding

201. Brian Steckler, “Hastily Formed Networks for HA/DR.” Classroom Instruction (Naval Postgraduate School, Monterey, CA. 22 June–16 September 2014).

202. General George S. Patton Jr., “Quotes,” accessed 13 January 2015, http://www.generalpatton.com/quotes/index.html.

of the roles and responsibilities of the DR mission teams combines relief efforts and presents an international based unified front for the DR.[203]

Issues, mentioned throughout the AARs and in Larry Wentz's comments, stress bandwidth saturation and the lack of a frequency management plan.[204] The preplanning that occurs during the development of the DRP and CDRP facilitates the creation of a frequency management plan. A local government dictated frequency management plan could potentially reduce some of the issues with bandwidth saturation and interference during disaster relief missions. Figure 21 illustrates the proposed partnership concept, and Figure 22 represents the private community relationship model.

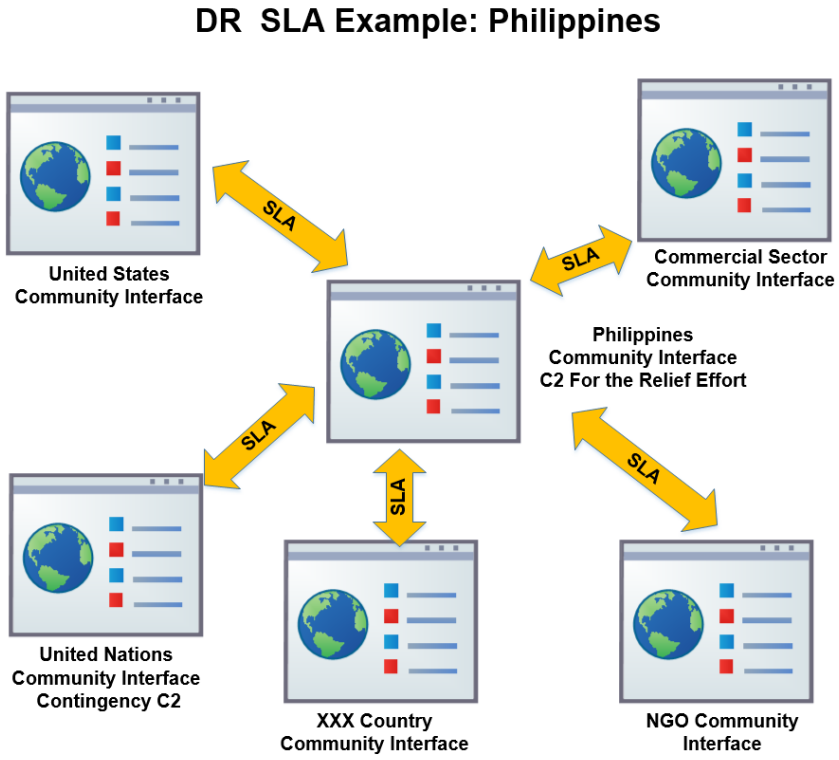


Figure 21. Service Level Agreement Partnership Concept.

203. Larry Wentz, "Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010," Center for Technology and National Security (National Defense University, Washington, DC, 08 August 2010).

204. Ibid.

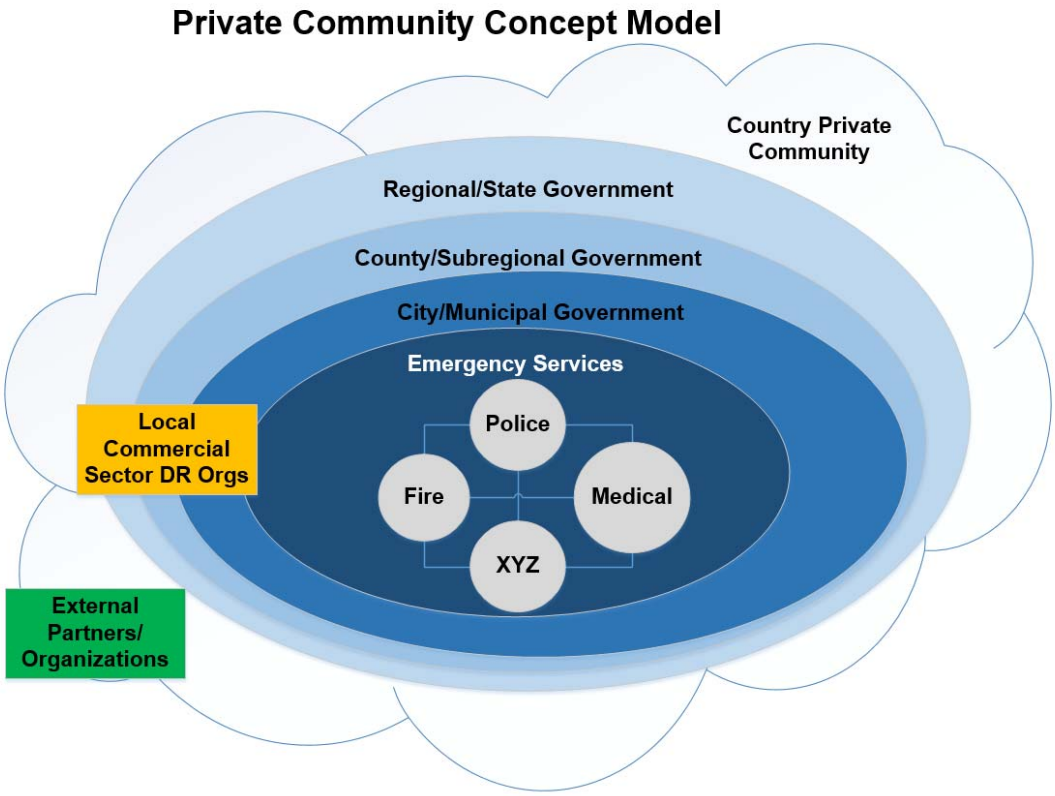


Figure 22. Private Community Relationship Model.

4. Private Community Application Interface

Some of the current web-based interfaces are extremely complicated and require significant time to learn how to use them effectively. The interface for DR missions should be highly intuitive. The user should not have to spend more than ten minutes learning the functionality of the interface. As such, some sort of instructional self-help and technical support options may be required. The following represent key functions of the interface:

1. Account creation
2. Interface command and control (C2)
3. Integration
4. Common operating picture
5. Disaster alert system

Figure 23 provides a visual (notional) representation of the DR interface.

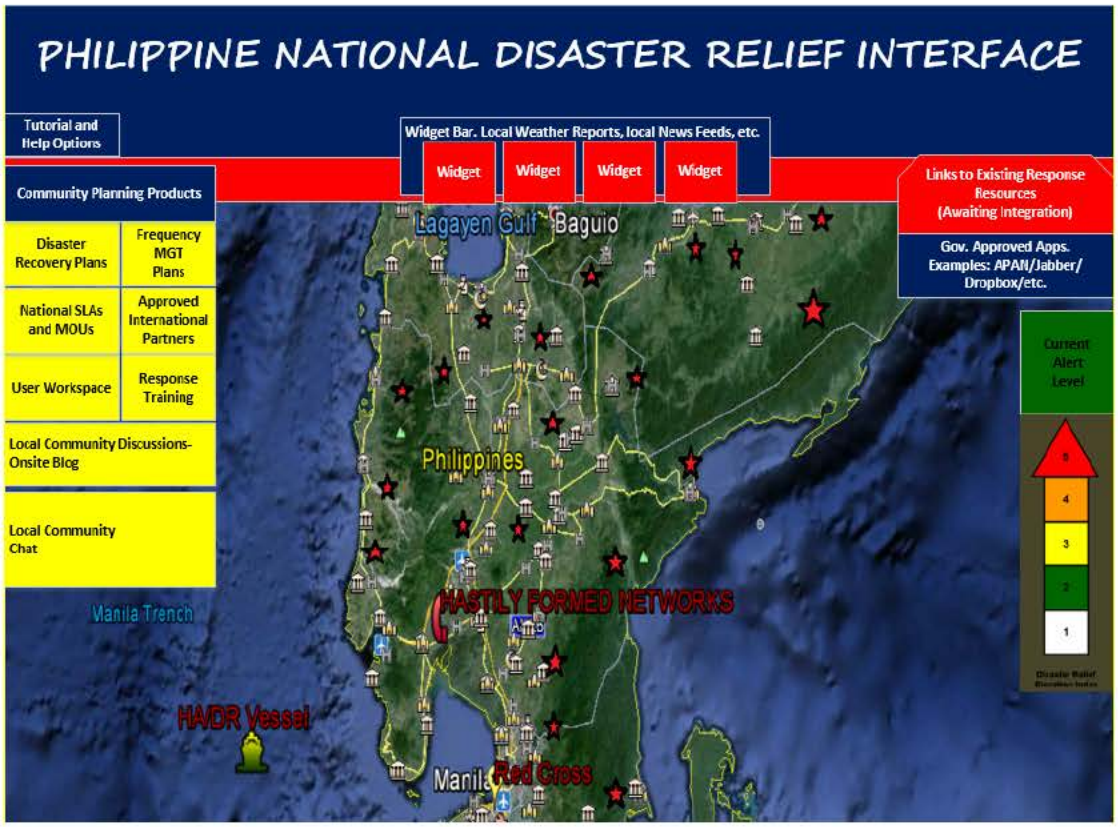


Figure 23. Example Private Community Interface.

a. Interface Account Creation

Account creation for private community interfaces is slightly different from traditional sites. The only way for a user to obtain access to an account within a private community is through organizational referral. Before the creation of the interface, the community owner (country government or organization) must designate individuals to serve as account managers. Account managers that are appointed should be working in a human resources or management role within the organization. This places the responsibility of user verification on the local governments. Accounts are restricted to government employees and critical disaster relief entities. Designated organization owners must approve or deny accounts outside the government. Each private organization may coordinate with the trusted organization to establish an account vetting system.

b. Interface Command and Control

The community manager or designated representatives dictate the functionality and tools of their interface. The trusted organization implements and manages the interface in accordance with community interface owner specifications. The private community owner (local government or organization manager) dictates the collaborative and organizational tools used for disaster response within its country. When external entities and partners elect to participate in the mission, they must use the designated tools indicated in the SLA of the affected country.

The community planning product section provides a space local to the interface where planning and collaboration can take place. The community products are only accessible within the community. The government or owner of the private community can dictate information shared with partners based on the SLA of each partner. The key buttons within the community planning section are DRPs and frequency management plan (FMP).

User tutorial and help options buttons are available within the interface. This feature allows the user to go through a ten-minute tutorial on using the interface and review the options available within the interface. Upon completion of the tutorial, the user has access to Frequently Asked Questions (FAQ) and technical support request sections. This section also contains contact information for an interface support section managed by the new organization.

The DRP and FMP sections are standard for each interface. The community owner can choose to upload their DRPs and FMPs to the site. This section also comes equipped with a DRP and FMP creation tutorial. In the event that the organization owner does not have a DRP of FMP, they can create the products using an automated process. Once the automated process is complete, the process generates a workflow process to allow for DRP and FMP approval process.

There are numerous additional features available within the community for planning and continuity. The government or community owner dictates the additional features available within the community planning section. The community planning section and tutorial sections are located on the upper left hand side of Figure 24.

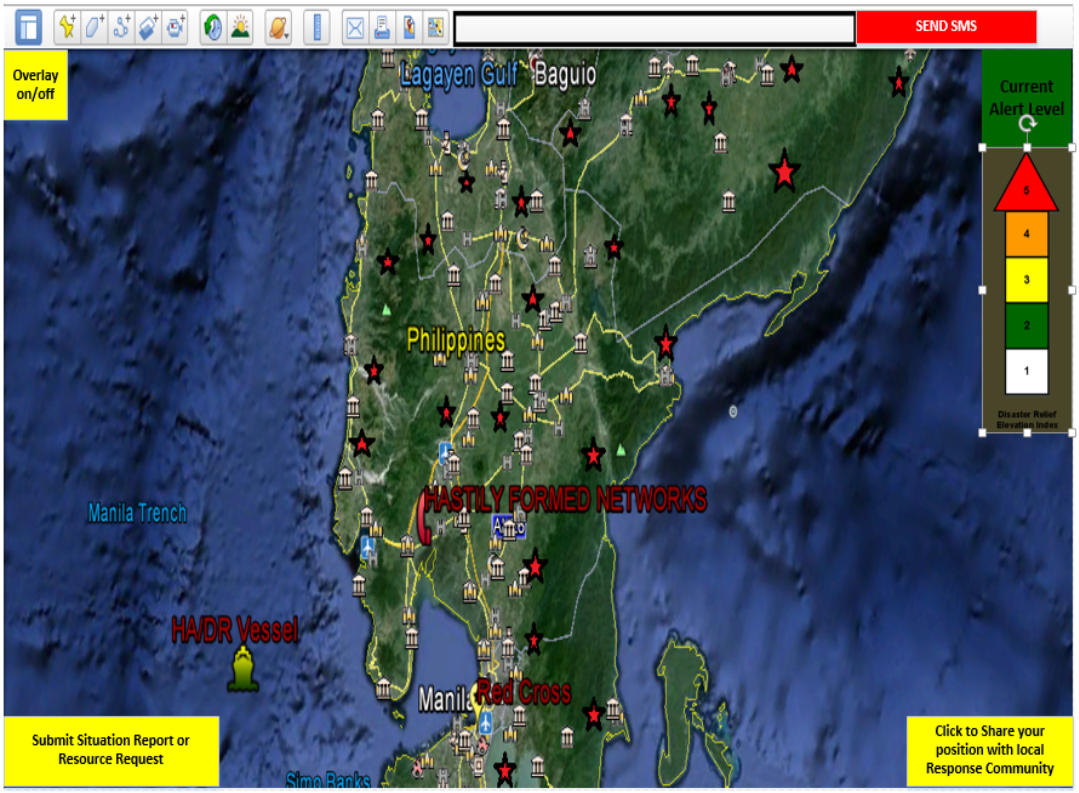


Figure 24. Mobile Application Interface.[205]

c. Integration with Existing 4C Products

Many organizations have developed inventive products for collaboration and communication for DR. With all of these tools available to DR mission teams, data becomes disparate and distributed among competing provider's solutions. Rather than creating a new tool, this model proposes an integration concept for collaboration and communications tools. This interface concept supports the use

205. Folsom, Eric and Brooks King, Private Community Concept Model, Naval Postgraduate School, February 2014.

of existing solutions for 4C. Integration of existing 4C solutions for governments and organizations occurs during the initial private community planning process. This allows DR users access to commonly used tools for DR missions within the common private community interface. Integration facilitates moving data to the private community when and if the community owner desires.

The integration concept includes developing an application repository. When governments and organizations require specific DR tools, the trusted organization must work with existing 4C providers to facilitate product integration. During the development of integration applications, users may require access to their preferred 4C products. Each user can add private links to preferred tools to the awaiting development container of the interface. Once the application is ready for use, the requesting user's organization receives notification, and it becomes available in the interface application repository. A repository structure also allows partner organizations to incorporate the use of designated tools as needed for DR missions.

In addition to integrating existing solutions, governments and organizations can integrate their existing traditional infrastructure with the interface. The trusted organization can work with each private community to provide a federated identity and single sign-on solution.[206]

d. Common Operational Picture

A common operational picture (COP) provides a means for the government and community to monitor the efforts of DR teams. The Pacific Disaster Center's (PDC) DisasterAware software provides the capability for real-time situation reporting; if internationally accepted, it could potentially serve as a viable COP solution provider. Unfortunately, the lack of trust and social complexity with the DR system has rendered international COP participation for

206. CA Technologies, "Federated Identity and Single Sign-On Using CA API Gateway," 2014, accessed 22 January 2015, http://www.ca.com/us/~/media/Files/whitepapers/federated-identity-and-single-sign-on-using-ca-api-gateway.pdf.

DR ineffective.[207] Instead of creating another COP solution, this thesis proposes an integration solution to COP.

As with most features in this interface concept, the owner of the private community dictates the mapping solution. This model supports map service provider neutrality. As long as the designated map provider has an application programming interface (API), the trusted organization can attempt to negotiate integration into the interface. The integration can ensure that data normalization is seamless to the user and the map datum is proliferated throughout the private community interface. Integration enables data normalization between the map provider and the integration interface. Once the integration occurs, government approved partner organizations have access to a common operating picture using their selected map provider.

An important step with the creation of this COP concept is to facilitate use of the interface in constrained bandwidth situations. Although 3G and 4G cellular technologies allow access to web-based interfaces via mobile phone, the cellular networks often become over-saturated when disasters occur. During Hurricane Ike in 2008, AT&T cellular service was flooded throughout Southwest Louisiana.[208] Because of the cellular congestion, AT&T implemented an automated message saying all circuits were currently busy.[209] In addition to diminished voice calls, SMS was also intermittent in the area.[210] Because of situations like Hurricane Ike, it is important to have other options for mobile 4C that do not rely on cellular service.

The common operational picture is very important for DR as it forms the basis for the mission. The ability to view the actual or projected position of a mission team is powerful. This functionality could mitigate some potential issues

207. Rebecca Goolsby Ph.D., Office of Naval Research, email message to author, 12 December 2014 (Appendix B).

208. Folsom, Eric M., personal experience, Fort Polk, LA, September 2008.

209. Ibid.

210. Ibid.

indicated in AARs and reports. If a DR mission team can view areas and other responders, they could potentially identify and deploy to areas with limited to no relief support. Teams deploying to an area in need of support could result in saving additional lives. The stars in Figure 25 indicate areas that need support; a DR team that possesses the resources needed could attempt to provide support to the entity. This could increase the productivity of individual mission teams as well as the collective relief effort.

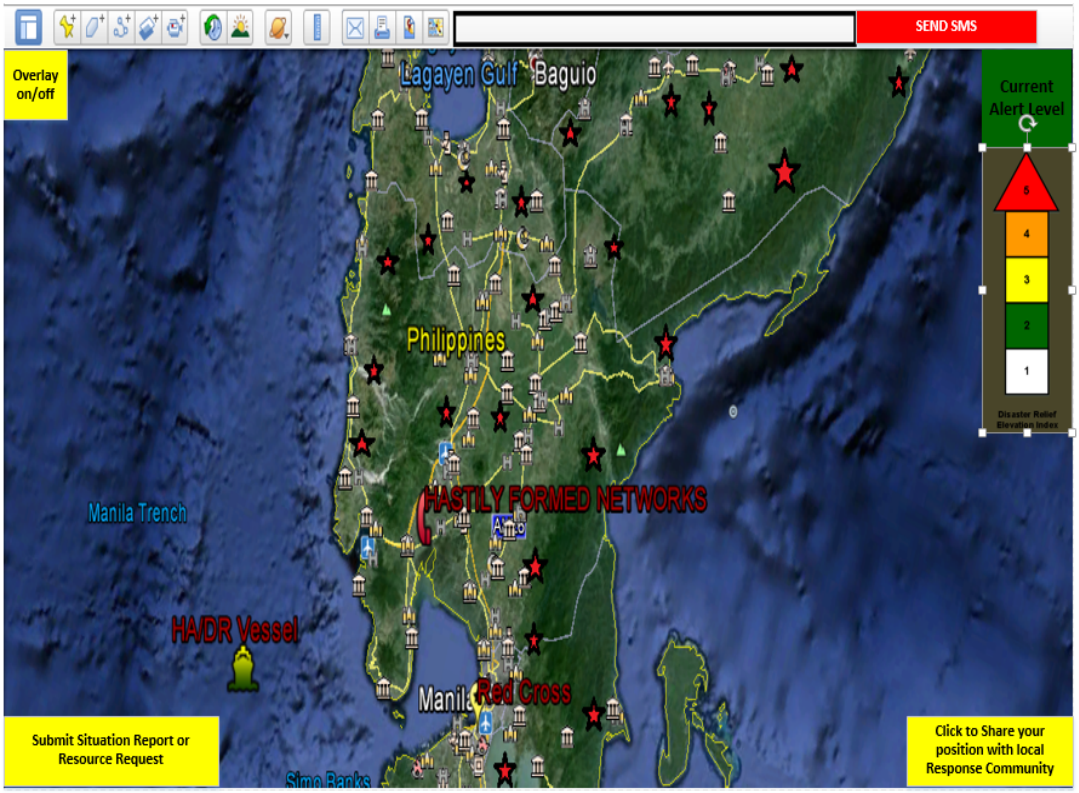


Figure 25. Mobile Application Interface.[211]

e. Disaster Alert System

At the current time, there is no internationally recognized DR alert system. However, the Common Alerting Protocol (CAP) is coming quite close to international acceptance. Without an internationally accepted alerting solution for

211. Folsom, Eric and Brooks King, Private Community Concept Model, Naval Postgraduate School, February 2014.

international DR missions, there is no way to establish a condition level for the relief effort. The interface provides a disaster alert matrix and condition elevation schema. The disaster relief elevation matrix in Appendix D provides a government managed alert system model for each private community.

The DR alert matrix places the responsibility of disaster response and disaster relief support on the local government. Each category has its respective authority levels and support categories. The example of a hypothetical situation below assumes that DRPs and CDRPs are established, that the government is using the interface, and that the U.S. Military serves as temporary C2 for the DR event.

A massive 9.0 earthquake wipes out the buildings and infrastructure of Cuba. The President and government leadership of Cuba is either dead or trapped beneath the rubble. There is no distinct leadership; chaos ensues.

In Santa Clara, one city official and several firefighters escaped from the building before it collapsed. The current disaster matrix status remains at level 1 of 5. After trying to contact higher government echelons, the official accesses the alert matrix to raise the level appropriately. Based on his assessment, the disaster level is elevated to level 5 of 5.

Private community partners and the U.S. government are automatically notified when the disaster level is raised. Based on Cuba's CDRP, the U.S. Military deploys and provides contingency C2 for the relief effort.

Although this is not a likely scenario for the model, the potential to have this effect is resident within the interface concept. Since the private community CDRP was in place for this scenario, no additional bureaucracy was required to deploy and provide DR. Having a contingency disaster relief plan in place will eliminate some of the confusion, chaos, and anarchy within the DR system.

5. Mobile Application Interface

The prolific nature of today's network technologies warrants provision of a platform non-specific integrated interface. Accessibility to the interface using mobile devices is paramount. Mobile devices represent an inexpensive alternative to large ICT solutions when cellular service is available.

In many of the disasters, cellular networks and critical communication infrastructure go down; the only access to communications is via satellite. Mobile Global Positioning System (GPS-based) ICTs are an option when cellular services are unavailable. GPS-based systems, such as Delorme, inReach, and SPOT allow the subscriber to send position information and a 160-character text message. Traditional web-based interfaces may not be accessible on GPS devices.

For mobile devices to communicate directly with the DR interface, the new organization must work with GPS ICT providers to develop a custom mobile application. Since the devices are GPS-based with onboard maps, viewing a private community COP would only require the transfer of metadata for reports and team positions.

The map portion of the interface provides normalized input and output for situational reports. A method of slimming down inputs for situational reporting allows only a unique ID field, GPS position field, and a details field consisting of no more than 160 characters. This reporting limitation may facilitate bi-directional traffic from mobile devices to the integrated mapping interfaces.

Incorporating mobile devices also supports an inexpensive prepositioning capability. Prepositioning mobile devices in critical locations, throughout countries or areas that experience frequent disasters, could significantly increase DR response quality. In some cases, this could reduce the time it takes to receive damage assessments from remote areas that have limited capability and funding. Within minutes after an earthquake occurs, or as the eye of the storm

passes over an area, a report generation is possible. Figure 26 provides an example of a potential mobile application interface.

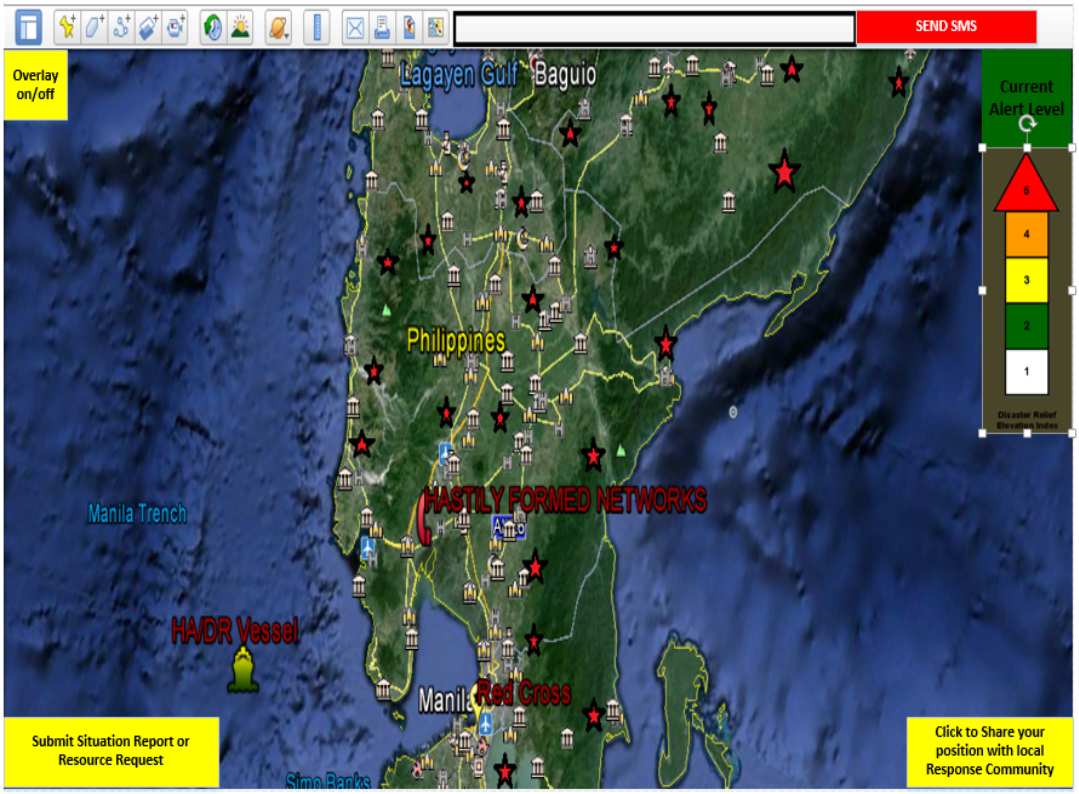


Figure 26. Mobile Application Interface.[212]

212. Folsom, Eric and Brooks King, Private Community Concept Model, Naval Postgraduate School, February 2014.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CYBERSECURITY

Large-scale, layered security mechanisms influence usability, functionality, and access to resources. This strategy proposes the development of a baseline security plan. A security plan specifies the system security requirements and the measures implemented to meet the requirements.[213] In addition, a security plan specifies responsibilities within the organization and defines acceptable systems usage.[214]

The primary purpose behind providing ICT capability is to facilitate communication between mission teams. Introducing security plans that occupy bandwidth in a bandwidth-limited environment may prove to be counter-productive. A communications strategy implemented without an overall security plan leaves DR mission teams vulnerable to cyber-attack.

Developing a security plan and implementing security mechanisms and measures within the DR system represents a technical and social challenge. The international community may not support unified security policies. Because of this, the security requirements and policies of each private community will differ significantly.

It is also a technical challenge because the model presented in this thesis is conceptual in nature. For this model, the trusted organization is responsible for security of data resident on private community interfaces. In addition, the organization is responsible for ensuring the data is bi-directionally secure from the IaaS systems to the private community users.

Because of societal differences and incomplete design specifications, a discussion of all security requirements and security controls is not possible. The

213. Marianne Swanson, Joan Hash and Pauline Bowen, *Guide For Developing Security Plans for Federal Information Systems*, National Institute of Standards and Technology Special Publication (NIST SP 800–18), Rev 1, February 2006.

214. Ibid.

security section discusses some general security considerations for common issues among disparate implementations.

A. INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

This security strategy supports a bring-your-own ICT (BYO ICT) concept. BYO ICT allows DR mission teams to procure communication capabilities that best support their organizational needs. ICTs function as 4C enablers and are primarily concerned with sending and receiving traffic. Since the focus of ICT is to facilitate 4C, one of the major concerns is securing data in transit to prevent adversary access to responder position and situation information.

Transport Layer Security (TLS) represents a simple solution for securing data-in-transit. TLS provides a reliable, secure connection for cryptographic key exchange and encryption of data-in-transit.[215] TLS provides confidentiality and message integrity through implementing symmetric, pre-shared keys.[216] It also allows the use of asymmetric cryptography for authentication.[217]

ICT mobile solutions present their own breadth of vulnerabilities. Mobile ICTs may consist of a combination of phones, tablets, PDAs, GPS devices, and items such as BRCK.[218] Due to the variety of systems, a feasible solution for securing data-in-transit for mobile ICTs is to develop a secure mobile application for each platform. The application requires user authentication and encryption for two-way transfer of situational information between the device and the integrated private community interface. Most financial mobile applications require single factor authentication but add extra single factor security to verify user identities. USAA federal savings bank adds personal identification numbers (PIN), security

215. Internet Engineering Task Force (IEFT), *TLS Protocol, ver. 1.0*, IEFT Request for Comments (RFC) 2246, January 1999.

216. William Stallings, *Data and Computer Communications*, ed.9 (Prentice Hall, New Jersey. 2011).

217. Internet Engineering Task Force (IEFT), *TLS Protocol, ver. 1.0*, IEFT Request for Comments (RFC) 2246, January 1999.

218. BRCK, “BRCK Specifications Page,” 2014, accessed 25 January 2015, http://www.brck.com/specification/.

questions, and phone number affiliation to match online personas with account holders. These techniques add additional security measures but still rely on single factor authentication techniques.[219] With mobile devices, multi-factor authentication may be the best option for ensuring confidentiality, integrity, availability, and authenticity (CIA-A).[220]

Additional considerations for mobile devices are physical access and protection of data-at-rest. Mobile devices are generally small and can be easily lost or stolen. If an adversary can obtain physical access to a mobile device, he or she can likely gain access to the resident data. Adding additional security layers, such as device access codes and drive level encryption would make it more difficult for adversaries to gain access to the device.

Some ICT platforms allow users to communicate using Wi-Fi and Bluetooth technologies. These technologies provide communications flexibility and represent an integral functionality for DR mission teams. Most Wi-Fi access points employed in these packages provide methods to protect data-in-transit using common encryption standards. Depending on when the device was developed, some ICTs rely on obsolete encryption standards.

The 9201 model BGAN in use for HFN relies on Wired Electronic Privacy (WEP) to protect data-in-transit over the local area network. The use of obsolete standards empowers adversaries with the capability to intercept and decrypt data-in-transit. DR mission teams need to be aware of encryption standards used in their packages and should replace legacy devices with an improved version when resident encryption standards become obsolete. As of 2010, it only takes three seconds to crack a 104-bit WEP key and sixty seconds to crack Wi-Fi Protected Access (WPA) using Temporal Key Integrity Protocol (TKIP)

219. Shon Harris, *All-In-One CISSP Exam Guide*, ed.4 (New York, NY: McGraw-Hill. 2008).

220. Ibid.

algorithm.[221, 222] As of 2013, the best wireless security standard available to the public is WPA2 Pre Shared Key (PSK) using Advanced Encryption Standard (AES) encryption.[223, 224] It is important to understand that WPA2 PSK requires administration and management. As a BYO ICT concept, private community owners are responsible for ensuring that approved ICT packages conform to industry encryption standards.

Some ICT platforms incorporate the use of the WiMAX (802.16) technology. WiMAX systems provide a broadband network connection over large distances using wireless line of site propagation (10–66 Ghz) or non-line of site (6–10 Ghz) using advanced modulation for mobile base station configuration.[225] WiMAX supports point-to-point, point-to-multipoint, multi-hop relay, and mobile configurations.[226] The system protects data-in-transit through use of security associations, X.509 digital certificates, and authorization keys to verify Base Stations (BS) and Subscriber Stations (SS).[227] Despite its enhanced security protection mechanisms, WiMAX is still vulnerable to RF jamming, base station impersonation, and eavesdropping. To reduce exposure to the adversary, DR teams should ensure that they use the highest available encryption standards.

---

221. Peter Sayer, "Researchers Crack WEP Wi-Fi Security in Record Time," IDG News Service, TechWorld, published 04 April 2010, accessed 23 February 2015, http://www.techworld.com/news/security/researchers-crack-wep-wifi-security-in-record-time-8456/.

222. Kevin Parrish, "WPA Encryption Cracked in One Minute," Toms Guide US, published 27 August 2009, accessed 22 January 2015, http://www.tomsguide.com/us/WPA-Cracked-Routers-Japanese-Scientists,news-4526.html.

223. Bradley Mitchell, "AES Versus TKIP for Wireless Encryption," AboutTech, accessed 22 February 2015, http://compnetworking.about.com/b/2008/08/21/aes-vs-tkip-for-wireless-encryption.htm.

224. Patrick Barker, "WPA2-PSK vs. WPA-PSK," Discussion Question, Microsoft Community Blog, published 13 September 2013, accessed 22 February 2015, http://answers.microsoft.com/en-us/windows/forum/windows_8-security/wpa2-psk-vs-wpa-psk/a014e1e1–5289–4f61–98b0-e9450824dbcf.

225. Karen Scarfone, Cyrus Tibbs, and Matthew Sexton, *Guide to Securing WiMAX Communications*, National Institute of Standards and Technology Special Publication 800–127(NIST SP 800–127), Computer Science Division (Gaithersburg, MD. September 2010).

226. Ibid.

227. Ibid.

Furthermore, process and policy based security controls can help to counter additional vulnerabilities.[228]

The information contained in the previous section only discusses security vulnerabilities identified during previous DR after action reports. There are other vulnerabilities specific to ICT implementation that should be researched and addressed. It is also important to understand that as ICT capability and functionality increases, additional vulnerabilities may arise.

B. RESPONSIBILITY AND INTERFACE DESIGN IMPLICATIONS

Many organizations and governments have existing security policies and security controls that help protect their current enterprise solution. The custom managed interface supports existing policies and security controls while allowing integration into the network using a federated identity management solution.

1. Service Agreement and Joint Responsibilities

The trusted organization serves as an external service provider to all organization owners. The customers (private community owners) subscribe to services from the external service provider (the trusted organization) that fall "outside of the traditional security authorization boundaries (physical or logical) established by the customer organization."[229] Customers or stakeholders who desire access to the integrated interface work with the trusted organization to develop a custom private community for each government and DR organization.

A service agreement (SA) is created between the trusted organization and private community owners to identify the level of service and indicate specific roles and responsibilities. The SA outlines and specifies general security policies and controls for the community. The SA serves as a baseline for the organization and assures the community owner that their data is protected. The policies and

228. Ibid.

229. U.S. Department of Commerce, Security and Privacy Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology Special Publication 800–53 (NIST SP800–53), Gaithersburg, MD. April 2013, updated 22 January 2015.

security controls, specified in the provider SA, apply to the entire community. The mutually approved SA provides the specifications for creating the detailed design document.

The detailed design document establishes guidelines for each community, map provider of choice, storage requirements, and existing 4C solutions that require integration. The trusted organization negotiates with existing 4C providers to provide integration support for the private community owner. This custom packaged interface allows the DR community owner to continue to use existing 4C solutions while accessing the products in a private community common interface.

Moving services to the cloud has many benefits, but significant additional vulnerabilities arise as a result. To protect community and user information, extensive time and thought must take place to deal with privacy and security issues.[230] The trusted organization must also ensure that the IaaS service provider provides detailed delineation of security boundaries. Applications are developed and tested prior to migrating integration applications to the repository.

2. Trusted Organization Limitations

The trusted organization is not responsible for security of the information that resides on the integrated solution provider's sites. Many DR organizations already use cloud based storage and collaboration tools. As such, the trusted organization is only responsible for the data resident within each private community within the limitations of the SA and detailed design document. The trusted organization is never responsible for verification of user identities. Prior to the creation of the private community interface, proposed community owners would need to have identity verification measures in place. Most governments and organizations have procedures to properly vet identities for their employees. The governments and organizations would dictate authorized users within their

230. Jansen Wayne and Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology Special Publication (NIST SP800–144) (Gaithersburg, MD, December 2011).

organization. The private community owner is responsible for vetting users and account management after the interface comes online. Private community owners negotiate with the trusted organization to identify what constitutes acceptable use for interface users.

The trusted organization cannot control individual user machines on an organization's corporate network, nor can they control a DR team's ICT implementation. Security, from the end user to the interface, represents the largest vulnerability to this concept model.

3. Final Notes for Private Community and Interface Security

The trusted organization must take a proactive approach to ensure the confidentiality and integrity of system data. To prevent potential future attacks, the organization must monitor for malicious activity, from the IaaS to the interface user, in order to identify and take corrective actions. They must clearly delineate between non-partner private communities to prevent unauthorized disclosure or access to customer information. To remain trusted, the organization must secure the data but remain open and transparent to private community subscribers. Allowing designated private community administrators access to a security dashboard may establish some level of transparency and trust. The trusted organization must ensure that security controls are in place to protect and prevent unauthorized access to private community interfaces.

The concepts in this thesis only discuss a few fundamental security measures but have left many others for future work. As such, the concepts should be fully developed based on a Systems Thinking perspective. Further research and development of the concepts discussed will enable the creation of a comprehensive security solution that fits within the DR system.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

Natural disasters can affect all inhabitants of this planet. As such, stakeholders should work together to provide effective international disaster relief (DR) capabilities that reduce the duration of relief mission support and increase victim survival rates.

International DR efforts represent a socially complex wicked problem. Because of DR's wicked nature, previous solutions developed to resolve issues fail to achieve their intended impact. Previous solutions have addressed aspects of communication, coordination, cooperation, and collaboration (4C) capability. However, they have only addressed symptoms of the system-level problem. As such, the solutions resulted in information overload, information disparity, bandwidth saturation, and a disjointed response effort. To develop a solution that would succeed, planners must better understand the DR system and its related components.

The Systems Thinking process represents a model where planners can attain a better understanding of the DR system and its interdependencies. In its current state, the DR system is destined to remain in an uncompromising vicious cycle. Using the Systems Thinking process, the variables that affect the system are as follows: scope of the disaster, number of DR mission teams, social complexity, anarchy, response quality, and stress.

The variables anarchy and social complexity negatively impact the system. Because of its impact significance, anarchy is the dominant system-level problem variable. Reducing system-level anarchy will significantly improve response quality, reduce overall stress, and potentially reduce the scope of the disaster.

Previous solutions for DR 4C increased capability, provided organization, and enabled collaboration. Because these solutions addressed symptoms of the problem, it is possible, that combining these solutions could lead to the

development of a valid system-level solution. Based on the Systems Thinking process findings, the injection point is the number of DR mission teams; and the 4C variables form the balancing loop. To truly reduce system-level anarchy, all four variables of the balancing loop must function synergistically. An internationally accepted communication strategy designed to support open and transparent 4C provides a means to reduce information anarchy. Reducing information anarchy can potentially reduce the impact significance of DR system-level anarchy.

The communication strategy concept proposed involves creating a trusted organization to manage cloud based private community interfaces, support the BYO ICT concept, and provide integration support for existing 4C solutions. Establishing a trusted organization to manage the interface could reduce existing DR based biases and creates a neutral entity for partner-to-partner negotiations. Establishing a completely neutral entity is not likely; however, a new organization's lack of an existing DR history or reputation may be sufficient to obtain international acceptance.

Due to the vast number of stakeholders, there is no way to dictate an ideal ICT solution for DR mission teams. Instead, the communication strategy supports the bring-your-own (BYO) ICT concept and provides some potential solution model examples based on the metrics of deployment, cost, and security. The three solutions are ICT Mobile, ICT Lite, and ICT Standard.

ICT Mobile is highly deployable and inexpensive but requires coordination with vendors to develop acceptable encryption for data-in-transit. ICT Mobile is designed for single person use or as designated as a contingency communications solution.

ICT Lite is highly deployable, significantly more expensive, and generally comes with features to secure data-in-transit. DR mission teams should ensure that their ICT Lite system does not rely on obsolete encryption standards. ICT

Lite provides service for up to eleven personnel using a minimum of one Wi-Fi access point.

ICT Standard is deployable, very expensive, and can come with additional security appliances. ICT Standard provides the most flexibility, but package cost is relative to desired service plan and organizational requirements.

The second part of the strategy proposes implementation of a cloud-based model that supports application development. The trusted organization provides integration application programming and community interface development in a PaaS service and hybrid deployment model. The DR stakeholders obtain access to the offered interface from the trusted organization using SaaS service and hybrid deployment model. The model allows the organization to focus on providing quality IT and integration services, while the DR stakeholders can develop operational content and service level agreements (SLAs) with desired partners. This model also supports and encourages the creation of disaster response plans (DRPs), collaboration with partners to create contingency disaster response plans (CDRPs), and establishing frequency management plans for communities and selected partners.

When DR teams initially deploy to the disaster area, their primary objective is to coordinate with local government to determine where help is required. This officially identifies local government as C2 for the relief effort. Unfortunately, this does not always occur. The second part of the strategy supports identifying local government as the primary communications coordinator and C2 through the creation of private community interfaces for each country, government, and organization. For teams to participate in DR within the affected country, they must obtain approval from local government and agree to use the local government's interface tools. Private community interfaces allow the local government, or its designated C2 contingency, to guide DR operations from start to finish. The private community and C2 concept add structure, organization, and reduce both information and general anarchy with the DR system. Since participating teams must use the designated DR tools, standing DRPs, CDRPs,

and frequency management plans of the respective private community interface, the impact of information fragmentation is negligible.

The third part of the strategy involves creating a mobile application interface. The principle behind the mobile application is to provide similar capabilities to mobile users using bandwidth-restricted devices. The mobile interface proposes creating an application that would allow information to be sent and received while requiring minimal bandwidth. The mobile application requires locally resident device maps. The only traffic sent or received is a unique identification code, location information, and a text message of up to 160 characters. This limitation will allow use of existing GPS device functionality while facilitating participation in the DR event using the local government's private community interface in near real time. The use of GPS for communications also negates some of the bandwidth saturation issues experienced during DR missions.

The final part of this strategy discussed the security considerations. The author has no control over what ICT solution or end devices each DR team or organization uses. Without an understanding of what is on the network, it is impossible to develop a sound security plan. Instead of proposing a security plan, this strategy briefly discusses the security concerns of the design and prototypes explained. The design-specific concerns cover identity verification, account management, encryption of data for the community interface, encryption standards used for ICTs, and private community roles and responsibilities.

This thesis examined disaster relief AARs, assessed DR as a system, discovered a system-level injection point, developed a strategy that considered all components of the system, and introduced strategy concepts that could result in significantly improving the current DR system.

A. LIMITATIONS AND IMPLICATIONS

The concepts discussed in Chapter IV and V address key features for consideration when developing an international communications strategy for DR.

It does not constitute a full solution for the problem within the DR system. Disregarding the concepts discussed in Chapter IV and V may result in failure of all subsequent solutions to address the DR system-level problem. Further research and development is required to ensure that the strategy obtains international acceptance and successfully reduces system-level anarchy without significant social implications. In addition, further deliberation and development of these concepts should warrant international DR stakeholder participation.

B. TOPICS FOR FURTHER RESEARCH

From the author's point of view, the proposed communication strategy represents a realistic model using existing technology. Possible future works include the following areas of research.

Hastily Formed Networks need to incorporate a layered approach to security. This approach should introduce mechanisms that account for all layers of the OSI or TCPIP models. Upgrading hardware that currently relies on obsolete encryption standards, incorporating wireless intrusion detection (WIDS), wireless intrusion prevention (WIPS), network security policies, and acceptable use policies are all requisites sound security posture. Researchers should ensure that all solutions developed are derived using a systems perspective. Doing this ensures that security features implemented do not impair the NPS HFN team's ability to participate in international 4C.

Another topic for further research is creating the detailed design document for the private community interface concept that would result in the use of cutting-edge technology. Although this thesis touches on some of the major issues with DR 4C, it does not provide a full solution to the problems within the DR system.

The creation of a third-party trusted organization constitutes another area requiring further research. Applicable areas of interest are organization or business type, future cloud models, organization diversity, and alternate sources for funding (social innovation funds). Any solution proposed should lean heavily on understanding the social implications of the DR system.

Development of a model that supports two-way communications with a single integration interface is another topic for further research. Some of the valid areas of research are as follows: integration applications repository, development of mobile applications for GPS devices, development of APIs for existing 4C vendors, and common operational picture data normalization.

APPENDIX A

Appendix A provides detailed steps for the Systems Thinking process. The Systems Thinking process reviewed in Chapter III, only introduces key products of the process. All steps and work done to assess the DR system are included in this Appendix.

A. SYSTEMS THINKING PROCESS DRAFT PRODUCTS

Initial Narrative: The anarchy created in the aftermath of a natural disaster is uncompromising. The lack of international legislation and designated C2, result in increasing the level of anarchy associated with disaster relief (DR).[231]

DR mission teams deploy to provide the assistance and resources for disaster relief to the local first responders, governments, and victims.[232] When a disaster occurs, there is extensive damage to the infrastructure of cities, homes, and the environment. Many times the debris and damage to infrastructure and roads make it difficult for responders to move to locations for 4C participation. Social complexity and anarchy also play a major role in forming barriers to effective 4C.

As DR mission teams arrive, the social complexity of the relief effort increases, reducing the desire and capability for teams to participate effectively in 4C activities. This lack of effective communication creates a sense of chaos, in which these teams attempt to correct through assuming command of the relief effort in their areas.[233] The individual efforts of the teams and assumption of

231. Larry Wentz, "Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010," Center for Technology and National Security (National Defense University, Washington, DC, 08 August 2010).

232. Brian Steckler, Hastily Formed Networks in Haiti, "Haiti Earthquake After Action Report and Lessons Learned (AAR/LL)" (Naval Postgraduate School, Monterey, CA., 8 September 2010).

233. Larry Wentz, "Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010," Center for Technology and National Security (National Defense University, Washington, DC, 08 August 2010).

command, limits the scope of the individual team's response and decreases the need for 4C between the participating teams. This, in turn, leaves areas that need support without aid for a longer period, resulting in preventable victim injuries, deaths, and destruction.

Table 6. Identification, Consolidation and Elimination Steps.

Identification	**Consolidation**	**Elimination**
Disaster/Catastrophe	Catastrophe Scope of the Disaster	Scope of the Disaster
Response	~~Response Capability~~ Number of ~~HA/DR~~ Teams	Number of DR mission teams
Communication	Communication	Response Quality
Coordination	Coordination	Anarchy
Collaboration	Collaboration	Social Complexity
Information Anarchy	Information Anarchy	Stress
Capability	Capability	
Shortfalls	Shortfalls	
Social Complexity	Social Complexity	
Security	Security	
Stability	Stability	
Victim Survivability	Victim Survivability	
Damage	Damage	
Relief/Aid provided	Relief/Aid provided	
Response Quality	Response Quality	
Stress	Stress	

Table 7. The Redefined Variables for Disaster Relief.

Variables	Redefining Variables
Scope of the Disaster	The degree of damage and level of impact that the physical and emotional damage have on the victims of the disaster. The actions of all stakeholders and victims affect the speed and efficiency of recovery operations.
Number of DR Mission Teams	Contingent upon severity of incident. The number of DR mission teams and capability required, in order to, facilitate an efficient and effective relief.
Response Quality	The overall quality of service provided by the mission teams combined.
Anarchy	Ultimate state of disorder, uncertainty, instability, insecurity, and identification of leadership.
Social Complexity	Humans tend to react in a certain manner based on their individual experiences, beliefs, morals, and values. These reactions are also based upon the norms, values, and belief systems of their country, state, city, and origin.
Stress	Level of stress associated with DR. This includes all stakeholders.

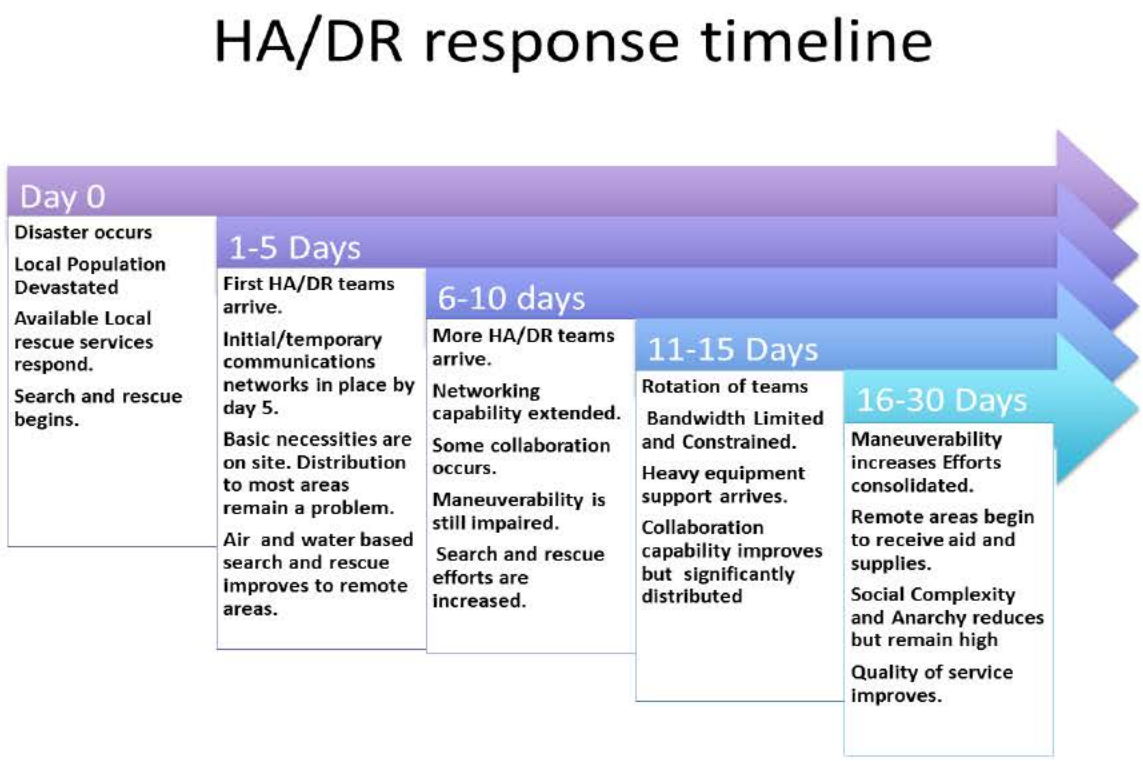


Figure 27. Timeline for Disaster Relief Missions.

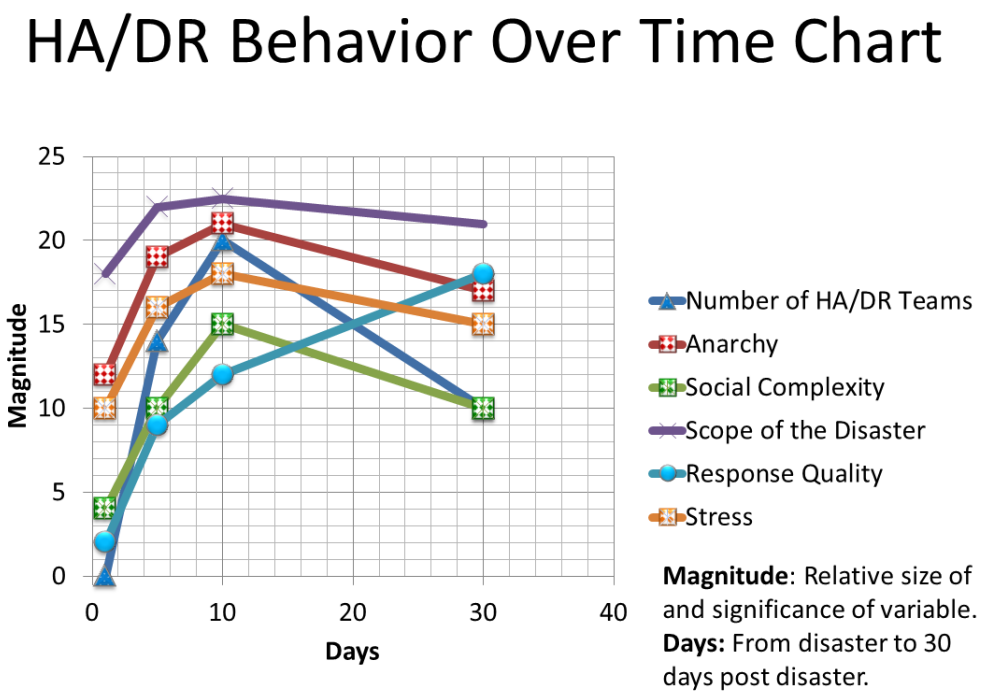


Figure 28. Disaster Relief Variable Relationship Over Time.

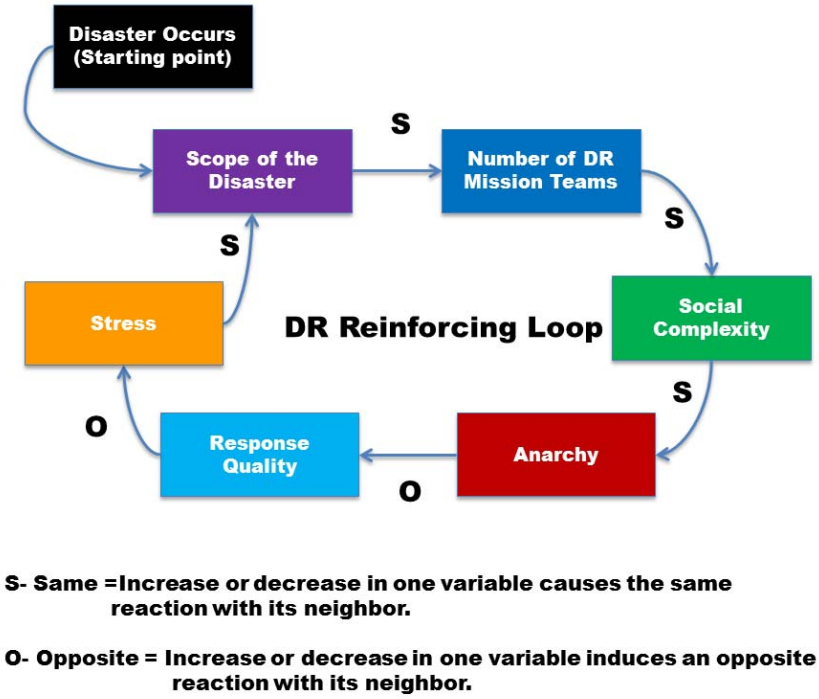


Figure 29. The Initial Causal Loop Diagram.

Table 8. The Balancing Loop Variables for Disaster Relief.

Balancing Variables	Definitions
Communications	The communications variable encompasses all forms of communication. This includes verbal, written, signaled, and electronic communication methods.
Coordination	The coordination variable encompasses, organizing efforts between disparate groups, in preparation for participation in an activity. Coordination works to prevent individual or group actions from interfering with the actions of other individuals and groups.
Cooperation	Cooperation encompasses coordination on a larger scale and occurs when organizations work together for a common beneficial outcome.
Collaboration	Collaboration encompasses the act of organizations working together and sharing information in order to generate a product or system. The product or system modifies, improves, or changes an existing system or process. Collaboration can also facilitate the creation of a new system.

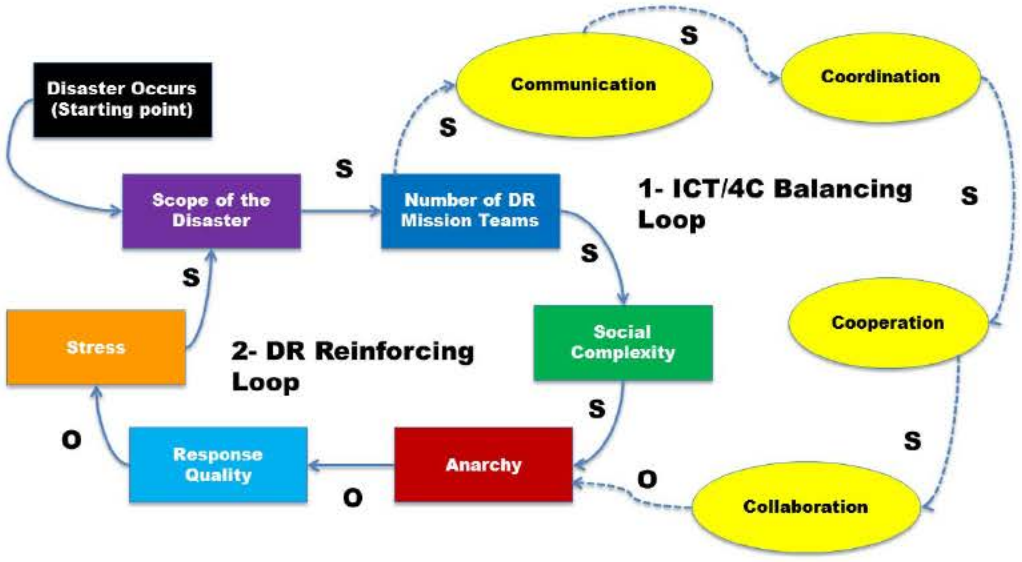


Figure 30. Final Disaster Relief Causal Loop Diagram.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

Appendix B contains the Rapid Technology Assessment Team executive summary. It provides an overview of the specifics related to RTAT.

Rapid Technology Assessment Teams (RTAT)
Executive Summary
25 October 2012

Overview
Information and communication technology (ICT) and power sectors are critical to the response after major disasters. Currently existing, post disaster assessments focus on areas other than ICT, power and Information Sharing. A rapid assessment of the ICT status will enable the host nation and the International humanitarian community to provide a targeted allocation of resources and result in a reduction of gaps and duplication of effort. The Rapid Technology Assessment Teams (RTAT) concept seeks to provide a pool of multidisciplinary experts who will rapidly deploy to the disaster zone to provide this information. The RTAT concept is supported by many organizations and individuals within the ICT disaster response community and is in the process of obtaining further funding. A crucial part of the development of the initiative is to gather support for the adoption of the concept by key disaster prone countries. Their involvement will enable RTAT to tailor responses based on specific country needs and to ensure that processes and operations will be as effective as possible.

The Problem:
The first hours and days after the onset of major global disasters are typically fraught with chaos and lack of situational awareness. While there are existing disaster assessment teams from major organizations that deploy to such events, these teams primarily focus on sector specialty areas other than ICT and Information Sharing. The ICT sector is critically important as it enables and supports all others.

Arrival of the global response community usually brings a welcome and powerful ICT capacity, but sometimes their arrival and the accompanying ICT equipment and capabilities do not link effectively with the host nations ICT or each other. This means that the effectiveness of the combined available resources is not maximized, leading to gaps and duplication.

Additionally, sometimes the host country has not requested international assistance after a disaster. In this case, the disasters have often been managed internally with requests only made for specific assistance, which can cause the host nation's resources to be stretched and unable to provide an accurate assessment of ICT and power needs. Complete ICT information is critical to

obtaining targeted support that will enable the response, business recovery, and minimize the effects of the disaster on the population.

Specific problems include:

In the immediate aftermath of a major disaster, there is often a gap in the knowledge of ICT infrastructure and a lack of communication between the International Humanitarian Community (IHC) and the affected state's national infrastructure.

What Exists Now:

There are teams that currently perform some very basic ICT assessment functions. Some of these teams are on standby to deploy rapidly in 12 -24 hours.

The United Nations Disaster Assessment and Coordination (UNDAC) international emergency response system, whose core mandates are assessment, coordination, and information management to assist the UN and governments in an emergency.

The Emergency Telecommunications Cluster (ETC)

The International Federation of Red Cross/Red Crescent (IFRC) First Assessment and Coordination Teams (FACT)

ICT based NGO's such as NetHope and TSF have some assessment responsibilities.

The Requirement:

The proposed solution would create the ability to rapidly deploy small, nimble, multi-organizational, multi-national integrated assessment teams of specialists in key ICT areas such as wireless data communications, voice communications, radio technologies, power, information sharing, social networking, etc. The real niche this program represents is that the teams can be made up of experts from a variety of different organizations such as industry, UN, NGO, academia, International Organizations, affected nation government/military, and international governments/militaries.

Once a comprehensive overview of the ICT situation has been established, a priority list of ICT needs can be drawn up in coordination with the host nation.

The RTAT teams can also be requested to provide specific ICT disaster assessments in the event that full international assistance has not been requested by the host nation.

The Teams Will Provide:

Field data containing both host nation and IHC information as well as communications technology and power needs and capabilities.

- Quality assessment of this information by experts and the distribution of *reliable and trusted* information.

This Initiative does not seek to duplicate any existing process but to reinforce and ena*ble the existing internationally* accepted processes by meeting a need that is recognized but that is not currently being effectively met. By concentrating on human interfaces and not technology, the team of highly trained inter-organizational personnel will identify and find answers to specific questions, compile a common operations picture and link with the host nation and the IHC enabling fast early recovery.

Specific requirements or capabilities include:
Having the ability to quickly deploy (within 24 hours)
Having direct links to local industry and government
The ability to stay in the disaster zone 1–2 weeks, then reassess need to remain longer or to rotate in new teams
The team having access to ICT expertise across the functional spectrum (ISP, cellular, data networks, power, etc.) with both the international technical community as well as local/national citizen experts
Understanding the need to work in close collaboration with existing teams on the ground

Team Makeup:

Ideally, these small teams of experts would be composed of 1–2 representatives from each of the following organization types: UN, NGOs, International Government Organizations IGOs, academia, industry, military, and government agencies from around the world. The formal/legal/business organizational makeup of the overall program and teams themselves would be determined by the founding member organizations.
The leadership of the teams should be:
Team Leader (from either the global or the regional technical community)
National affected state Member (such as National Disaster Management Agency, Ministry of Communications or equivalent affiliated organizations)
We still need to determine:
Skill sets, qualifications, and exact number of people to make up each team
Current thinking is to have government and/or industry experts from the ISP industry, the GSM/other cellular/landline industry, the power infrastructure industry, the wireless broadband industry, and the satellite communications industry.

Teams Readiness Status:

Small teams of qualified/trained experts from across the ICT spectrum are on 24X7 stand-by to deploy as soon as possible but likely for 1–2 weeks in shifts.
We believe that before deploying to a specific disaster zone there should be a BASELINE ICT/Info Sharing assessment capability in place. These assessments should be accomplished well ahead of time in each country prone to regular disasters. Such assessments could be done by RTAT supporting entities such as industry and academia. The benefits for such assessments, which would be provided to the host nation government, would go well beyond the RTAT concept and be able to point out potential general ICT vulnerabilities and resilience gaps to all concerned parties.

Team Locations:

RTAT teams would be stationed at key locations around the world, perhaps modeled after the UN Disaster Assessment and Coordination Teams program, or possibly as associate members of NetHope, the UN Emergency Telecommunications Cluster (ETC Cluster) or other similar teams. The host nation, UN agencies such as OCHA, WPF, or a regional entity such as ASEAN could call on these teams.

Timeline of RTAT Concept Development:
In late 2011, we began work on a process of developing the concept, identifying founding member organizations, outlining team member qualifications forming the teams, training and exercising these teams, and iteratively refining the program. We believe that if a real-world disaster event happens any time in the near term future, and if the teams have been identified and the roles, responsibilities and operating procedures are sufficiently advanced, then there could be an opportunity to "jump start" the entire process by deploying to that real -world event. Caution of course would be needed to ensure this would not hinder but rather help the overall response efforts.

Organizations That Have Helped Develop the RTAT Concept:
UN/NGO Community:
- UN (UN-OCHA)
- UN (UN-World Food Program/ FITTEST)
- UN (Emergency Telecommunications Cluster (ETC))
- NetHope
- Demining NGO community
- Telecoms Sans Frontieres
-New Zealand Red Cross
- InSTEDD
- CrisisMappers.Net

Industry:
- Cisco Systems
- Microsoft
- Global VSAT Forum
- Delorme
- Inmarsat Government Services, US, Inc.
- Oceus Networks
-MEDWEB

Academia:
- Naval Postgraduate School (US)
- University of Texas
- San Diego State University
- National Defense University (US)

Government/Military Community:
- U.S. Department of Defense
- Pacific Disaster Center
-Japan Resiliency Initiative
- International Association of Emergency Managers (IAEM)

Point of Contact:
Brian Steckler, U.S. Naval Postgraduate School, Monterey CA USA
Cell: 831.402.1584 - Work: 831.656.3837 - steckler@nps.edu

APPENDIX C

Appendix C contains the digital messages referenced in the body of the thesis. The email messages contained in this appendix are to provide validity to the claimed quotations in the body of the thesis.

RE: A quick Question about satellite bandwidth saturation

Lonnie Wilson

Sent: Friday, December 12, 2014 11:27 AM

To: Eric Folsom

Cc: Brooks King

Eric,

"The issues that HA/DR has with bandwidth saturation occurred when lots of people with ICTs moved to the same location. I assume it is because they are all on the same frequency band and the subscribers set BW does not allow for that much congestion in the same area."

1. Digital BW (in bps) is the fundamental limitation for any Communication System in a specific Frequency Band.
2. The Digital BW is assigned / utilized by the users; and when user demands / requirements exceed the Digital BW capability then saturation occurs.

"As I was looking through some stuff I found a neat device called Delorme inReach Extreme. The device has the capability to send two-way text messages and location. The problem I am having issues with is that the center frequency range is GPS frequencies L-band 1100–1500 Mhz."

Key question: Does inReach rely on the same satellites for its GPS and communication capabilities?

No, the inReach GPS and satellite communications components rely on different sets of satellites. The GPS component relies on the Global Positioning System, maintained by the U.S. government. inReach Communication capabilities rely on the Iridium satellite network.

The inReach Extreme product uses the Iridium Global Satellite System. Iridium Communication between satellites and handsets is done using a TDMA and FDMA based system using L-band spectrum between 1,616 and 1,626.5 MHz.

Iridium Communication System's transmissions do not interfere with GPS unit operations.

However, inReach Communication units have very low Digital BW capabilities. Certainly, messages are limited to 160 characters per message. I do not think this Digital BW is sufficient for this mission.

"The data it would send and receive would be minimal, however, because BGAN (the primary device HA/DR teams use for connectivity) operates on 1.5 - 1.6605 Ghz, I feel like the GPS frequencies could potentially become congested due to noise."

As stated above, GPS performance should not be degraded with these units.

"… however, because BGAN (the primary device HA/DR teams use for connectivity) operates on 1.5 - 1.6605 Ghz …"

The BGAN is a global satellite Internet network with telephony using portable terminals. The network is provided by Inmarsat Satellite Communication System and uses three geostationary satellites called I-4 to provide almost global coverage.
From Wikipedia, Broadband Global Area Network for use on land. BGAN benefits from the new I-4 satellites to offer a shared-channel IP packet-switched service of up to 492 kbits / second (uplink and downlink speeds may differ and depend on terminal model) and a streaming-IP service from 32 up to X-Stream data rate (services depend on terminal model). X-Stream delivers the fastest, on demand streaming data rates from a minimum of 384 kbits / second up to around 450 kbits / second. Most terminals also offer circuit-switched Mobile ISDN services at 64 kbits/s and even low speed (4.8 kbits/s) voice etc., services. BGAN service is available globally on all I4 satellites.

Inmarsat Communication does not interfere with GPS systems.

For the Inmarsat I-4 implementation, these Digital BWs may not be sufficient for potentially large missions that you might be considering.

I suggest you consider: The Inmarsat I-5 Ka-Band Global Xpress Network!

Inmarsat I-5 satellites are used in the new Inmarsat Ka-band Global Xpress network. This network delivers high-speed mobile and fixed broadband services around the world at speeds of up to 50 Mbps. This Digital BW should be sufficient for the mission.

Lonnie A. Wilson, PhD.

APPENDIX D

Appendix D contains figures from the text that did not legibly fit within the normal dimensions of a standard figure.

Alternate Power Generation Comparison Chart:[234][235]

ALT Power Attributes	Generators	Inverters	Hybrid Devices	PV Solar	Wind	Fuel Cells	Lithum Ion Batteries	Ideal Solution
Compact/Light Weight								
Maintenance Free								
Flexibility								
Mobility								
Local Resiliance								
Indoor Use								
Low Noise								
All-Weather Operation				Sunny Only	Windy Only			
Integration with Renewables				N/A	N/A			
High Power Output								
Cost								
Critical Dependancy - Fuel								
	Good/Desirable	Not As Good	Poor					

Attributes	Definition
Compact/ Light Weight	System is small and easily carried in large quantities.
Maintenance free	System does not require additional maintenance processes or procedures. Operates independently without requiring petroleum products.
Flexibility	System has the capability to support power for critical operations while simultaneously providing charging functions for other devices. System supports power sensitive operational equipment where down time can result in loss of life or critical communications.
Mobility	System is commercial airline transportable in large numbers.
Local Resilience	System can draw power from any available power source commonly found in disaster areas.
Indoor Operation	System does not require ventilation and noise level allows indoor operation.
All-Weather Operation	System does not require specific weather patterns for continuous effective operation.
Integration with Renewables	System allows the use of alternate power sources to support continuous operation.
High Power Output	System can output enough power to support all ICT capabilities.
Cost	Total Cost of Procurement.
Critical Dependancy - Fuel	Requires fuel for operation.

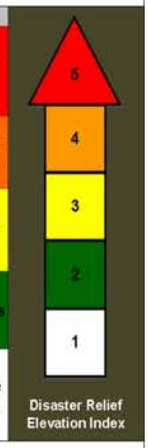
234. Brooks King, Team Alternate Power Generation Comparison, phone conversations, 10–29 January 2015.

235. Brian Steckler, Team Alternate Power Generation Comparison, personal correspondence, 10–29 January 2015.

Disaster Relief Elevation Matrix:

Disaster Relief Elevation Matrix	*City/Municipal Emergency Services Down	*County/Subregional Government Down	*State/Regional Emergency Services Down	*Country Emergency Services Down	All Emergency Services Down
*City/Municipal Government Down	1	2	2	2	3
*County/Subregional Government Down	2	2	3	3	3
*State/Regional Government Down	2	3	4	4	4
*Country Government Down	2	3	4	5	5
All Government Down	3	3	4	5	5

Level	Severity	Elevation Level	Support level Authority	Support Categories
5	CATASTROPHIC	International	Any surviving Government or Emergency Services Representative	Initiate National Response Plan and integrate with partners
4	EXTREME	*Country	Highest Ranked Country Government Official	Initiate National Response Plan and alert International Partners.
3	EXTENSIVE	*State/Regional	State Level Director	Initiate State Disaster Response Plan with escalation as needed.
2	MAJOR	*Sub-regional/Regional	Subregional and Regional Authority Director	Initiate Regional Disaster Response plan with escalation as needed.
1	MINOR	*Municipal	Local	Initiate Local Disaster Response plan with escalation as needed.



* Note: Entity name is contingent on geographical location.

APPENDIX E

Appendix E contains presentation slides from the Middlebury Institute of International Studies at Monterey (MIIS), Cyber Initiative. Brian Steckler gave a briefing on Hastily Formed Networks for HA/DR, and the author followed with a presentation and discussion on the concepts of this thesis.

A Communication Strategy for Disaster Relief

Unclassified Information Brief March 2015

Prepared by Eric M. Folsom, Student Cyber Systems and Operations

Background

- What do disasters do?
- Stakeholders?
- Problems?
- What has been done to correct problems in disaster relief?
- Why create another technical solution for DR?

Issues Identified

- **Cost**
- **Interoperability** issues
- **Satellite** communications limitations, **bandwidth over-utilization**, and **frequency management**.
- Network **security policies** were not in place
- Internal **trust and collaboration** issues result in **Information overload**
- Lack of **automated reporting**
- Lack of **social media integration**

Audience Questions

- Does current technology allow us to create such a solution?
- Is a solution possible considering the social implications of DR?
- How can we better understand the system?

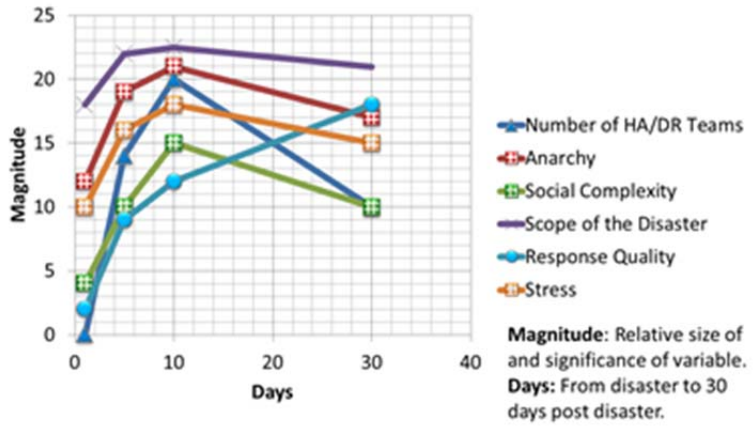
Systems Thinking process

1. Narrative
2. System level variable ID
3. Disaster relief (DR) timeline
4. Behavior over time
5. System causal loop diagram (CLD)
6. System level problem variable
7. Properly frame the problem
8. DR Injection point
9. DR balancing loop variables
10. Final DR causal loop diagram (CLD)

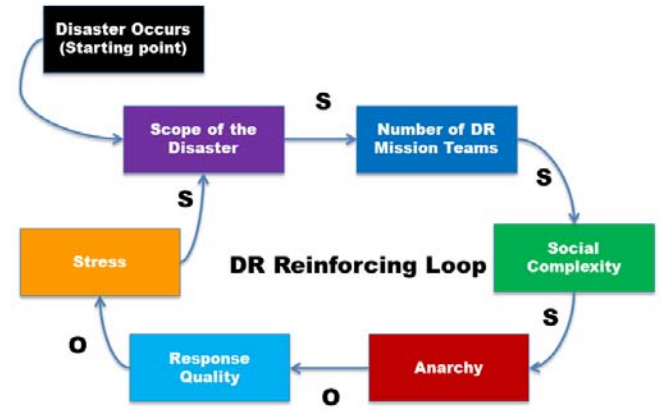
DR System Level Variables

- Scope of the disaster
- Number of disaster relief (DR) mission teams
- Social complexity
- Anarchy
- Response quality
- Stress

Variable Behavior Over Time



Current Disaster Relief System



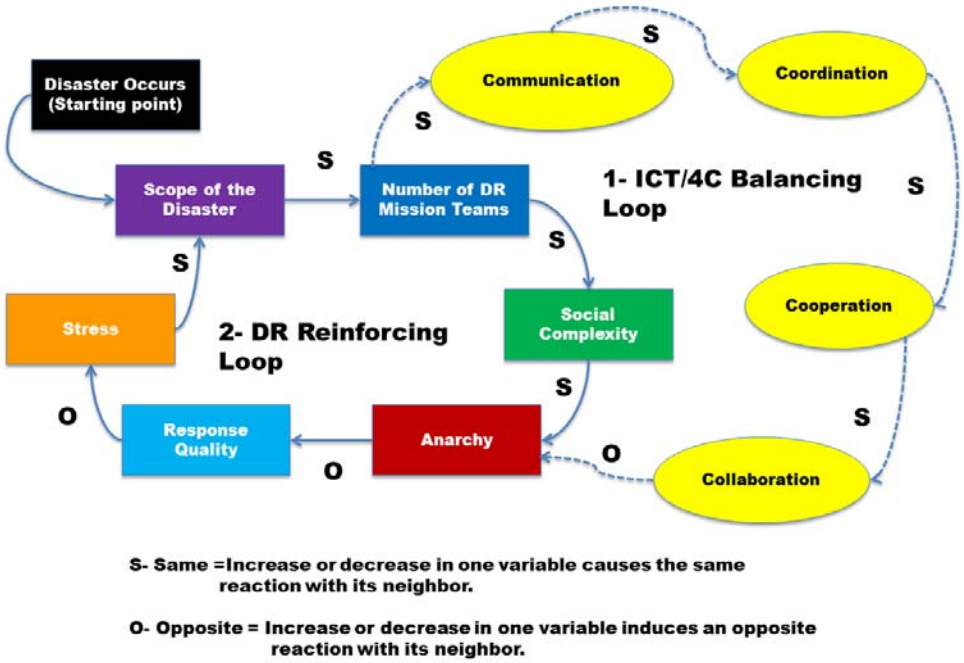
S- Same =Increase or decrease in one variable causes the same reaction with its neighbor.

O- Opposite = Increase or decrease in one variable induces an opposite reaction with its neighbor.

Balancing Variables

- Communication
- Coordination
- Cooperation
- Collaboration
- All four combine to create the 4C concept

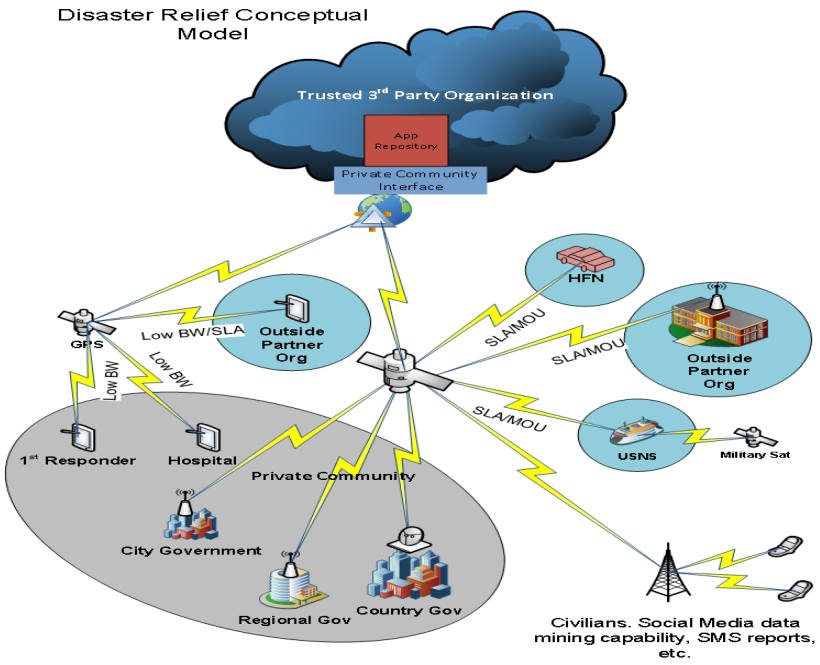
Adjusted DR System Loop



DR Communication Strategy Concepts

- A Connection Capability
- A Trusted Organization for Interface Management
- Cloud Model of Service and Deployment

A Connection Capability



ICT Options

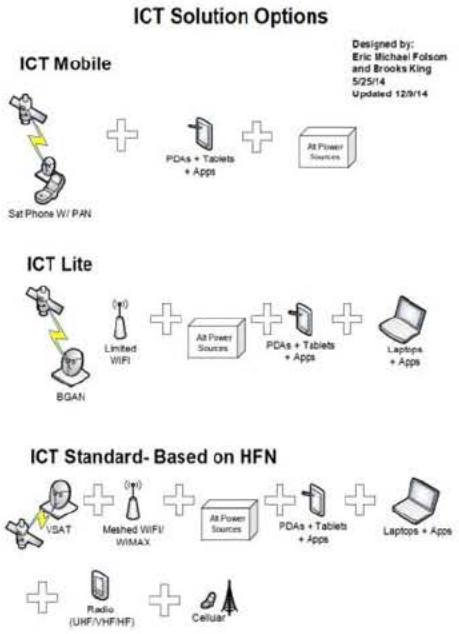
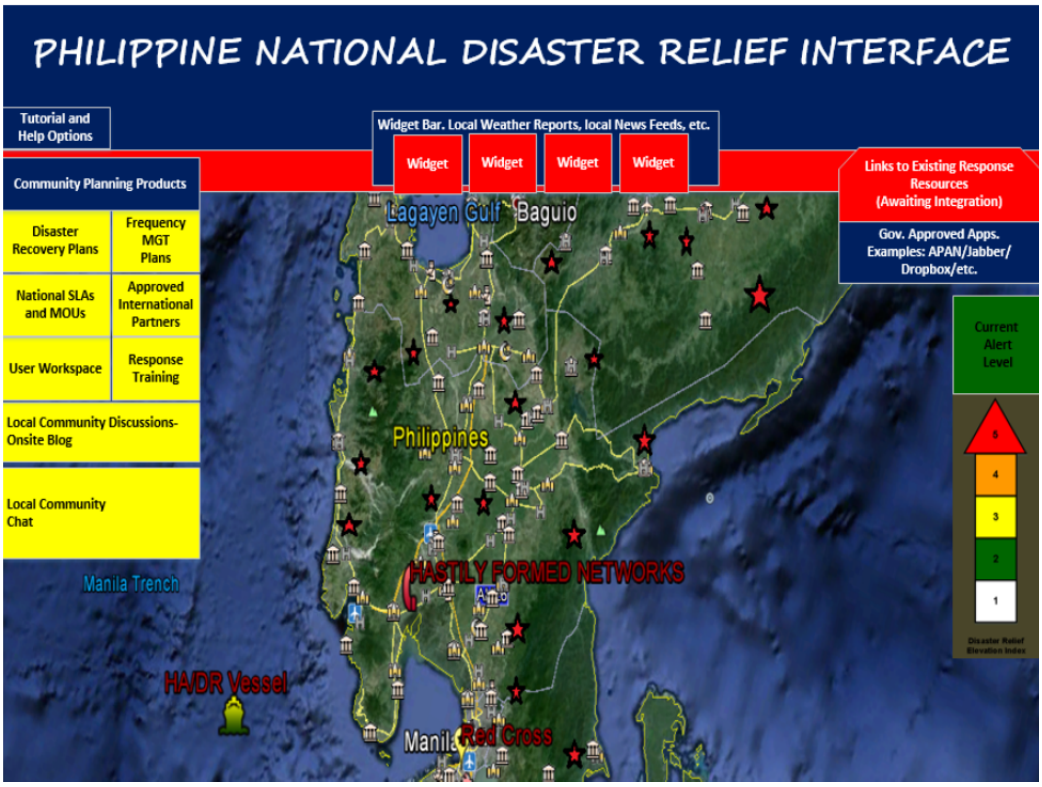


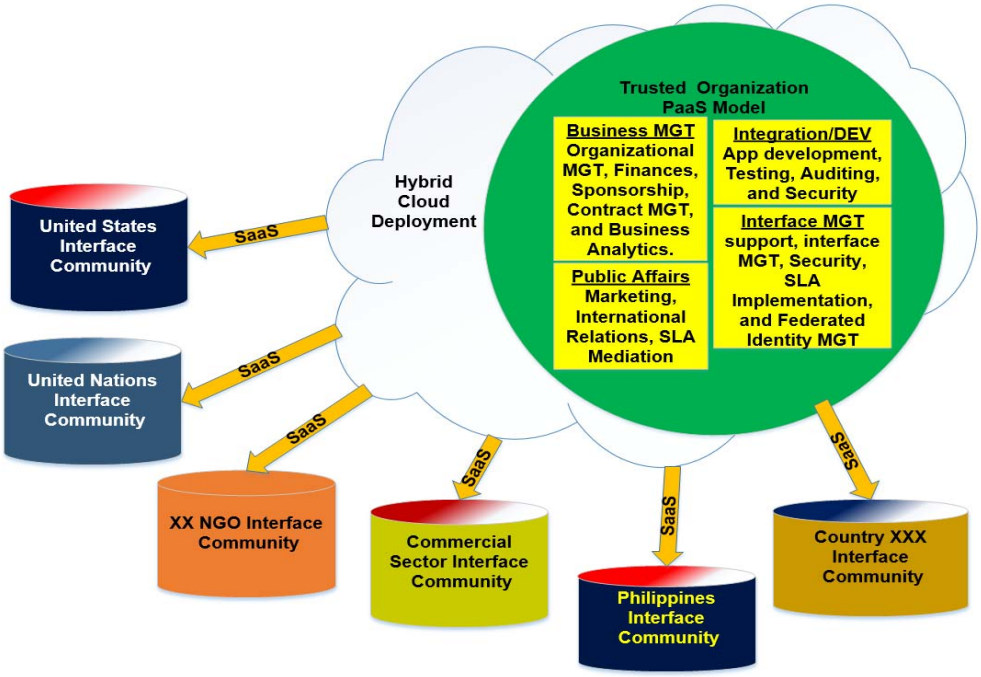
Figure 16. Hughes 9201 Broadband Global Area Network (BGAN). [168]

A Trusted Organization For Interface Management

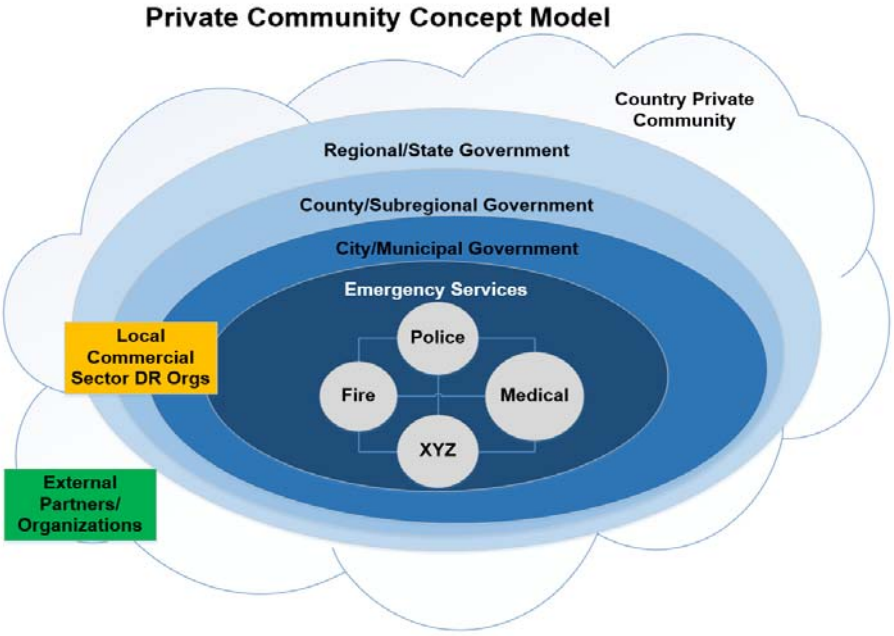
- Why a new trusted organization?
- Why not use an existing relief organization?
- Trusted organization responsibilities



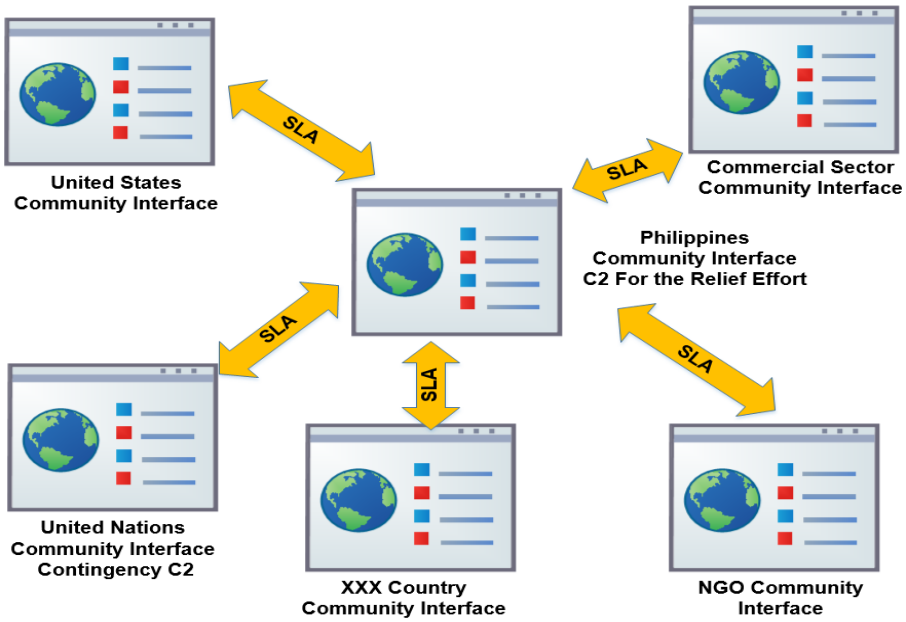
Cloud Model of Service



Private Community Model



Community Partnerships



Disaster Relief Elevation Matrix

Disaster Relief Elevation Matrix	*City/Municipal Emergency Services Down	*County/Subregional Government Down	*State/Regional Emergency Services Down	*Country Emergency Services Down	All Emergency Services Down
*City/Municipal Government Down	1	2	2	2	3
*County/Subregional Government Down	2	2	3	3	3
*State/Regional Government Down	2	3	4	4	4
*Country Government Down	2	3	4	5	5
All Government Down	3	3	4	5	5

Level	Severity	Elevation Level	Support level Authority	Support Categories
5	CATASTROPHIC	International	Any surviving Government or Emergency Services Representative	Initiate National Response Plan and integrate with partners
4	EXTREME	*Country	Highest Ranked Country Government Official	Initiate National Response Plan and alert International Partners.
3	EXTENSIVE	*State/Regional	State Level Director	Initiate State Disaster Response Plan with escalation as needed.
2	MAJOR	*Sub-regional/Regional	Subregional and Regional Authority Director	Initiate Regional Disaster Response plan with escalation as needed.
1	MINOR	*Municipal	Local	Initiate Local Disaster Response plan with escalation as needed.

* Note: Entity name is contingent on geographical location.

Future Research

- Prototype Development
- Detailed Security Plan
- Alternate Funding Sources

Questions

- Contact Information:
- Eric M. Folsom
- ericfolsom1@gmail.com

LIST OF REFERENCES

Akkoc, Raziye. “2004 Boxing Day Tsunami Facts.” *The Telegraph*. http://www.telegraph.co.uk/news/worldnews/asia/11303114/2004-Boxing-Day-tsunami-facts.html.

All Partners Access Network. “About page.” https://community.apan.org/p/about.aspx.

Amazon Web Service. “Storage Pricing.” AWS EC2. Accessed 20 January 2015. http://aws.amazon.com/ec2/pricing/.

Anderson, Virginia and Lauren Johnson. Systems *Thinking Basics: From Concepts to Causal Loops*. Waltham, MA: Pegasus Communications. 1997.

Antillion, Oscar D. “Hastily Formed Networks as an Enabler for the Emergency Response Community.” Master’s thesis, Naval Postgraduate School. March 2012.

Ashton, Jennifer. “Aboard the USNS Comfort in Haiti.” *CBS News*. 20 January 2010. http://www.cbsnews.com/news/aboard-the-usns-comfort-in-haiti/.

Austin Center for Design (ac4d). *Wicked Problems: Problems worth Solving.* Accessed 05 December 2014. https://www.wickedproblems.com/1_wicked_problems.php.

Barker, Patrick. “WPA2-PSK vs. WPA-PSK.” Discussion Question. *Microsoft Community Blog*. 13 September 2013. Accessed 22 February 2015. http://answers.microsoft.com/en-us/windows/forum/windows_8-security/wpa2-psk-vs-wpa-psk/a014e1e1-5289-4f61-98b0-e9450824dbcf.

Beason, Travis. “RTAT Survey v6.” PowerPoint Presentation. Naval Postgraduate School. Monterey, California. n.d.

Bradford, Bryan, Steve Urrea, and Brian Steckler. “After Action Report and Lessons Learned from The Naval Postgraduate School’s Response to Hurricane Katrina.” Master’s thesis, Naval Postgraduate School. September 2005.

Brandel, Mary. “Cloud Security: The Basics.” *CSOonline*. 15 June 2010. http://www.csoonline.com/article/2125258/cloud-security/cloud-security--the-basics.html.

BRCK. “BRCK Specifications Page.” 2014. Accessed 25 January 2015. http://www.brck.com/specification/.

CA Technologies. “Federated Identity and Single Sign-On Using CA API Gateway.” 2014. Accessed 22 January 2015. http://www.ca.com/us/~/media/Files/whitepapers/federated-identity-and-single-sign-on-using-ca-api-gateway.pdf.

Cabrera, Derek Anthony. “Systems Thinking.” Dissertation, Cornell University. Ithaca, NY. May 2006.

Chief of Naval Operations. *Disaster Response Operations.* Navy Warfare Publication (NWP 3-29). Norfolk, VA: Office of the Chief of Naval Operations. 2011.

Conklin, Jeff Ph.D. *Dialogue Mapping: Building Shared Understanding of Wicked Problems*. John Wiley & Sons. 2005.

Dawson, Christopher and Jennifer Grub. “How to help Typhoon Haiyan Survivors.” *CNN World News Online*. 22 November 2013. Accessed 23 November 2014. http://www.cnn.com/2013/11/09/world/iyw-how-to-help-typhoon-haiyan/.

Defense Advanced Research Projects Agency. “Request for Information (RFI): Strategic Collaboration.” DARPA White Paper Request. *FedBizOpps.gov.* 2 April 2007. https://www.fbo.gov/index?s=opportunity&mode=form&id=c705f867a67b945de03592276252b605&tab=core&_cview=0.

Delorme. “Delorme inReach Explorer Extreme.” *Delorme website*. Accessed 14 December 2014. http://www.inreachdelorme.com/product-info/inreach-explorer-extreme-communication-kit.php.

Denning, Peter J. “Hastily Formed Networks.” *Communications of the ACM* 49, No. 4. April 2006. http://faculty.nps.edu/dl/HFN/documents/HastilyFormedNetworks_Denning.pdf.

Ground Control Global Communications. “Inmarsat BGAN pricing.” Accessed 14 December 2014. http://www.groundcontrol.com/Hughes_9201_BGAN.htm.

Ground Control Global Communications. “Inmarsat Service Plan pricing.” Accessed 14 December 2014. http://www.groundcontrol.com/BGAN_rate_plans.htm.

Harris, Shon. *All-In-One CISSP Exam Guide*. ed.4. New York, NY: Mcgraw-Hill. 2008.

Hughes. “9201 BGAN terminal documentation.” Accessed 14 December 2014. http://www.hughes.com/technologies/mobilesat-systems/mobile-satellite-terminals/hughes-9201-bgan-inmarsat-terminal.

Hughes and Inmarsat. *BGAN 9201 User Manual*. ver. 4.0. Hughes Network Systems LLC. Germantown, MD. 2009.

Internet Engineering Task Force (IEFT). *TLS Protocol. ver. 1.0*. IEFT Request for Comments (RFC) 2246. January 1999.

Jansen, Wayne, and Timothy Grance. *Guidelines on Security and Privacy in Public Cloud Computing*. National Institute of Standards and Technology Special Publication 800–144 (NIST SP800-144). Gaithersburg, MD. December 2011.

Kapucu, Naim Ph.D. “Collaborative governance in international disasters: Nargis Cyclone in Myanmar and Sichuan Earthquake in China cases.” *International Journal of Emergency Management*. 8(1). 2011.

Lancaster, David D. “Developing a Fly Away Kit to Support Hastily Formed Networks for Humanitarian Assistance and Disaster Relief (HA/DR).” Master’s thesis, Naval Postgraduate School. 2005.

Lehembre, Guillaume. “Wi-Fi Security WEP, WPA and WPA 2.” *Hakin9.org*. vol. 6. June 2005. http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf.

Microsoft Azure. “Storage Pricing.” MS Azure. Accessed 20 January 2015. http://azure.microsoft.com/en-us/pricing/details/storage/.

Miller, Scott, Terry Ogletree, and Mark Soper. *Upgrading and Repairing Networks*. ed. 5. QUE publishing. 11 May 2006.

Mitchell, Bradley. “AES Versus TKIP for Wireless Encryption.” *AboutTech*. Accessed 22 February 2015. http://compnetworking.about.com/b/2008/08/21/aes-vs-tkip-for-wireless-encryption.htm.

MR3 Inc., and Black Swan Solutions. “Communicating in a Crisis.” MR3 and Black Swan Solutions Joint Webinar. 20 January 2015. http://www.mir3.com/mir3-inc-and-black-swan-solutions-present-joint-webinar-on-communicating-in-a-crisis/.

Mullen, Jethro. “Super Typhoon Haiyan, one of the strongest storms ever, hits central Philippines.” *CNN World News*. Updated 08 November 2013. Assessed 23 November 2014. http://www.cnn.com/2013/11/07/world/asia/philippines-typhoon-haiyan/

Nelson, Catherine B., Jeannie A. Stamberger, and Brian Steckler. “The Evolution of Hastily Formed Networks for Disaster Response, Technologies, Case Studies and Future Trends.” IEEE Global Humanitarian Technology Conference. 2011. http://www.cisco.com/web/about/doing_business/business_continuity/Paper_124_MSW_USltr_format.pdf.

Network Innovations. “BGAN or VSAT Comparing Technologies.” 26 April 2012. Accessed 14 December 2014. http://www.networkinv.com/bgan-or-vsat-comparing-the-technologies/.

Nixon, Steven. “Commentary: Wicked Problems. Network Solutions.” *Defense News*. 1 December 2013. http://www.defensenews.com/article/20131201/DEFREG02/312010009/Commentary-Wicked-Problems-Network-Solutions.

O’Neill, Mark. “SaaS, PaaS, IaaS: A security Checklist for Cloud Models.” *CSOonline*. 31 January 2011. http://www.csoonline.com/article/2126885/cloud-security/saas--paas--and-iaas--a-security-checklist-for-cloud-models.html.

OXFAM. “Haiti Earthquake – our response.” OXFAM International. Accessed 30 October 2014. http://www.oxfam.org/en/haiti-earthquake-our-response.

Oxford Learners Dictionary. “Definition of Wicked.” Oxford University Press. Assessed 02 September 2014. http://www.oxfordlearnersdictionaries.com/definition/english/wicked_1.

Pacific Disaster Center. “Disaster Response and Recovery Remain Challenging in the Central Philippines.” Published 22 November 2013. http://www.pdc.org/news-n-media/pdc-updates/Disaster-Response-and-Recovery-Remain-Challenging-in-the-Central-Philippines/.

———. “Haiyan Response Efforts in the Philippines Transitioning to Recovery Phase.” Published 29 November 2013. http://www.pdc.org/news-n-media/pdc-updates/Haiyan_Response_Efforts_in_the_Philippines_Transitioning_to_Recovery_Phase/.

———. “Massive Response Efforts Underway in the Philippines for Typhoon Haiyan.” Published 15 November 2013. http://www.pdc.org/news-n-media/pdc-updates/Massive-Response-Effort-Underway-in-the-Philippines-for-Typhoon-Haiyan/.

———. “DisasterAware Powered Emergency Operations.” http://www.pdc.org/solutions/products/disasteraware-emops/.

Parcelle, Jacobin. “Social Psychology of Conflict and Conflict Resolution.” International Encyclopedia of the Social and Behavioral Sciences. Elseviers Science Ltd. 2001.

Parrish, Kevin. “WPA Encryption Cracked in One Minute.” *Toms Guide US*. 27 August 2009. http://www.tomsguide.com/us/WPA-Cracked-Routers-Japanese-Scientists,news-4526.html.

Patton, George S. Jr. “Quotes.” Accessed 13 January 2015. http://www.generalpatton.com/quotes/index.html.

Persistent Systems. “Wave Relay Brochure, Manual-WR-01.” ver. 1.1. Issued 12 April 2012. Accessed 14 December 2014.

Ready.gov. “Emergency Response Plan.” 19 December 2012. http://www.ready.gov/business/implementation/emergency.

Redline Communications. “WiMAX Line of Sight Antenna.” Accessed 14 December 2014. http://rdlcom.com/products/ras-extend.

Reese, Fredrick. “Parts of New Orleans Struggle to Recover From Katrina.” *Mint Press News*. 15 August 2013. http://www.mintpressnews.com/inconsistent-progress-characterizes-new-orleans-ongoing-recovery/167036/.

Richards, Victoria. “Cyclone Pam: Vanuatu will run out of food “in a week” as officials slam aid agencies for wanting ‘publicity.’” 19 March 2015. http://www.independent.co.uk/news/world/australasia/cyclone-pam-vanuatu-will-run-out-of-food-in-a-week-as-officials-slam-aid-agencies-for-wanting-publicity-10119369.html.

Rittel, Horst W. J., and Melvin M. Webber. *Dilemmas in a General Theory of Planning.* Policy Sciences 4. 1973. pps.155-173.

Roberts, Nancy, Ph.D. Professor Naval Postgraduate School. “Coping with Wicked Problems.” Classroom Instruction. Monterey, CA. 22 September – 18 December 2014.

Rouse, Margret. “Short Message Service (SMS).” *techtarget*. July 2007. http://searchmobilecomputing.techtarget.com/definition/Short-Message-Service.

Satcom Resources. “Mobile VSAT terminal.” Assessed 14 December 2014. http://www.satcomresources.com/Viasat-Exede-Pro-Portable-Satellite-Terminal?sc=8&category=7313.

Sayer, Peter. “Researchers Crack WEP Wi-Fi Security in Record Time.” IDG News Service. *TechWorld*. 04 April 2010. http://www.techworld.com/news/security/researchers-crack-wep-wifi-security-in-record-time-8456/.

Scarfone, Karen, Cyrus Tibbs, and Matthew Sexton. *Guide to Securing WiMAX Communications*. National Institute of Standards and Technology (NIST) Special Publication 800–127(SP 800–127). Computer Science Division. Gaithersburg, MD. September 2010.

Stallings, William. *Data and Computer Communications*. ed.9. Prentice Hall. New Jersey. 2011.

Steckler, Brian. “A Report on the Naval Postgraduate School Response to the 2004 Southeast Asia Tsunami.” Naval Postgraduate School. Monterey, CA. 05 July 2005.

———. “Hastily Formed Networks: A report on Naval Postgraduate School Response to the 2004 Southeast Asia Tsunami.” Naval Postgraduate School. Monterey, CA. 25 July 2005.

———. “HFN-USNS Mercy Mission Report AAR.” Naval Postgraduate School. Monterey, CA. 11 July 2006.

———. “Hastily Formed Networks in Haiti: Haiti Earthquake After Action Report and Lessons Learned (AAR/LL).” Naval Postgraduate School. Monterey, CA. 8 September 2010.

———. “Hastily Formed Network Information Brief.” FCC Data Workshop. 4 October 2011. http://transition.fcc.gov/pshs/docs/summits/DACA/Steckler%20-%20FCC%20DACA%20Workshop.pdf.

———. HFN Support Briefing on Typhoon Haiyan/Yolanda. Naval Postgraduate School. Monterey, CA. January 2014.

———. Naval Postgraduate School Professor. “Hastily Formed Networks for HA/DR.” Classroom Instruction. Naval Postgraduate School. Monterey, CA. 22 June-16 September 2014.

Swanson, Marianne, Joan Hash, and Pauline Bowen. *Guide For Developing Security Plans for Federal Information Systems*. National Institute of Standards and Technology Special Publication 800–18(NIST SP 800–18). Rev 1. February 2006.

Washington Post. “Katrina’s Staggering Blow.” Washington Post Editorials. 31 August 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/30/AR2005083001554.html.

Tiger Direct. “Western Digital Hard Drive Advertisement.” http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=3580091&csid=_61. Accessed 29 January 2015.

———. “Seagate Hard Drive Advertisement.” Accessed 29 January 2015. http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=9557692&CatId=4357.

United Nations. *UN Humanitarian Civil-Military Coordination Officer Field Handbook*. Office for the Coordination of Humanitarian Affairs. Emergency Services Branch. Geneva, 2008.

———. “About.” Office for Coordination of Humanitarian Affairs. Accessed 23 September 2014. http://www.humanitarianresponse.info/about.

———. “History of the United Nations.” UN Online. Assessed 01 October 2014. http://www.un.org/en/aboutun/history/ .

———. “What is the Cluster Approach?” Humanitarian Response. Assessed 26 October 2014. http://www.humanitarianresponse.info/clusters/space/page/what-cluster-approach.

U.S. Agency for International Development. *Field Operations Guide for Disaster Assessment and Response*. USAID/OFDA. 2005.

U.S. Department of Commerce. *Security and Privacy Controls for Federal Information Systems and Organizations*. National Institute of Standards and Technology Special Publication 800–53 (NIST SP800-53). Gaithersburg, MD. April 2013, updated 22 January 2015.

U.S. Department of Defense. *Quadrennial Defense Review 2014*. Washington, DC: Office of the Secretary of Defense. March 2014.

U.S. House of Representatives. *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. 15 February 2006.

U.S. Senate. *Preparing for a Catastrophe: The Hurricane Pam Exercise. U.S. Senate Committee on Homeland Security and Governmental Affairs*. Senate Hearing 109–403. Washington, DC. 24 January 2006.

Waddell, Joshua, and Brian Steckler. “Marine C2 in support of HA/DR: Observations and Critical Assessments Following Super-Typhoon Haiyan.” *19th International Command and Control Research and Technology Symposium*. 2013. http://dodccrp.org/events/19th_iccrts_2014/track_chair/papers/120.pdf

Wentz, Larry. “An ICT Primer: Information and Communication Technologies for Civil-Military Coordination in Disaster Relief and Stabilization and Reconstruction.” Center for Technology and National Security Policy. National Defense University. Washington, DC. June 2006.

———. “Haiti Information and Communications Observations: Trip report for Visit 18 February to 1 March 2010.” Center for Technology and National Security. National Defense University. Washington, DC. 08 August 2010.

Wycoff, Jacob. “Flashback to Hurricane Katrina…8 Years Ago Today.” *WeatherBug*. 29 August 2013. http://knowbefore.weatherbug.com/2013/08/29/flashback-to-hurricane-katrina-8-years-ago-today/.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California