Using Web 2.0 Technology to Support Humanitarian Assistance and Disaster Relief Operations:

Applying the lessons learnt from the United States Military response to the 2010 Haiti Earthquake to improve the utilisation of the New Zealand Defence Force's Communications and Information Systems during Humanitarian Assistance and Disaster Relief Operations

A thesis presented in partial fulfilment of the requirement for the degree of

Master of Arts

In

Defence and Strategic Studies

At Massey University, Manawatu,

New Zealand

Liam Stewart Jones

2011

Abstract

Humanitarian Assistance and Disaster Relief (HA/DR) Operations are complex multidimensional environments requiring the deployment of a military force. These operations will have multiple agencies responding including military forces, emergency responders, United Nations agencies, None Government Organisations (NGOs) and Private Volunteer Organisations all of which specialising in the provision of the necessities of life to survive a disaster including food, shelter, water, sanitation, medical and logistics support. The coordination of the relief effort and ensuring resources are applied where they can achieve maximum impact is a significant challenge. Information and communications technology, and in particular the Internet, has matured to a level now where this technology can be used to aid with the coordination challenges facing the multiple responders in a HA/DR operation.

This paper examines the command and control arrangements that the New Zealand Defence Force has in place to support deployment on HA/DR operations and looks at modern commercial information technology trends, labelled broadly as Web 2.0, and proposes ways that these trends in information and communications technology might be utilised to increase the effectiveness of a New Zealand Defence Force Deployment. It examines the use of Web 2.0 type technology that was used by the United States Military during their deployment to Haiti and compares this with the use of information and communications technology by the New Zealand Defence Force during a response to a major earthquake in Christchurch and on an HA/DR exercise in the South Pacific. It seeks to highlight ways that the New Zealand Defence Force might use information and communications technology to enhance responses to HA/DR incidents in the future.

Acknowledgements

I would like to acknowledge the help and assistance of the New Zealand Defence Force and specifically the J6 of the Joint Force Headquarters and the Commanding Officer of 1 Signals Regiment provided to me while researching this topic.

Contents

Table of Figures

Introduction

The Military define Humanitarian Assistance and Disaster Relief (HA/DR) Operations as "complex multidimensional environments requiring the deployment of a military force will undoubtedly be experiencing dire humanitarian and human rights situations".[1] These operations will have multiple agencies responding including United Nations (UN) agencies, None Government Organisations (NGOs) and Private Volunteer Organisations (PVOs) all of which specialising in the provision of the necessities of life to survive a disaster including food, shelter, water, sanitation, medical and logistics support. Where the threat levels are high or the level of disaster is significant this will likely trigger the deployment of military forces to aid in the provision of life saving support.

Usually the response of a military force to an HA/DR event, and an international response as a whole for that matter, will be at the request of the government of the nation affected by a humanitarian or natural disaster. As such the sovereignty of the host nation will dictate the limitations that may be applied to the nature and range of assistance provided, and these agreements are usually established bilaterally through a pre-existing Status of Forces Agreement (SOFA), Memorandum of Understanding (MOU) or Third Party Note (TPN).[2] Military forces will have to work in complex environment with many stakeholders and interested parties.

The interaction between the military, the international responders and the civil environment in which they all operate is potentially crucial to the success of the response. The Multinational Force (MNF) Commander will most likely require specific command and staff arrangements for the management of civil-military cooperation (CIMIC) and the coordination with civil actors including the local population, local authorities, international agencies, and national and non-governmental organisations and agencies.

[1] Australian Defence Force ADDP 3.8: *Peace Operations* (Canberra:Australian Defence Force, 2009), 4.40.

[2] Australian Defence Force ADDP 00.3 *Multinational Operations* (Canberra: Australian Defence Force, 2011), 2.59.

The aim of these CIMIC arrangements is to coordinate civilian and military activities in support of humanitarian assistance and disaster relief efforts in order to achieve maximum support for the operation. The longer-term aim will be to generate stability and self-dependency within the local community, reduce local dependency on external aid and enable the smooth exit of military forces[3].

Underpinning any military response and coordination of the military response to align it with the civilian responders, local government and the civilian victims is the ability to effectively command and control the forces to enable them to achieve their aims to provide critical relief and support. In order to support effective command and control the provision of effective Communications and Information Systems (CIS) and the underpinning Information and Communications Technology (ICT) is essential. CIS is defined by NATO as the "assembly of equipment, methods, and procedures, and if necessary personnel, organised so as to accomplish specific information conveyance and processing functions."[4] It is a military term that is all encompassing of the entire spectrum of use of CIS from the physical equipment through the people who use and operate the equipment to the operating procedures and techniques to achieve this information flow.

This thesis intends to examine the way in which the New Zealand Defence Force (NZDF) is currently employing its CIS in support of HA/DR operations and suggest ways in which it can adapt its equipment, methods and procedures in order to make better use of existing technology to enable a more effective response to HA/DR incidents. It will do this by looking at past instances of NZDF responses to HA/DR situations both on exercise and during the recent Christchurch Earthquake and compare this with the US military response to the Haiti Earthquake in 2010. Arguably the US response to Haiti represents a

[3] Australian Defence Force, ADDP 00.3, 5.76.

[4] Larry Wentz, *An ICT Primer: Information and Communication Technologies for Civil-Military For Civil Military Coordination in Disaster Relief and Stabilization and Reconstruction* (Washington: Center for Technology and National Security National Defense University, July 2006), 110, http://www.ndu.edu/CTNSP/docUploaded/DTP31%20ICT%20Primer.pdf

watershed moment where US Forces started to integrate to a far greater extent with the civilian responders and aid agencies. At the same time the US Forces and other responders were making significant use of Web 2.0 type technologies to aid in there task to provide life saving support to the Earthquake victims. It is this aspect that makes the Haiti Earthquake an effective case study to enable the identification of key lessons that will enable the NZDF to make better use of existing CIS and to provide some indication of possible future directions to take Command and Control projects and acquisitions to enable them to leverage the way CIS and Web 2.0 is moving internationally.

Command and Control and the New Zealand Defence Force

Command and control are two essential components to enable the effective application of military assets to a achieve tasks or missions. Command is the authority that a commander in a military service lawfully exercises over subordinates. It also encompasses the responsibility for effectively using available resources and for planning the use of military forces. This includes organising, directing, coordinating and controlling military forces for the accomplishment of assigned missions.[1] It also includes responsibility for health, welfare, moral and discipline of assigned personnel. Commanders on operations tend to exercise command in this way. The commander of a unit will exercise command over deployed troops in the field. Control on the other hand tends to be used more for delegations to staff and is used to free the commander to enable him or her to make key command decisions.

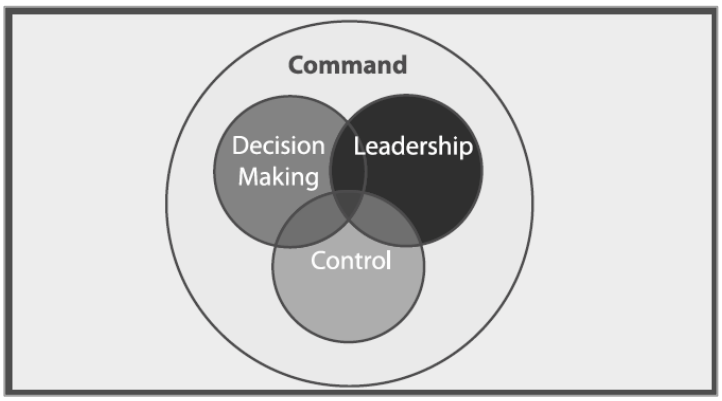

Figure 1. The Command Model[2]

Control, a subset of command, is authority exercised by a commander over part of the

[1] New Zealand Defence Force, *NZDDP–D: Foundations of New Zealand Military Doctrine (*Wellington: New Zealand Defence Force), 2008, G-1

[2] New Zealand Defence Force, *NZDDP-00.1 Command and Contol in the New Zealand Defence Force* (Wellington: New Zealand Defence Force), 2008, 1-4.

activities of subordinate organisations, or other organisations not normally under command. This encompasses the responsibility for implementing orders or directives. All or part of this authority may be transferred or delegated.[3] Control tends to be used in the implementation of command and is a process of monitoring progress and results.[4] It is about managing the implementation of commands and monitoring when changes are needed or decisions are required to be made.

Command is divided into three distinct but overlapping areas, one of which is control along with leadership and decision making (Figure 1 above). Leadership is the use of personality and character to inspire subordinate forces to achieve allocated missions. Leadership is, in essence, the human factor or charismatic part of the commander that aids in his or her ability to command. Control is the aspect, as mentioned before, that allows the commander to free themselves from the ongoing monitoring and checking processes, which is often delegated to a staff, to enable them to focus on making effective decisions. Decision making is the last critical aspect that makes up command. Making timely and effective decisions is a critical aspect of command.

Taking these three critical aspects into account it becomes evident that any command and control system must effectively support these three aspects. In order to support command and control it must enable the commander to apply their personality somehow. It must be able to inform the staff to enable effective control by a process of monitoring and reporting. By providing information to support this activity it enables the staff to monitor the ongoing progress of a force on achieving the commander's directives and identify when the situation has arisen that the commander is required to make a decision. Finally the system must enable a commander to make effective timely decisions by providing appropriate information to them in a timely manner. Too much information, incomplete or contradictory information or late information can all contribute to delaying the commander in making a decision.

[3] New Zealand Defence Force, NZDDP-D, G-1.

[4] New Zealand Defence Force, NZDDP-00.1, 1-4

Traditionally the New Zealand Army, in particular, has adopted commander's intent to overcome uncertainty and the fog of war[5]. The fog of war is a general term to define the state of the unknown or confusion as to what is happening during military operations. In order to overcome a situation where the fog of war prevents a commander from communication then if he or she has dictated his or her intent ahead of time subordinate commanders can make appropriate decisions. Command and control systems and communications technology can inevitably overcome these problems.

The utopian goal of technology is to remove the fog of wire until it is a "fine day"[6]. Yet if the system is not used effectively the end result may be an amplified fog to create such a thick pea soup that no commander can act with any certainty. Networks and Information and Communications Technology (ICT) can reduce the uncertainty but can equally amplify this uncertainty. Traditionally command has been centralised and decision making decentralised as long as subordinate elements work within the framework provided by the commander's intent. Linked Networks provide the ability to decentralise command decisions and enable command to be exercised at lower levels within the overall commander's intent by providing information at lower levels than previously achievable however this can be undermined by a number of situations. Technology can deliver quantities of accurate data but in a timeframe that prevents any real analysis within a reasonable timeframe to make a logical military decision. Secondly although subordinate elements may be able to draw on an array of battlefield assets, they are likely to be increasingly disassociated from the results of their decision making. Finally while decentralised war fighting might be enabled, the temptation to use increased connectedness may well lead to an increased temptation to centralise and direct war fighting from a higher and higher level.

[5] Ibid., 5-4.

[6] D.J. Schmidtchen, *The rise of the strategic private: technology, control and change in a network-enabled military* (Duntroon: Land Warfare Studies Centre, 2006), p9.

The New Zealand Defence Force applies the principles of military communications when planning technology support to Command and Control. The NZDF tends to adopt ABCA[7] doctrine which is moving from a hierarchical based system where radio communications were placed to allow the chain of command to operate in a hierarchical fashion to a more network based concept where situational awareness is spread across the entire organisation to enable forces to self synchronise. Self synchronisation is a concept emerging from Network Centric Warfare (NCW).

The Australian Defence Force Doctrine currently talks about self synchronisation as a key to its success. Self-synchronisation is an NCW aspects that attempts to change from a top-down hierarchical process with key decision makers at each level to a more lateral organisation that to achieve synchronised operations using shared situational awareness to recognise opportunities to act without direction while overall maintaining the mission objectives by a good understanding of the Commander's intent. Moving to self-synchronisation aims to make the ADF faster and more effective by capitalising on the shared understanding and collective initiative of lower–level commanders and staff.[8] The doctrine also notes that "self-synchronisation is not achievable until ADF network connectivity is ubiquitous at the strategic, operational and tactical levels, and the necessary tools are available at the desktop or weapons console."[9]

In fact networks are critical to the application of NCW principles and without good networks there is very limited ability to leverage modern ICT systems. The ADF doctrine talks about the "Achilles heel...[which]...lies with the networks that make it possible. Poorly planned and managed networks leave platforms and individual fighters isolated"[10]. It goes on to say that "the potential reduction of combat power due to poor network

[7] ABCA stands for Australia, Britain, Canada and America. This is a military interoperability forum that now includes New Zealand with effect 2006.

[8] Australian Defence Force, ADFP 6.0.1.1 CIS Planning (Canberra: Australian Defence Force), Ch 2 2.31.

[9] Ibid., Ch 2 2.32.

[10] Ibid., Ch 1 1.12.

performance is dramatic and may be decisive in a military engagement"[11]. Good networks are therefore critical to enabling effective use of the communications systems employed.

A review of the NZDF doctrine has revealed very little about the use of networks and applying NCW principles in any form. The NZDDP 3.0 Joint Operations talks about the need for Joint, Interagency and Multinational approach but the doctrinal diagram for command and control in a NZDF contribution to an international or national coalition (Figure 2. C2 Arrangements for an NZDF Contingent deployed as part of a Multinational Operation below) does show a closed box with very little in the way of actors external to the NZDF. The operating environment (Figure 3 below) does acknowledge the existence of a variety of actors that will contribute to the overall operation but the implication is that the NZDF elements will act as a discrete organisation and deploy liaison officers or establish liaison links as required for the specific operation at hand and these will form the interface points into specific command headquarters staff within a hierarchically controlled organisation.

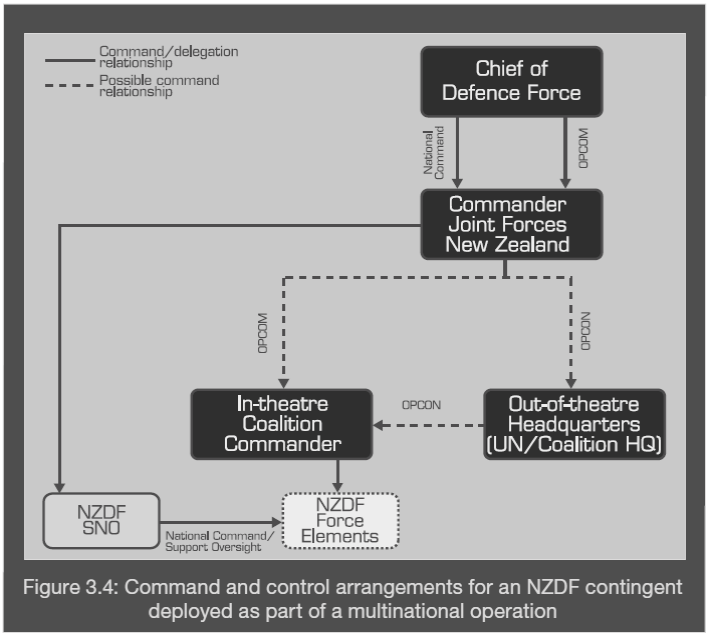

Figure 2. C2 Arrangements for an NZDF Contingent deployed as part of a Multinational Operation[12]

[11] Ibid.

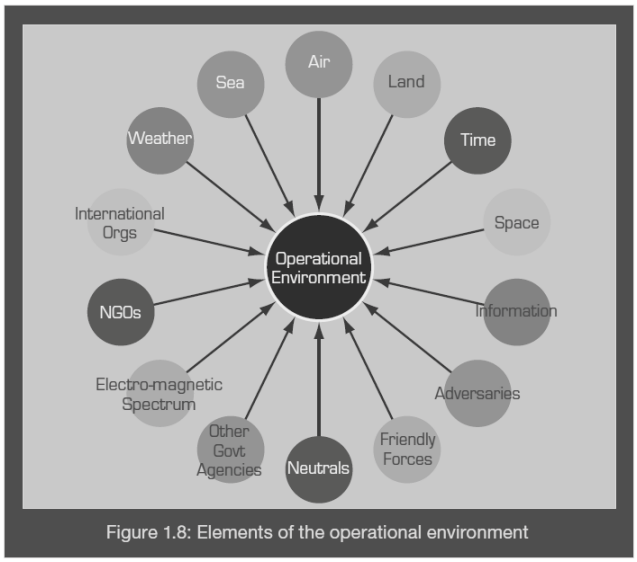

Figure 3. Elements of the Operational Environment[13]

The Royal New Zealand Signals Corps (RNZSigs) has had the traditional land based strategic communications and information systems technology role. In the 1990s this was provided by 5 Signals Squadron, at Air Force Base, Hobsonville. The unit was structured around three strategic capabilities – Strategic Communications, Trunk Radio and Electronic Warfare as well as a cipher support capability[14]. The unit was considered Force Troops and held capabilities that were intended to be employed at the strategic level. The overall focus of the 5 Signals Squadron, however, was one of strategic support and it worked directly to the Land Command HQ, located nearby in Takapuna, a HQ that was later subsumed when the HQ New Zealand Joint Forces was formed in Trentham camp in July 2001.[15] The capabilities of both the strategic communications unit and the trunk

[12] New Zealand Defence Force, *NZDDP-3.0: Joint Operations, (*Wellington: New Zealand Defence Force), 2010, 86.

[13] Ibid., 24.

[14] Laurie Barber and Cliff Lord, *Swift and Sure: a history of the Royal New Zealand Corps of Signals and Army Signalling in New Zealand* (Wellington: New Zealand Signals, 1996), 284.

[15] HQ New Zealand Defence Force, *New Zealand Defence Force*, 27 May 2011, http://www.nzdf.mil.nz/operations/deployments/east-timor/history.htm.

communications unit were dated with modern movements in ICT quickly outdating the equipment they employed.

Data and voice distribution at the operational level has seen a gradual decline since the 1990s. Trunk communications in the 1990s made use of the American Army Radio Relay equipment, acquired in the 1960s[16], which predominantly supported voice with a very limited data capability. This was eventually declared obsolete in August 2003 and retired from service in May 2004[17] without any replacement. There were a number of subsequent projects placed on the long term development plan to create a capability to distribute data on the battlefield, predominantly known as the Army Tactical Wide Area Network[18], but these have not seen any fruition to date and currently the capability requirement seems to exist in the C4ISR project.[19] There is a similar story with regards to strategic communications capabilities; however, with the advent of deployments to East Timor strategic communications has been replaced with ad hoc equipment over time to meet immediate mission needs.

Strategic communications in the 1990s utilised equipment called Medport based on a long range High Frequency (HF) radio capability. HF radio communications were difficult to manage due to a reliance on predicting the state of the atmosphere at any one time to enable radio links to be established and the Medport itself was large and cumbersome shelter mounted equipment, needing to be mounted on a Unimog 1700 truck[20]. While state of the art at the time, it quickly became obsolete and a move into satellite communications occurred with the acquisition of INMARSAT commercial communications capabilities in the early 1990s.[21] Significant defence capabilities were established by both

[16] Barber and Lord, *Swift and Sure*, 224.

[17] Lyle Mills, email response, 2008.

[18] *Defence Long Term Development Plan*, 2003 (Wellington: New Zealand Government); *Defence Long Term Development Plan*, 2008 (Wellington: New Zealand Government); *Defence Capability Plan*, 2011 (Wellington: Government of New Zealand).

[19] New Zealand Defence Force, C4ISR Project Capability Requirements Document, 2011.

[20] Barber and Lord, *Swift and Sure*, 226.

[21] Ibid., 225.

the ADF and by the USA, however the ANZUS rift of the put a stop to initial informal negotiations with the USA over access to satellite capabilities and access to access to US Defence satellite coverage in the Pacific.[22] The narrowband satellite systems acquired by the NZDF were limited in their capabilities and because they were essentially a dial up telephone system they were extremely expensive to use for extended periods of time[23]. It can be assumed that the long gap between the acquisition of VSAT[24] terminals in the early to mid 1990s and the larger capability procured after the deployment to East Timor in September 1999[25] is down to limited financial resources or a lack of will to acquire a strategic capability along with a very limited overseas commitment of NZDF land elements to operational service.

Traditional land based joint exercises in the 1990s to early 2000s were NZ based and focused on Brigade or Battalion groups with their associated support forces[26] and were not practiced much into the late 1990s as exercises were scaled down in size and duration. These appeared to be very traditional land based exercises with limited or no use for strategic communications because they seemed to adopt a philosophy of training in a brigade environment rather than training the brigade and therefore the highest exercising HQ was the Brigade HQ itself. The duration of the exercises of two to three weeks and because there was no offsite larger HQ there was not likely to be any demand for significant welfare or strategic communications. Also the local nature of the exercise and the availability of cell phones meant that coordination with home locations while exercising in New Zealand had suddenly become much easier. In essence there was no role to play for strategic communications so there was no demand likely for additional capabilities. Medport was retired from service in May 2000[27] with no replacement in

[22] Barber and Lord, *Swift and Sure*, 225-226.

[23] Murray Dick, interview by Liam Jones about the introduction of C-Band into the NZDF, 2012.

[24] Very Small Aperture Satellite Terminals which are small portable satellite terminals.

[25] HQ New Zealand Defence Force, *New Zealand Defence Force*, 2011.

[26] Foreign Affairs Defence and Trade Committee. *Questions for Written Response - 2007/2008 Financial Review (NZDF.* Wellington, 26 March 2009), 1-3.

[27] Mills, email, 2008.

capability other than the high cost, pay as you go Inmarsat capability already in service and a single channel Harris HF radio[28]. Where there was an imperative, however, the capability was developed and paid for readily.

At the same time as the Army was downgrading its strategic communications capabilities the Navy, who had a very real need for long distance strategic communications capability, were rapidly increasing their satellite requirements. They established a very capable IP network that was need to interoperate with other Navies as part of the AUSCANZUKUS[29] group meant that their capability was kept reasonably modern throughout with similar capabilities to the v-sat terminals on land but hard-wired into the ship with dedicated satellite bandwidth. The current Naval Doctrine states that "to address [unsupportable Allied and Coalition Information Exchange Requirements] a number of related initiatives were implemented. During Joint Warrior Interoperability Demonstration (JWID) 97 the initial aspects of a multi-national maritime WAN were demonstrated, and in RIMPAC 98 Commander Pacific Fleet (COMPACFLT) established what was to become a Wide Area Network (WAN) between Australia, Canada, United Kingdom, and the United States. Subsequently, there have been many incremental advances driven by operational requirements that led to the creation of a number of tactical mobile WANs or the extension of shore-based networks to sea"[30]. Because of these developments the ships required a dedicated communications bearer the satellite bandwidth which had dedicated funding and was managed on an ongoing basis by the Navy as a necessary capability. This was later to form the basis for the move to establishing significant strategic communications support in the Pacific once the NZDF got involved in its first major deployment in some time, to East Timor.

[28] Barber and Lord, *Swift and Sure*, 225.

[29] Australia, Canada, New Zealand, United Kingdom and the United States of America

[30] Combined Communications-Electronics Board, *ACP 200(C): Maritime Tactical Wide Area Networking,* (Washington: Combined Communications-Electronics Board, 2010), 1-1.

Smaller deployments of individuals and small numbers of people continued throughout, mainly to the UN, but these were of such small scale[31] and with significant support by host nations that national strategic communications was not required. The Air Force deployment to Somalia was one of the larger deployments but this made use of the not insignificant Air Force strategic HF radio communications capability[32] and was probably the last significant use of HF on any New Zealand Operational Deployment. Other deployments, such as to UNPROFOR in Bosnia saw the deployment of signallers in support of the Force for local communications but the strategic communications was provided by the host forces, in this case the UK military.[33] This is not to say that the skills had been downgraded. In fact New Zealand communicators had a very good reputation. They had provided significant communications support to a number of UN missions and were very well regarded in their skills for providing all levels of communication from tactical to strategic, particularly after the RNZSigs deployment to Cambodia in the early 1990s.[34] It was because of the nature of the deployments, as part of coalition forces or UN forces, that the capabilities had not been deployed. In fact throughout this time it was hard for the NZDF to see itself deployed in anything but a support role because of its inability to keep pace with the technological advancement of other nations.[35] It would not be until a significant deployment to East Timor that this mindset would appear to change and the NZDF would start to invest significant resources into developing ICT capabilities in support of command and control in any significant way, shape or form. This was evident when the first forces into East Timor, which had to make use of voice

[31] New Zealand Defence Force, *New Zealand Defence Force Deployments,* 2012, http://www.nzdf.mil.nz/operations/deployments/default.htm (accessed February 2012, 2012).

[32] Barber and Lord, *Swift and Sure*, 225.

[33] Ibid., 206.

[34] Ibid., 207.

[35] Piers Reid, 'Jointness: Lessons from Recent NZDF Peace Support Missions', in Joel Hayward (ed.), *A Joint Future?: The Move to Jointness and its implications for the New Zealand Defence Force: The Proceedings of the Third Annual Conference, 26-27 August 2000* (Palmerston North, NZ Defence and Strategic Studies Programme), 2000, 45.

communications over a satellite telephone[36] and narrow band satellite[37] which could be used for military messaging or data.[38]

Up until the deployment to East Timor deployments had been small and supported by other host nations with very capable radio communications capabilities that enabled NZDF personnel to communicate with New Zealand. East Timor the first time that infrastructure was needed. New Zealand forces were deployed in an isolated location in Suai, away from their Senior National Commander, located in Dili and their Support Elements, located in Darwin. Once it became apparent that the initial costs were going to be exceedingly expensive to operate the in-service satellite telephone systems and without the availability of significant strategic command and control capabilities, the NZDF was forced to acquire hybrid systems using commercial off the shelf acquisitions driven by the requirement of the Land Command HQ in Trentham. This was mainly driven by the need to provide welfare telephone services for the deployed personnel and the expense of doing this using in-service satellite telephones. Very quickly they were able to deploy a very capable C-Band satellite system with a small network into Suai which enabled the NZDF to venture into the realms of ICT support to Command and Control[39]. While there had been earlier opportunities to achieve this with the NZDF deployment to Bougainville, there was probably less of a financial imperative due to the nature of the operation and its short deployment duration[40]. This could not be said the same of in 1999 when the NZDF deployed a significant Joint Force into East Timor. This along with the formation of the Joint Force HQ was to be the catalyst of to highlight the need to replace the legacy tactical communications systems with something more capable and permanent.

[36] Mini-M Satellite Phone

[37] Inmarsat-B Terminal capable of a voice call or 64kbits of data

[38] Dick, interview.

[39] Dick, interview.

[40] Reid, 'Jointness: Lessons from Recent NZDF Peace Support Missions', 45.

Timor represented a significant watershed moment in strategic command and control facilitated by communications technology. The deployment drove the need for NZDF to take command and control of a force deployed for long periods of time and in isolation from other national forces and in fact they had now become responsible for other nations, such as the Irish and the Nepalese. Here was a very real need to support NZDF forces with modern strategic communications without the safety net of a bigger coalition partner. It became very quickly apparent once the strategic communications C-Band satellite systems were purchased and deployed to create a broad band data link from a deployed force to the NZDF, to meet the welfare communications needs long term, that connecting the systems within New Zealand with deployed systems to create a basic command and control system would offer significant benefits.[41] This was a major step forward in capability, which was driven mainly due to financial factors as opposed to a deliberate acquisition and the acquisition was commercial in nature rather than dedicated military systems and was limited in their deployability. The NZDF has not purchased purposely designed command and control systems to date.

A review of the long term development plans show that the NZDF has had plans to upgrade systems to meet its strategic communications systems in support of deployable forces for some time but have yet to implement these capabilities. There are essentially two requirements from a communications perspective. The first is to connect the deployed forces via some sort of international communications link, be this via a dedicated link such as the East Timor C-Band satellite link, over allied or a coalition partner's system or over a pre-existing network such as the Internet or another data service like mobile broadband. The second requirement is a distribution system in-theatre that allows for the connection of dislocated forces to communicate with each other as well as other parties, such as coalition partners, government agencies and non-government agencies (NGOs) as well as back to New Zealand.

While the various long term development plans have showed a desire to acquire such systems they have yet to provide any significant capabilities. The Joint Command and

[41] Dick, interview.

Control System project, a critical software project to address command and control requirements across the three services has been in the Long Term Development Plan since 2003[42] and has yet to be delivered. The Army Tactical Trunk Communications System, another critical capability to enable networking within NZDF deployed forces was identified on the Long Term Development Plan in 2003[43] and is undelivered and been subsumed into a larger project incorporating some Intelligence, Surveillance and Reconnaissance capabilities on the 2008 Long Term Development Program[44]. The recent buy into the World Global Satellite system will go some way to satisfying the requirement for satellite communications and the Defence Command and Control System (DC2S) project and the Network Enabled Army initiative will address command and control requirements for deployed Joint Forces. There have also been a number of subsequent communications projects that have enhanced the capabilities but these have been largely in the same vein as the original C-Band project to East Timor. The capabilities largely remain static systems with limited ability to distribute the information required to command and control to the wider deployed forces in-theatre.[45]

The other significant requirement, once a suitable bearer system has been established, is the command and control systems installed on the networks that enable effective command and control. Again the NZDF has had a number of projects to meet these requirements but currently it employs basic off the shelf systems.[46] This consists mainly of the Microsoft Office suite of applications such as word and excel with basic web applications and email. File storage is managed thorough a number of shared drives with access determined through the use of workgroups or branches and units within the organisation with information sharing between these silos done through the use of email.

---

[42] Ministry of Defence, *Defence Long Term Development Plan 2003*, 31-32.

[43] Ministry of Defence, *Defence Long Term Development Plan 2003*, 34.

[44] Ministry of Defence, *Defence Long Term Development Plan 2008*, 60.

[45] Paul Dragicevich, interview by Liam Jones about 1 Signals Regiment Perspective of HA/DR Communications Support, 2012.

[46] James Drybrough, interview by Liam Jones about NZDF CIS Support to HA/DR Operations from a Joint Headquarters J6 Perspective, 2012.

A number of specialist applications are available such as military messaging but these consist mainly of legacy applications that existed pre-internet and are hangovers from older systems. While the DC2S project looks to address the need for a common operating picture there does not appear to be any project to address the acquisition and exploitation of Web 2.0 capabilities.

Web 2.0 concepts are considered a revolution in the business world and there are important parallels with using the same concepts in a military context. Web 2.0 is best described by Tim O'Reilly who describes it as "harnessing collective intelligence"[47]. Important aspects of this concept include blogging, micro-blogging (Twitter), wikis (Wikipedia), Facebook and other social media, video and picture websites (such as YouTube and Flickr), mapping (such as Google maps and Google earth), user reviews on websites such as Amazon, feedback and comments (such as EBay) and video (Skype). These capabilities characterise the nature of Web 2.0 as they allow networking of individuals and create content that is gathered by sharing, learning and allow users of the technology to build on others contributions in a collective environment.[48] There have been some basic movement into the realm of file sharing and collaboration but these are basic capabilities based on Microsoft SharePoint with limited collaboration and information sharing capabilities and largely seem to be a web replacement for the existing storage drives currently in use which maintain the centrally controlled, stove-piped working groups with limited external collaboration facilities.[49]

The net result of the history of NZDF Command and Control systems development was that it was limited in its application and the organisation as a whole was very immature in its understanding of the use of ICT in support of Command and Control. It has a basic network developed to support stove-piped areas of operation with very little collaboration capabilities to enable wider networking except within the Navy which had

[47] Tim O'Reilly, 'Web Squared: Web 2.0 Five Years On', October 2009, http://www.web2summit.com/web2009/public/schedule/detail/10194.

[48] Tim O'Reilly, 'What is Web 2.0?', 5 September 2005, http://oreilly.com/web2/archive/what-is-web-20.html.

[49] New Zealand Defence Force, *InfoRM Project User Guide*, 2012.

developed its own capability in order to interoperate with allies in the maritime environment. It has limited static communications capabilities that have been procured in a hurried, ad hoc fashion to meet immediate operational needs rather than a long term deliberate strategy. It seems to continue to maintain the desire to procure command and control support systems, with several projects and experimental activities underway, but these projects have yet to deliver capability. The ability to network both internally and externally using web 2.0 type technologies is not currently a capability the NZDF has developed.

The Defence Network Enabled Capability Strategy[50] provides some guidance as to how the NZDF intends to develop its capabilities into the future. It identifies that the networking of military capabilities is essential for a modern defence force and highlights that modern information technology is a key enabler to link sensors, decision makers and weapon systems to help people, units and platforms work together more effectively to achieve the NZDF Joint Effect. It identifies that future capabilities will be required to operate effectively regardless of location, platform or operational partner so any capabilities acquired should support interoperability with key non-military partners and allow for interoperability in the HA/DR environment.

The Defence Capability Plan 2011 gives some real indication of where capability is likely to move into the future. It states the to "maximise the effectiveness of NZDF interventions, these capability sets must be embedded in network-enabled command and control structures which support joint activity between the Services; independent action by New Zealand in certain circumstances; interoperability with security partners; and responsiveness to whole-of-government requirements."[51] New Zealand Defence Force investment in networks has been focused on the corporate with less focus on operations. Operations to date, such as Afghanistan and East Timor, have been static and operating from forward bases.[52] In addition capability programs such as the Army Networking

[50] Ministry of Defence, *Defence Long Term Development Plan 2008*, 11.

[51] Ministry of Defence, *Defene Capability Plan*, 2011, 10.

[52] Drybrough, interview.

Projects and the Joint Command and Control project have not delivered capabilities to date so it seems that significant investment is needed to enable the networked vision in the Army Capability Plan.

In order to achieve the vision of providing a capability that is able to maximise the NZDF as a capability "development within the NZDF out to 2015 will focus on reorienting existing units and assets into a Joint Amphibious Task Force to provide an integrated and effective response to [the NZDF's] security needs."[53] Figure 4 below is a graphical representation of the structure that the Joint Amphibious Task Force is envisioned to look like. This Task Force will be able to carry out the non-combat tasks such as humanitarian assistance and disaster relief, however capability development does not mention expanding the command and control capability to include interfaced capabilities with other Government Agencies or networking with the wider responder community and working with NGOs and PVOs.

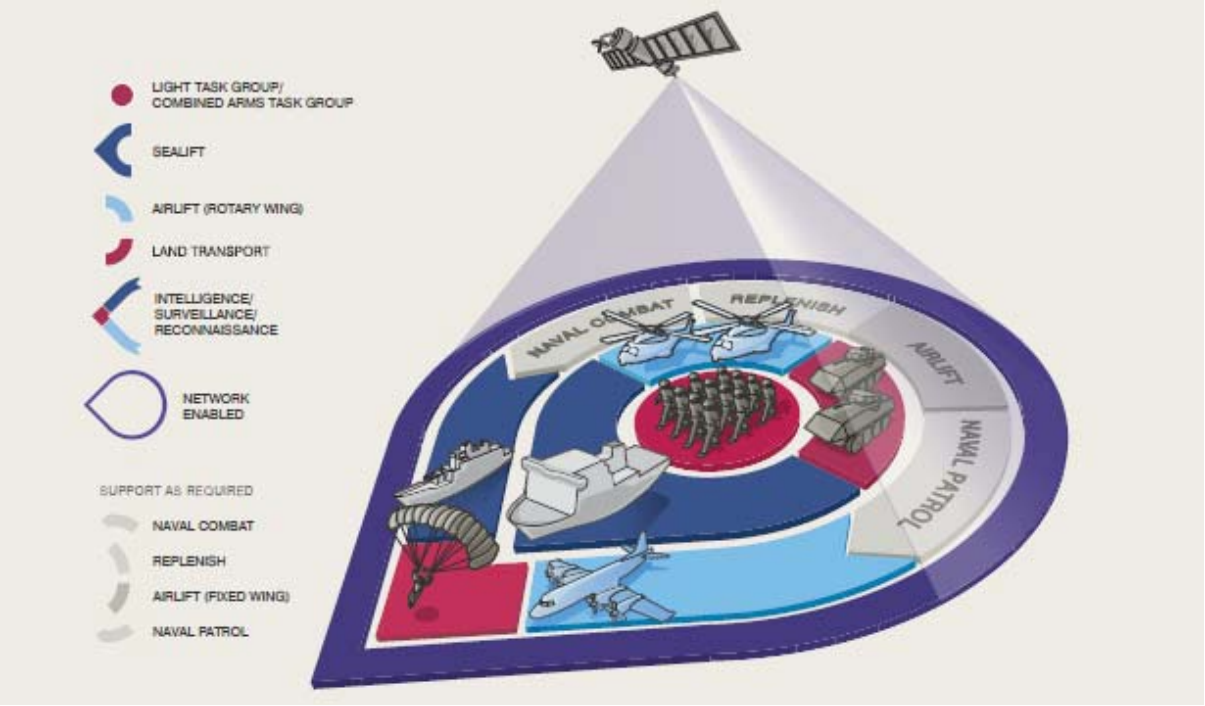

Figure 4. 2015 Joint Amphibious Task Force

[53] Ministry of Defence, *Defence Capability Plan 2011*, 12.

Integrated and complementary command and control, and intelligence, surveillance and reconnaissance capabilities, support deployed assets, including ground forces, by allowing them to conduct effective independent and coalition operations. Battlefield command and control systems with support communications and intelligence, surveillance and reconnaissance sensor networks are the key to this. These systems incorporate both personnel and technical equipment.

The Defence Command and Control System (DC2S) is a capability under acquisition. This programme will collect, collate, process, display, store, disseminate, and protect command and control information in near real-time. The system will enable force elements from all three Services to work together efficiently and effectively by enhancing their situational awareness and decision-making processes.[54] The initial phase of the project has been implemented on the Multi-Agency Network (MAN) but as discussed before, the limited capabilities of the MAN give it a limited reach and the majority of partners needed to coordinate during an HA/DR event are unlikely to have access to this system. Also, being a military system, the project is focusing on deployment of systems across the higher security networks used for military operations and not during HA/DR situations. While there will be significant benefit for command and control of internal NZDF capabilities there is limited ability for the program to implement capability outside of the organisation and it is unlikely that this capability will interface with Web 2.0 type technologies or enable the types of networking required in the hastily formed network environment that the NZDF will possibly find itself in if operating in HA/DR events on a large scale in the Asia Pacific Region.

A related programme is known as the Network Enabled Army or NEA. This project is in the initiation stage and will support the command and control of deployed ground forces and provide an enhanced ability to support the intelligence, surveillance and reconnaissance needs of the NZDF in the land environment. The Network Enabled Army will have command and control systems that are capable of collecting, synthesising and

[54] Ibid., 36.

disseminating data, information and intelligence in a timely manner to allow ground forces to manoeuvre and report simultaneously.[55]

The New Zealand Army has made significant movements forward with the implementation of the C4 Battlelab.[56] This battlelab has enabled the Army to experiment with leading edge capabilities and many of the Web 2.0 facilities are creating the opportunity to enable networking in a more collaborative way across multiple organisations. The battlelab has been able to integrate Voice, Collaboration and Messaging, a Common Operating Picture, Publish, Discover, Subscribe and Productivity Tools. [57] All these are the initial building blocks for enabling networking. In addition action has been taken to build unclassified networks into the architecture and this potentially will enable integration into wider networks

The Defence IMX project has recently been implemented. While this has claimed to incorporate a collaboration component this has been implemented in a very limited way and is more about the ability to store and manage documents as well as to meet legislated archiving policy requirements. It enables collaboration to a limited extend through the use of shared collaborative spaces where documents can be managed and shared between teams. It is not, however, intended to allow networking across boundaries and does not facilitate cross organisational collaboration to any significant extent. It also does not implement any Web 2.0 type collaboration technology.[58]

[55] Ibid., 36.

[56] Drybrough, interview.

[57] Jim Dryburgh, "New Zealand Army's Command and Control (C2) Battle Lab" Asia Pacific Defence Forum. 2010. http://www.asiapac-defenceforum.com/2010-presntations.aspx and Dryburgh, interview.

[58] New Zealand Defence Force, *IMX Overview and Progress Update.* Wellington, August 2009.

Web 2.0, Hierarchies vs Networks and Network Centric Warfare

In order to understand how a Military Organisation might make better use of its communication systems it must first understand where the world is moving with world wide communications. It is often said that the military is a microcosm of the wider community so in order to understand where the military needs to position itself it needs to understand where the world is right now. The most significant of these trends is the move to Web 2.0.

The World Wide Web moved the Internet from being a technical environment used by specialists to store and share information to a more easily accessible network for the everyday computer user. The initial Web or Web 1.0 as it is sometimes known used hypertext mark-up language, or HTML as it is commonly known, to present static web pages on a browser to enable easy access to information. The next iteration of the wide world web, which was coined as Web 2.0 was when this information moved from being static pages to be read to becoming more interactive. Web 2.0 allows Internet users to interact with each other and with the information online. The move to Web 2.0 in the wider business community has seen a dramatic shift from static company supplied information to a situation where the customer (user) interacts with the company (originator) to create online content building communities and networks that have enabled some companies to expand exponentially (Facebook, Twitter, Amazon, Google, Skype et al). Web 2.0 is not just a new version of the old Web. It is significantly different for a number of reasons. For example Web 2.0, facilitates flexible Web design, creative reuse, provides a rich, responsive user interface; facilitates collaborative content creation and modification; enables the creation of new applications by reusing and combining different applications on the Web or by combining data and information from different sources; establishes social networks of people with common interests; and supports collaboration and helps gather collective intelligence and updates.[1]

[1] San Murugesan, 'Understanding Web 2.0', *IT Pro* (IEEE Computer Society, July/August 2007), p34-35.

Web 2.0 has a number of techniques that differentiate it from Web 1.0. To create value participants must be able to locate what they are looking for on the web and Web 2.0 tools provide the means in which to do this. Links guide browsers to important pieces of information and provides structure to online content. The best pages, which are those linked to and the most frequently used, are highlighted and presented higher in precedence. The ability to author is an important technique for creating content. For example, Internet blogs allow participants to create content for a broad audience and wikis enable group authorship which can create convergent and accurate content. Content is categorised by creating tags that are simple, one-word descriptions reflecting the information structure and relationships in use by participants. Extensions automate some of the work of categorisation and pattern matching of information online through the use of algorithms so that relevant information is presented without the user needing to search for it. Amazon's recommendation system is an example of the use of extensions and provides suggestions of books that the user may be interested in based on what other readers with similar tastes have bought. Signals provided instant notification when there are changes to content that users are interested in. The user indicates they are interested in particular pieces of information, for example, and an email or notification is sent to the user when this information changes for some reason.[2]

The primary difference between Web 1.0 and Web 2.0 is the customer-centric, user-interactive and dynamic nature of the Web 2.0 environment. Interaction is the central premise of Web 2.0 and activities such as networking and social computing are key using mediums such as blogs, podcasts, vodcasts, social networks, search engines and voice over IP to enable interaction across the web. The key characteristics of these capabilities are that they are always on and available on demand. They are accessible at all times from anywhere from a home or work computer, cell phone or mobile device such as an iPad. Their content is predominantly controlled by the users and consumer, not by the

[2] Sang M. Lee, Taewan Kim, Yonghwi Noh and Byungku Lee, 'Success factors of platform leadership in web 2.0 service business', *Service Business. An International Journal* (Jun, 2010), Vol.4, No. 2, 91.

owners. They are mainly global in nature crossing international boundaries and they constantly changing and evolving.[3]

In essence the shift from Web 1.0 to Web 2.0 is two fold. There is the technical evolution of the Internet and the continued evolution from the static to the dynamic, secondly there is the changing user experience. This social science side suggests that the web now is the users, not just a tool used by users. Amy Shuen, a writer on the Web 2.0 subject, suggests that in the Web 2.0 world people are "shaping the Web and the world's digitized collective knowledge in unexpected directions through their uploads, content, and billions of clicks a day."[4] The millions and millions of Internet users are shaping the content of the Web and are learning and changing the way they think through sharing collaborating and trading. Tim O'Reilly, who is one of the foremost experts on Web 2.0 summaries the concept of web 2.0 as a "business revolution… …caused by the move to the internet as a platform, and an attempt to understand the rules for success on that new platform. Chief among those rules is this: Build applications that harness network effects to get better the more people use them."[5] The network effect that O'Reilly is talking about is central to Web 2.0 and is an extension to Metcalfe's law[6] which states that "the value of a telecommunications network is proportional to the square of the number of users of the system"[7]. The key aspects of this changing in the Internet is how new technology enables large numbers of people come together to work, share, and build.[8] Shuen highlights some specific reasons as to how and why this occurs including users create value, networks multiply effects and people build connections.

---

[3] T. Singh and J. Cullinane, *Surfing the rift: The Executive's Guide to the Post-Web 2.0 World* (Kindle Version, CullinaneMedia, 2009), 19-22.

[4] Amy Shuen, *Web 2.0: A Strategy Guide* (Kindle Version, O'Reilly Media, 2008), location 289.

[5] http://radar.oreilly.com/archives/2006/12/web_20_compatc.html, sited in Shuen, Web 2.0, location 340.

[6] Jesse Wilkins, 'Web 2.0: What does it mean and why does it matter?', Infonomics (Jul/Aug 2007), 11.

[7] Robert Metcalfe cited in Wilkins, 'Web 2.0', 11.

[8] Shuen, *Web 2.0*, location 341.

The idea that users can add value has been around for a while but it was not until the implementation of Web 2.0 technologies that the ideas have crystallised into reality. With the advent of Web 2.0 users have made the leap from passive consumers of information to active participants who are contributing to the overall web of information. Shuen describes this as online DIY (do-it-yourself) where users are able to "interact, combine, remix, upload, change, and customize for themselves."[9] Shuen argues that this turbo charges the network (the Internet) by allowing users because the interaction benefits all users and the contributions of one user benefit many others, as well as themselves making the overall network collectively more useful to all the participants. Examples of this would be the provision of reviews that enable a user to read the opinions of others. Collective ratings give an average overall rating of a movie or book for instance enabling someone to judge if they will find the product of interest. Amazon provides suggestions for other items a user may be interested in based on their previous purchases and what others with similar interests have bought. Flickr, an online photo sharing site, uses a complex, undisclosed, algorithm to rate online photos creating a highly effective rating system. Meta data with specific tags or key words, provided by the user as they upload their data, enable users to hone in quickly to the areas they are interested in. Tag clouds or graphical representations of tag words where the size of the word on the page indicates the number of tagged photos behind it enable quick navigation to areas of interest using fuzzy, human guided searches rather than having to navigate large, search engine generated, hard to navigate lists.

Traffic is critical to creating positive network effects. A dynamic Web 2.0 environment enables the creation of networks in a far more dynamic way than was ever possible in a static Web 1.0 situation. The more a network is used the more effective it becomes and the bigger the growth of the network as it becomes more useable. Overtime these positive network effects create a "bandwagon effect as the network becomes more valuable and more people join"[10]. The web, as a network has "an intrinsic value that grows exponentially with the amount of information or network connections contained

[9] Shuen, *Web 2.0*, location 473.

[10] Dion Hinchcliffe, 'Why all the fuss about Web 2.0?', Infonomics, Jan/Feb 2010, 28.

within them."[11] The network effects are what make the network valuable and encourage the growth and use of the network over time. There are a variety of network effects to be considered.

The different kinds of network effects that are in action with Web 2.0 including direct, indirect, cross-network and demand side effects, all of which overall magnify the positive effect of a network. The basic premise, however, is that positive network effects increase the value of a good or service as more people use or adopt it. The simplest of these effects are direct effects. The more a network is used the greater the increase in value of a system. Skype is an excellent example of this. As more people join skype there are more people to call. The usefulness of skype becomes greater and greater as more and more users join.[12] As the network utilisation grows the useful of the network increases to the participants of the network, thereby encouraging further participation in the network.

Indirect network effects relate to the usage of a network and the effect it creates by spawning the production of increasingly valuable complementary goods or services that add value to the original network product or service. The example that Shuen uses is Windows and file compatibility. The indirect network effects are created by the addition of complementary applications that increase the usability of windows as a product.[13] Similarly cross-network effects creates an effect because the rise in usage of one group of users increasing the value of a complementary product or service of another distinct group of users. For example a rise in usage of an online auction network, such as Trademe, by sellers means that there is a greater variety of goods and therefore an increase in quality for users who are using the website to buy goods. The online auction site has two distinct user groups, sellers and buyers, and an increased usage by one group increases the quality of the service for the other. The fourth network effect is the social network effect. This is the effect that online social groups create. The behaviour of an individual is directly influenced by the decisions of a small subset of other consumers that

[11] Ibid.

[12] Shuen, *Web 2.0*, location 1299.

[13] Ibid., location 1132-1331.

they are connected to by an underlining network, such as a social network or business network.[14] By understanding these network forces and making use of them businesses (and the military) can take advantage of Web 2.0 Internet networks and increase the value of their products and services.

Following on from networking it is important to understand that participation is critical. People that build connections and "success comes down to one critical factor: Participation… …there must be an active and involved core community with members who are willing to stay invested"[15]. Shuen has identified that online social networks using Web 2.0 technology, such as Facebook have three important advantages over previous ways of making contact with clients or customers. Firstly social networks are much more powerful customer acquisition engines and are able to connect and reach far more people than offline networks. Secondly the users on social networks tend to be highly interactive and engaged. Finally value is created by the significant uploading of user information creating huge databases of organised content.[16] The use of Web postings, Instant messaging, email, audio and video enables significant social connection within a network. Information can be instantly published and share enabling people to become information providers, brokers through the provision of information using such tools as email, blogs and wikis.[17]

It is also important to understand that users behave in a variety of different ways but all levels of engagement and user behaviours have benefits within a Web 2.0 environment. Passive users provide content through a record of the history of their activity and when this is collected it can be used to influence other users' behaviour, providing added value. For example Amazon recommends books to users based on what other readers, with similar profiles, have purchased. Minimally active users add their own content to other people's content but rarely create their own unique content. They will Tag other people's

[14] Ibid., location 1331.

[15] Jessica Dye, 'Collaboration2.0: Make the web your workspace', EContent (Jan/Feb 2007), 36.

[16] Shuen, *Web 2.0*, location 2007.

[17] Ibid., location 2121-2131.

photos or write small amounts of content themselves. For example they will add comments to articles and blogs online or writing their own Blog. Collaborative users that are very active will work together over the net to add collaborative, collective content. For examples a wide range of people contribute small amounts of data to Wikipedia which collective make Wikipedia a reasonable accurate and valuable source of information.[18] What is critical here is that all Web 2.0 users are adding value and thereby increasing the overall value of the network.

The military is not a profit driven organisation but can still make use of Web 2.0 and the power of networks. The way the military implements networks and harnesses the power of Web 2.0 can enhance the way the command and control works. By enhancing the way a military uses networks it is able to transition from to what Wentz terms "knowledgably intervention"[19] As shown previously the NZDF currently uses a hierarchical system of command and control where the communications follows the chain of command. This method of command and control was used because information flows in wartime was slow and expensive. The internet and the rapid increase in storage, processing and communications speeds and capacities have meant that military communications is now fast and inexpensive. [20] It could be argued that this has created the need to review the hierarchical command and control structure and consider modifying or replacing it to better leverage the rapid change in information and communications technology and the advent of Web 2.0.

As a consequence of the difficulties faced by the Federal Emergency Management Agency (FEMA) during Hurricane Katrina, the US Military has been studying the impact of networks during disaster relief operations and the results of these studies parallel the theories of Web 2.0 very closely. In August of 2005 Hurricane Katrina hit the states of

[18] Moria Levy, 'Web 2.0 implications on management', *Journal of Knowledge Management*, Vol 13, No 1 (2009), 122.

[19] Larry Wentz, *Haiti Information and Communications Observations: Trip Report* (Washington: National Defense University Press, 2010), 32.

[20] Peter Denning and Rick Hayes-Roth, 'Decision Making in Very Large Networks', *Communications of the ACM*, November 2006, Vol. 49, No. 11, 21.

Louisiana and Mississippi in the Southern United States severely damaging the infrastructure. For this particular situation FEMA was made the lead agency to coordinate the relief effort. FEMA failed to meet the objectives set and was plagued by a number of organisational problems, disputes, information overload, delays, fraud and wastage of relief funding.[21] The problems faced by FEMA during Hurricane Katrina were similar to the problems faced by hierarchical military organisations when coordinating in complex military operations including HA/DR operations. In fact during HA/DR activities the networks that are formed are made up of hastily formed, disparate organisations that are thrust together to conduct the relief and recovery operations.

Hastily formed networks are formally defined as being an organisational structure that is "(a) put together quickly in response to an emergency, crisis or urgent situation, (b) from a collection of entities who have expertise or local responsibility to help but have not worked together before, (c) and who accept no higher decision making authority."[22] This accurately describes the first response organisations that usually react to an HA/DR activity. In order to understand why FEMA failed during Hurricane Katrina and how these organisations can better work together it is important to understand the driving factors behind hastily formed networks.

These networks can also be closely related to the issues that NCW highlights and is attempting to resolve. If units on the battlefield are seen as organisations that need to operate closely together in a coordinated fashion, where their hierarchical coordinating body is intermittently in command due to the severely challenging communications environment, does not want to be overloaded with information and wants to react quickly and effectively to a changing situation it attempts to put networks in place that encourage self synchronisation under the commanders intent. Similarly in a HA/DR activity, speed is important and the delay in operations can have serious implications for the victims on the ground. The central command agencies (ie FEMA) cannot afford to be overloaded with information and to some extent the hierarchy or central command

[21] Ibid., 19-20.

[22] Ibid., 19.

structure cannot exist, given the multitude and disparate formations that make up the first responders. The communications environment is likely to be severely damaged and existing communications systems non-existent or intermittently available. In fact what needs to occur is self synchronisation of a hastily formed network of responders. Modern communications make it seem easy to establish networks and operate effectively. Quite clearly it is not that easy as FEMA's response to Katrina showed. This has not only occurred with FEMA during Hurricane Katrina but other responses to tsunami relief along the Indian Ocean in 2004 and several earthquakes in 2005 all of which displayed similar problems . Establishing effective networks using modern technology is not easy. In order to establish effective networks the principles highlighted by the experiences growing from the use of Web 2.0 need to be considered.

Level	Focus	Examples	Systems Perspective	Biology Perspective	Issues	Principles
4 **Hyper-Networks**	Federated activities toward common goals among multiple organizations that retain their separate identities and have no common hierarchy	B2B exchange, ecosystems (Amazon.com, iTunes, eBay, Wikipedia, blogs), consortia (W3C, IETF, OMG), hastily formed networks	Complex adaptive systems Systems of systems	Ecological communities	Information sharing, information overload, valued information at the right time (VIRT), shared models and semantics, cross-organization structure, collaborative commerce	Push, pull, search, filters, context-aware models, conditions of interest, distributed decision-making, need to share
3 **Organizations and Communities**	Coordinated activities within a single organization or community that has a single purpose	Businesses (Amazon.com, iTunes, eBay, Paypal), enterprises, supply chains, processes	Coordination systems Transactions Workflows	Life forms	Enterprise architecture, information assurance, information overload, organizational structure, command and control, process specification and management	Concurrency control, interaction rules, social network structure, channels for content types, need to know
2 **Internet Service Providers and Customers**	Accounts, access, and bit-flows managed by protocols and middleware	Protocols (email, datagram, file transfer, remote login, Web service, secure sockets, WiFi), middleware (name services, search engines, single sign-on, business VPN, packet telephony, audio and video streaming)	Information flow systems	Circulatory system Central nervous system	Protocol design, end to end error recovery, access control, firewalls, congestion, spam, virus, Trojan horse attacks, secret communications, most of network invisible to search engines	Protocol verification, domains of protection, bottleneck control, queuing, resource contention and prioritization
1 **Signals and Telecommunications**	Physical components, links, signals	Routers, fiber cables, leased lines, switches, Hamming codes, routing algorithms, network cards, local networks, wide area networks, IP addressing	Physical systems	Neurons and their connections	Connectivity, packet loss, link or router failure, error recovery, congestion, buffer overflow	Redundancy, dynamic routing, fundamental laws of throughput and response time, power laws of connectivity

Figure 5. Four Levels of Network[23]

[23] Ibid., 20.

Traditionally the military and ICT wider community have considered networks in a layer model called the Open Standards Interconnect Model (OSI Model). This model saw a computer network as starting at the physical layer (the cables and devices) through to the application layer (the programs that run on a system). It has become increasingly important to view the systems in the way organisational specialist see them, with human networks as layers above the applications layer. If the human network layers are taken into account this broadens the understanding of the system and allows for considerations other than the technical considerations as a consequence of applying the OSI model. The additional layers include the organisations and communities layer (layer 3) and the hyper-network layer (layer 4). Figure 5 above illustrates these layers.

The important layer from a HA/DR perspective is the hyper-network layer. This layer is where multiple networks interact beyond their normal scope in a collaborative manner. No longer are the networks bounded by their organisational boundaries but they stretch beyond, interact and enable information to flow into and out of an organisation at multiple levels. Traditional hierarchical systems attempt to choke these interactions and control the flow of information into and out of an organisation. When hyper-networks exist this is no longer the case. It allows for the formation of interest groups and collaborative groups across organisational boundaries and at multiple levels. Good examples of these are eBay or Amazon, making use of the advantages that Web 2.0 technology brings. While these websites seem to be a contiguous single identity, in reality they are a collection of separate networks all working together in a collaborative sense to put sellers and buyers together. They contain many different businesses and communities that value add. For example, Amazon.com has large networks of book suppliers, book promoters, customers and other interested parties all facilitating the rapid increase in the volume and pace of transactions across the various layers of networks. [24] The advantages that Shuen highlights that networks can provide enhances the capabilities of the responder forces.

[24] Ibid., 21-22.

Hastily formed networks are a form of hyper-network and should follow the behaviours shown by networks utilising Web 2.0 technology. As is the case with the military, most of the first responders to a HA/DR activity are hierarchical in nature (Police, Military, Fire Service for example) but some are quite clearly not. Some of the Non-Governmental Organisations and Aid Agencies may be run as flat organisations or loose collections of interested parties and sub-organisations. The United Nations, for example, operates a cluster concept where individual organisations are clustered together in functional groups. What is different in these situations, as opposed to the Hurricane Katrina example, is that there is no top level. Rather than having one organisation in the lead (FEMA) each organisation works as part of the network at the same level, networked together but sharing the decision making process applying what NCW defines as self synchronisation. Decisions are made in a distributed and collaborative way, rather than a structuring decision making through a chain of command.

Where the FEMA example arguably struggled was the expectation of what the chain of command could do. The expectation is that modern communication systems will allow an organisation (such as FEMA) to overlay a chain of command structure onto national, regional and local relief operations. The problem with this is that it has all the same issues identified by NCW and accentuates the fog of war, or as Jim Walsh called it in a presentation he made to the New Zealand Defence Force Command and Staff Course in 2011, the "fog of relief"[25] by which he meant the sheer number of participants in a disaster relief scenario and the total confusion that this causes. "The effectiveness of a hastily formed network depends as much on the participating people and organizations as it does on the communication system through which they interact."[26]

HADR activities in effect pose a new command and control problem. Networks thrive on connectivity and users. In order to achieve the network effects seen using Web 2.0

[25] Jim Walsh, 'Civilian Response Stakeholders', presentation to the New Zealand Command and Staff Course, Center for Excellence in Disaster Management and Humanitarian Assistance, Hawaii, USA, 22 November 2011.

[26] Peter J. Denning, 'Hastily Formed Networks', *Communications of the ACM*, April 2006 Vol. 49, No. 4, 15-20.

technology there has to be connectivity in order to join users together. Connectivity aids command and control but without effective means of communications then networks cannot operate because the flow of information. Military organisations, such as the NZDF tend to be setup to operate in a military environment and working in a broader collaborative environment to make maximum use of Web 2.0 capabilities to enable collaboration and networking across inter-service and inter-agency environments effectively in HA/DR situations is a new concept.[27] Knowledge and wisdom is seen to be proportionate to rank and experience so a traditional hierarchical system has emerged as the preferred network structure in the defence environment. This type of structure is not the best structure to make best use of Web 2.0 and network technology that is emerging in a modern connected world and is counterproductive in an operational situation where broad networking across multiple organisations is needed.[28] The situation that arises with HA/DR activities is there is generally a group of disparate organisations that come together to provide assistance within the affected area of country. These organisations include local government organisations, international and national aid agencies and foreign government agencies just to name a few. All these organisations tend to operate their own communications capabilities which tend not to be interoperable, unless there has been a deliberate strategy to do so.[29]

It is argued by a number of people that 21st century networks are defeating the hierarchies of the 19th century war fighting organisations. Lieutenant Colonel Schmidtchen, of the ADF, concedes that there is an element of truth to this but also argues that the importance of hierarchies is underrated and that the value of networks is over rated.[30] He argues that networks and hierarchies can co-exist. Hierarchies are appropriate in a military organisation because they enable conflict resolution by having a clear chain of command and allocation of resources to tasks, especially when resources

[27] Drybrough, interview.

[28] Schmidtchen, *The rise of the strategic private*, 10.

[29] Ibid., 8.

[30] Ibid., 27.

are scarce. Networks co-exist in the spaces between the hierarchies. They are the more informal groups that form, leveraging off social capital using the values of trust, reciprocity and citizenship. These networks have always existed within the military hierarchy but, with the advent of Web 2.0 and the increase in communications capabilities, there is now the ability to significantly enhance or break these networks and have significant ramifications for an organisation.

Hierarchies, without a doubt, are critical to ensuring military capability. The real gains to be made are the ability to integrate hierarchies and allow for free flow of information at more than just the higher levels of the hierarchy to other hierarchies and into other organisations such as other agencies and other militaries for instance. These horizontal flows exist already. Desk officers and commanders make phone calls to their peers within other organisations and liaison officer exchanges occur on an as needed basis when incidents occur.[31] By creating the opportunity for networking by the provision of tighter technical network connections between boundaries at these lower levels the leverage of network effects will enhance the overall usefulness of Web 2.0 technologies.

The opportunity that Web 2.0 and networks present to Defence Forces to enable them to make effective use of technology is suggested by Goldsmith and Eggers to be a confluence of four trends. Goldsmith and Eggers contend that influential trends are altering the shape of the public sector worldwide: third-party government, joined up government, the digital revolution and consumer demand. Schmidtchen re-labels them to terms that are probably more familiar to NZDF personnel: whole of government approach, growth in the use of contractors, computing and communications revolution and mission diversity. Goldsmith and Eggers contend that public administrators must reconcile their traditional static top down hierarchies with horizontal networks.[32] This phenomena means that the NZDF needs to be cognisant of horizontal networks when preparing for, planning and deploying on HA/DR operations if it wants to make effective use of technology during these activities.

[31] Drybrough, interview.

[32] Schmidtchen, *The rise of the strategic private*, 32.

NCW also touches on this subject with the idea of self organisation. Self organisation occurs in networks in a bottom up fashion where their efforts combine to create complex behaviour. The combined efforts of the individual network nodes create more than each individual node is capable of and create high level collective sophistication. A simple example is a flock of birds. Each individual bird is just following the leader but the result is a complex collective behaviour where the flock moves almost as if it is a living organism itself. Enabling this capability through networking using sophisticated commutations technology should enable a force intervening during a disaster event to achieve sophisticated behaviour to enable it to maximise its response during that activity.

The ability to self synchronise is not a new phenomena in the NZDF. The Army has long had the concept of mission command. The commander passes his intent to his subordinate organisations and these organisations use this intent to formulate their actions and take advantage of situations as they arise, within the overall commander's mission and intent. The concept of mission command was not formulated to take advantage of horizontal networking, however, but rather to mitigate the risk of no network at all. In the absence of communication the organisation still needs to function so by creating an overall intent or framework for the organisation to operate against, it mitigates against the risk of paralysis and ensures that subordinate commanders have enough information to operate the absence of information. Ironically in an organisation that is using complex modern technology the problem is not so much a lack of information but the opposite, information overload.

Due to their hierarchical nature, defence organisations utilising modern communications technologies often find themselves in information overload. The HQ no longer has the capacity to process the deluge of information they are confronted by. The power of networks and the ability to network horizontally is that much of the information does not need to go upwards and can remain below and only that information that is seen as essential is passed on or made available. The detail of information is shared locally at a lower level between different organisations at the relevant level. There is still the requirement for mission command and commander's intent to be specified as it guides the actions of the networks at the various levels and by specifying these parameters, the

intent, and the organisation mitigates itself against paralysis by information overload. This type of networking is essential in HA/DR activities because it allows the exploitation of Web 2.0 network effects.

Networking is essential during HA/DR activities because organisations tend to be overwhelmed by the sheer level of work required and information needing to be processed. The ability to self synchronise comes from the ability to interoperate and information transparency, the ability to provide the information required. If these two things are achieved then the networks can be expanded beyond the traditional organisational boundaries of the hierarchical organisation. This is exactly what is needed in a HA/DR situation where there are many disparate organisations all needing information to be effective and all gathering information others need to achieve their role. The ability to create a scalable network that can expand, contract and adapt to changing circumstances is paramount to enable the individual organisations within the network to achieve their missions.[33]

What this means for HA/DR operations for the NZDF is twofold. Firstly it needs to ensure greater connectivity across inter-service boundaries. There is a traditional stove-piped communications between the individual service boundaries and there is a need to open these up. The introduction of the multi-roll vessel will, by de facto, encourage this. Experiences during training and operations have indicated that there are communication problems from naval to the land elements.[34] By investing in and expanding the tactical networks across defence using web 2.0 technology will enable things such as self synchronisation to occur. In a HA/DR situation this will enable the better allocation of resources through better information sharing across service boundaries. This will need a shift in culture from Single Service focus to a more Joint oriented culture.

The traditional military structures exist as tried and true methods of command and control. Hierarchical methods work and are effective on the battlefield. Web 2.0 type technologies are great enablers for situational awareness but the ability to control the

[33] Ibid., 35-38.

[34] Dragicevich, interview.

Defence Force elements through a hierarchical system is still needed. What can be achieved though, is better situational awareness and decision making in the absence of an identified overall lead or command of the entire HA/DR effort, but still guided by a well articulated Military Commander's intent exploiting the effects generated by networks.

The New Zealand Defence Force Approach to Command and Control in a Humanitarian Relief/Disaster Response Scenario

The NZDF doctrinal approach to command and control varies depending on the type and nature of the task. An HA/DR situation is likely to be either New Zealand based or based within the Pacific Region. If it is based in the Pacific Region the NZDF can respond with anything from a large contingent of people and equipment to an individual platform such as a single ship or aircraft. In the case if a deployment of an individual platform the deployed ship or aircraft will usually use of its own internal communications and is likely to be on a limited task such as search and rescue or aid delivery and as such the communication problems are simplified so is out of the scope for consideration. The deployment of a contingent is a lot more complex. Figure 6 below shows the deployment arrangements for a New Zealand contingent supporting an overseas operation. As can be seen there is a deployed Commander or Senior National Officer who is attached to the coalition commander with a relationship to both the in theatre Force Commander and to the NZ Joint Force Commander back in New Zealand. Also likely attached is a National Support Element to provide logistic type support.

This diagram indicates a number of communication issues for consideration. Firstly there is the integration of New Zealand based command and control systems with the Coalition Force. There is also the inter-service connection to enable force elements to communicate with each other. There is also the communication issue with other elements in the area of operations, Non-Government Organisations, Government Organisations and other interested parties. Finally there is the communication requirements back to New Zealand. It does not specifically detail how liaison with other nationalities and agencies may be accomplished though the task of coordinating the communications plan or NZDF Force Elements in theatre[1] is designated to the Senior National Command Element of which the Senior National Officer is a part.

[1] Ibid., 5.13.

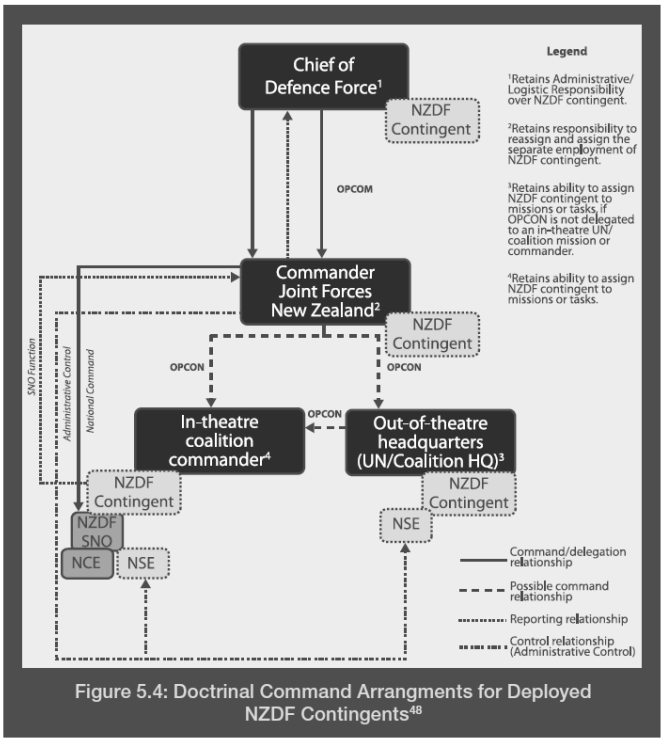

Figure 5.4: Doctrinal Command Arrangments for Deployed NZDF Contingents[48]

Figure 6. Doctrinal Command Arrangements for Deployed NZDF Contingents[2]

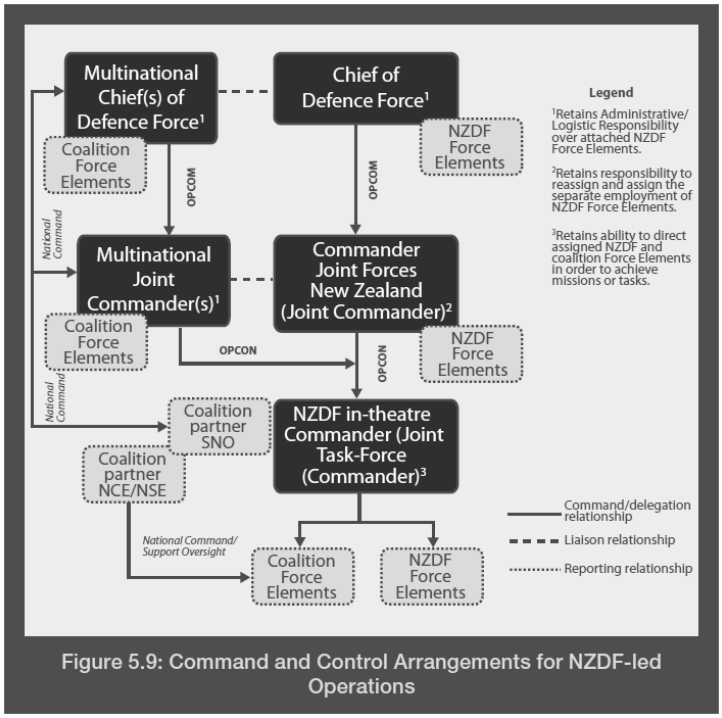

Figure 5.9: Command and Control Arrangements for NZDF-led Operations

Figure 7. Command and Control Arrangements for NZDF-led Operations[3]

[2] New Zealand Defence Force, NZDDP-00.1, 5-7.

When New Zealand is the lead nation there is an added complexity. Figure 7 above outlines the command and control arrangements for a New Zealand led operation. It involves not only providing the communications requirements for the NZDF deployed forces as described in the previous example but also providing the communications structure for command and controlling the assigned other national assets. This creates the challenge of either integrating other national command and control systems with the NZDF's systems or providing a coalition wide capability. In both these examples (New Zealand participating as a coalition contributing nation or as a lead nation) it is likely that an HA/DR incident will happen at very short notice.

The detailed doctrine for the NZDF planning considerations for CIS on Multinational Operations is based on ADF doctrine. The doctrine focuses on networks and gives some basic advice noting that communications via radio and computer are critical. It notes that planning considerations should include frequency management, equipment compatibility, procedural compatibility, cryptographic and information security, identification friend or foe, and data-link protocols. It also notes that a lack of interoperability between national communications systems is to be expected and that many communications issues can be resolved through equipment exchange and liaison teams. Use of technology is important for protecting forces and providing security.[4] While this is probably appropriate for interoperability for a component as part of a multinational force it does not take into account the issues surrounding interoperability with civilian agencies particularly around interconnection of networks and the rapid declassification of data to enable information sharing.

The doctrine goes on to note that the increased demands on a multinational force can cause congestion in the radio frequency spectrum and it is essential that communications requirements are coordinated early by technical communications systems control centres. It also notes that in all multinational operations a broadband, unclassified computer network will be a critical requirement for multinational coordination with

[3] Ibid., 5-14.

[4] Australian Defence Force. ADDP 00.3 *Multinational Operations* (Canberra: Australian Defence Force 2011), 5.89.

military and non-military participants. It also highlights that access to satellites for broadband internet may need to be provided if not available in theatre and all communications requirements need to be closely coordinated with the host nation to ensure the local civilian systems are not overloaded.[5] This is beginning to touch on some critical areas that need to be considered. The host nation communications systems are under a significant amount of strain but as will be shown later the cell phone networks in particular are critical to interoperability and command and control. Again what will be shown is that the demand on bandwidth and satellite bandwidth in particular is significant with everyone from aid agencies to news agencies all usually turning up with their own satellite communications solutions, most of which will be at the very least the same part of the electromagnetic spectrum if not the same systems. Also the host nation, having experienced significant stress is unlikely to be functioning sufficiently to coordinate the management of such things as frequency allocations.

In order to deal with short notice situations it can be deduced that the command and control systems themselves need to be able to interoperate at short notice. This means that there must either be compatible or command and control systems that can be connected or some form of unified system (a coalition command and control system) which participants either connect to or are provided with. During a successful HA/DR incident, then, if command and control is effective, then a well designed command and control structure supported by a well connected command and control system would likely have been employed. In order to asses the effectiveness of the NZDFs ability to achieve this the lessons learnt from both the Exercise Tropic Twilight (an HA/DR simulation exercise run by the NZDF in the Pacific) and Operation Canterbury Quake (a domestic operation run by the NZDF in response to a major earthquake in Christchurch New Zealand) will be examined.

HADR activities are becoming a significant part of role of Military and have been a major focus for NZDF. Contingency Plan No 103: Pacific Relief addresses the provision of relief

[5] Ibid., 5.90-5.91.

in the event of a disaster in the South Pacific.[6] This document highlights that the New Zealand International Development Group[7] are responsible for managing the All of government (AoG) response to a natural disaster in the Pacific.[8] This suggests that in order to manage the NZDF response to disasters the organisation will need to coordinate closely with these agencies and other responders. It indicates that the method to do this is through normal email communications. The HQ New Zealand Defence Force Strategic Commitments and Intelligence (SCI) Branch has the ongoing liaison responsibility and an LO will be attached to MFAT/NZAID in the initial stages.[9] The liaison officer will communicate primarily through email and cell phone with no indications of any specific communications utilising web technologies or collaboration technologies. The deploying forces will be provided with a communications suite coordinated by the J6 Branch (the branch responsible for CIS for deployed forces).

The plan has a light concept of communications support. It talks about deploying a satellite phone with the initial forces and utilising the data from the deployed Naval Force with initial deployed ships. Should it be needed a broad band satellite system would be deployed.[10] The plan focuses on the deployed forces and makes no mention of specific use of CIS to coordinate with other agencies either prior to or during the activity. It does not address the loss of infrastructure in the country forces are deploying to and any liaison at the local level other than allocating this as a task to the various force elements deployed[11]. The air element is allocated the responsibility to establish MFAT/AID liaison with NZDF during the initial phases of the operation.[12] All three service elements (Land,

[6] HQ Joint Forces New Zealand. "HQ JFNZ CONPLAN 103: PLAN PACIFIC RELIEF (ISSUE 4)." (Wellington: New Zealand Defence Force, 2010), Covering Minute.

[7] MFAT/NZAID.

[8] HQ Joint Forces New Zealand, CONPLAN 103, 2.

[9] Ibid., 4-5.

[10] Ibid., 17 and Annex D.

[11] Ibid., 10-14.

[12] Ibid., 12.

Sea and Air) are tasked with establishing strategic links back to New Zealand.[13] Overall the Forces seem well served to manage voice and limited data communications back to New Zealand but networking horizontally with other agencies in theatre and managing the lack of local infrastructure does not seem so well catered for.

The HQ Joint Forces New Zealand regularly deploys reconnaissance teams to Pacific Island Countries to liaise with the New Zealand Diplomatic Staff and Head of Mission (HoM) to conduct planning and review existing contingency plans. As part of this a communications expert is deployed to review the existing communications capabilities. These are documented and held on file for future reference during planning activities triggered by an incident such as a natural disaster that requires an NZDF response.[14] While these plans are kept as up to date as possible they are updated on a cyclic rotation so a country that has not been visited in a while may be out of date. Apart from researching publicly available information such as the Internet this is the only source of data a planner has to get a picture of what the communications capabilities are of the New Zealand diplomatic staff, local government and non-government organisations and civilian telecommunication providers and other Information Technology providers.

Tropic Twilight was conducted by the NZDF over the period 25 June to 23 July 2010 in Tuvalu in support of the MFAT Official Development Assistance (ODA) programme. While the exercise was to test the Pacific Relief Contingency Plan it was mainly used to deliver projects supporting health and education. The exercise post activity report comments that "Tropic Twilight is a structured exercise, with set objectives and planned tasks, and is scripted far more than a disaster response"[15] As such it therefore did not have the same stresses placed on it that an HA/DR activity might generate. There were only two nations participating; a deployed New Zealand Force of about 300 personnel on board the HMNZS Canterbury along with a French Armed Forces New Caledonia (FANC) helicopter

[13] Ibid., 13-14.

[14] Brent Lancaster, interview by Liam Jones, NZDF Communications Planning for HA/DR Relief Operations, 2012.

[15] 2nd Engineer Regiment, Post Activity Report: Exercise Tropic Twilight 2010, (Linton: New Zealand Defence Force, 24 September 2010), F-1.

embarked.[16] Other government agencies were invited but other than MFAT/NZAID participation was limited to some observers. It would likely be the case that there would be significant other involvement from other New Zealand and international based organisations should the situation be a live HA/DR event. It is likely that any communication issues experienced on this exercise would also be magnified.

A number of communication issues were experienced during the exercise which highlighted that a significant level of networking between elements was not achieved. Coordination issues between HMNZS Canterbury and deployed Land elements were noted by the Land Commander[17] and by the Maritime Commander.[18] Direct communications between the ship and the land forces was difficult. Radio communications are line of sight so any deployment of the Ship out of the HQ area meant that communications were lost and the maintenance of long range communications is limited between land and maritime assets due to complexity and compatibility issues. This meant that there was limited ability to coordinate effectively between the two elements. Coordination issues were also experienced between NZ based personnel and deployed personnel.[19] It appeared from the observations that personnel were not working from common documentation. For example the load manifests did not match with what was expected on arrival of aircraft. There was also confusion over administrative details and these were not communicated effectively back to New Zealand.[20] The use of a common source of information or access to the same data may have alleviated these problems. This was not possible, however, because the primary use of communications was via voice (cell and satellite phone) and email (via NZDF IT systems) both of which do not make full utilisation of web 2.0 type collaboration type technologies. While voice is a valid form of command and control information passed by

[16] Ibid., 2.

[17] Ibid., F-7.

[18] HMNZS Canterbury, Post Exercise Report: Exercise Tropic Twilight 10 (TTW10), (Auckland: New Zealand Defence Force, 10 August 2010), Annex A.

[19] 2nd Engineer Regiment, Post Activity Report 2010, F11.

[20] Ibid., F-5.

voice is either person to person (ie telephone call) or held in a small network (ie radio network) and therefore is hard to record and share with a wider network of participants.

It was commented that the use of open internet must be preferred to secure means for speed and ease of communications.[21] Had this source of information been readily accessible, via established hotspots in the primary locations for instance, it may have provided a more effective capability and allowed more people to establish and maintain connections. There was, however, limited use of collaboration tools. While the All Partners Area Network (APAN) was utilised on the exercise, the APAN network was not heavily used during the exercise but it "could be a useful tool in a [Conplan Pacific Relief] real-time event".[22] Had more access to the internet been readily available then this might have been used more extensively. For instance the National Command Element staff were often required to teleconference with the NZDF and other agencies but did not have the capability to conference call.[23] Collaboration capabilities were available on APAN but without general take-up of the technology across the board and good access to high internet along with habitual use these facilities are not employable.

Of interest the NZDF were required to adhere to recover and dispose of equipment in New Zealand and were not able to leave equipment in country.[24] It is anticipated that in an HAD/DR type situation there would be significant loss of communications capabilities in country. It is not unreasonable to expect that agencies will rely on those organisations that have significant resources available, such as the NZDF, to provide them with access to communications capabilities in the short term. Should the NZDF be deployed for a short period of time, consideration might be given to leaving an IT presence in the affected country to enable contributing agencies to aid the ongoing recovery, after the withdrawal of primary responders such as the NZDF. Withdrawing IT systems early could potentially cripple the communications capabilities of smaller agencies until such time as

[21] Ibid., F-15.

[22] Ibid.

[23] Ibid

[24] Ibid F-2.

the local and international telecommunication providers were able to establish effective systems in-country.

Overall Exercise Tropic Twilight seemed to be a good exercise to practice the deployment and recovery aspects of the NZDF involvement in the exercise but it did not provide and environment to test the multi-agency operations aspects of an HA/DR situation. Given the situation where the NZDF would have to respond to a real incident there would be multiple agencies all requiring to coordinate their activities, including local government and agencies such as police. The NZDF currently uses email and voice communications but during the exercise this has shown to be limited in its ability to provide real information sharing and collaboration, especially given the different systems each agency is likely to use. The internet was suggested as a good common medium and open source web tools were explored as a possible option for coordination, collaboration and information sharing. The infrastructure was intact so there was no real problems communicating with the local population which is unlikely to be the case in a disaster and the NZDF, with its extensive resources and skilled people, may need to be prepared to establish communications in support multiple agencies in a multi-agency situation.

The doctrinal NZDF response in a local HA/DR event is subtly different from that for an overseas event. The Contingency Plan AWHINA[25] details the likely NZDF response to a local disaster in the same way Contingency Plan Pacific Relief does for an overseas disaster. The Ministry of Civil Defence and Emergency Management (MCDEM) has primary responsibility for coordinating response and recovery tasks in the event of any Civil Defence emergency. Plan AWHINA details how the NZDF will respond as a supporting agency.[26] The NZDF response to disasters varies based on the level of the emergency. There is a high level of discretion when responding to small disasters and the deployed forces can operate independently based on the overall intent of the Chief of Defence Force. Should the emergency reach the state of a national emergency the NZDF will respond as a coordinated force and, due to the nature of the event, they will be

[25] New Zealand Defence Force, New Zealand Joint Service Plan No 102: Plan Awhina." DFO 91(1) (Wellington: New Zealand Defence Force, 10 August 2011).

[26] Ibid., 5.

coordinated centrally by MCDEM and have to liaise with multiple agencies, definitely at the national level and possibly at the international level.[27] It is at this higher level that the NZDF response will be considered.

According to Contingency Plan Awhina the NZDF will conduct a number of tasks and activities. The National Crisis Management Centre (NCMC), usually in Wellington, will be provided with NZDF Liaison Officers. Forces will be activated and controlled from the HQ JFNZ and local Liaison Officers will be deployed to Civil Defence Emergency Management (CDEM) Groups in the areas where NZDF force elements will be deployed.[28] While the NZDF expects to command and control the forces hierarchically from the Chief of Defence Force through the Commander Joint Forces, the deployment of Liaison Officers at multiple levels recognises the need to coordinate horizontally in a networked fashion but keeping "the appropriate chain of command... ...informed as soon as possible."[29] The NCMC is the hub for the operation with the NZDF interfacing at this level through links into SCI Branch and HQ Joint Forces New Zealand.

The NCMC operates an independent system that is not connected to the NZDF networks. Again, as was the case with Pacific Relief, the communications between the NZDF and the NCMC is through the use of telephones and email.[30] There is no evidence of the intended use of collaboration tools across multiple agencies or the use of any CIS tools more advanced than email. While Liaison Officers are deployed there is no deliberate articulated plan to establish and maintain interconnected networks between the multiple government agencies and to make use of collaboration or information sharing tools. In order to see how the NZ Defence Force responds to an HA/DR situation in NZ the response to a major earthquake in Christchurch will be used as a case study.

At 1251 on 22 February 2011 Christchurch suffered a large earthquake of magnitude 6.3 which caused significant damage and loss of life mainly in the Christchurch central

[27] Ibid., 9.

[28] Ibid., 12-13.

[29] Ibid., 13.

[30] Ibid., 16.

business district (CBD), but also across the wider region. The NZDF were starting a large exercise, Exercise Southern Katipo, in the area, and had significant military resources including Army troops and equipment as well as HMNZS Canterbury located at Lyttleton near Christchurch itself. The exercise was cancelled and the NZDF was re-tasked to assist with the relief efforts in Christchurch including assisting the NZ Police in establishing a cordon around the CBD and security patrols around the city, medical support, accommodation, food for the Police and Fire Service, transport, provision of fresh water and liaison tasks[31]. The support represented a very significant response to a natural disaster relief support operation for the NZDF and should provide valuable command and control lessons learnt.

The basic NZDF hierarchical structures deployed on the operation were vital.[32] The ability to operate with HQ at various levels was essential for managing the large numbers of deployed people and overall the command and control process in place from a structural perspective were effective. The structures most used were the Platoon sized (around 30 people) and Company sized (usually 3-4 platoons for a total of about 100-120 people). This structure is tried and true and allows for effective management of soldiers. Any use of CIS to augment command and control should look to support this structure rather than undermine it while allowing for increased situational awareness and networking. This enabled the organisation to effectively integrate with other organisations such as the police.

Integration of NZDF and NZ Police Command was achieved by integrating at the company and platoon level.[33] Effective coordination and liaison was achieved through the co-location of networks. As will be outlined below the ability to communicate between the NZDF was limited so physical co-location was essential. What is clear from this however is that it would enhance command and control if NZDF elements at the Platoon and Company level were able to integrate at the same level without necessarily needing to

[31] NZCTC, "Lessons Learnt Collection: Operation Christchurch Earthquake February 2011", Post Activity Report, (Wellington: New Zealand Defence Force, 20 June 2011), 1.

[32] Ibid., 2-3.

[33] Ibid., 3.

collocate should collocation become a challenge for any reason. This essentially allows the various hierarchical organisations deployed at the crisis to network together and keep each other situational aware and exchanging information in a network fashion.

There could be a time delay in establishing a Joint Forces Deployed HQ as the airport was closed for 24 hours.[34] It was noted that had the forces not been deployed in Lyttleton Harbour aboard the HMNZS Canterbury the response time would have been a lot longer. There is therefore a need to make sure that forces can become quickly up to date and functional in their concentration areas and then step forward to the can establish virtually and then transition. This could suggest two things. Firstly that the HQ involved need to be situational aware before they deploy so that they can prepare adequately for the task and become situational aware prior to deployment and that they are able to remain situational aware during the deployment and establishment in the area. The networks have to exist before the situation, not be established during it if possible. The networks also have to be able to be established and re-established quickly and easily. These networks have to be open and available to all responders because there are a number of nodes in the network .

The extensive use of liaison officers including Canterbury EOC, Christchurch Emergency Control Centre (ECC), New Zealand Police, Urban Search and Rescue HQ and Canterbury District Health Board indicated just how big the network was that the NZDF was part of.[35] The response to the Christchurch earthquake was not so much a series of hierarchical forces centrally coordinated from the NCMC. It was a large network of interconnected nodes at multiple levels, connected in this instance by Liaison Officers. These Liaison Officers relied on cell phones and these were intermittent and therefore unreliable.[36] With the intermittent cell phone usage the network often relied on physical liaison through face to face contact and in some incidences, when the CIS was deployed and established, by email. Because the networks of the individual organisations were not

[34] Ibid.

[35] Ibid., 3-4.

[36] Ibid., 4.

connected (there was no evidence of inter-organisation communication other than cell phones) this should mean that there should be evidence of confusion between organisations.

It can be seen, when examining the lessons learnt, that, while the hierarchical organisations within the separate organisations were effective, there was confusion along the boundaries. Communication between the three services (Naval, Land and Air) and between the military and civilian organisations was limited, mainly due to the lack of interoperability. There were multiple military HQ deployed and these were not integrated which created confusion and highlighted limited interoperability between the services.[37] Coordination of Air was disparate and not through command chain. The land commander in Christchurch did not have control or information awareness of tasks allocated to Air Force assets.[38] There was no standing reliable communications link between the Canterbury and Land Elements.[39] There was a lack of interoperability between the NZDF and OGA, IO, NGOs and local private companies and enterprises.[40] This highlights several key aspects. Firstly the establishment of a network is a priority, as illustrated by the extensive deployment of Liaison Officers. Secondly it is clear that networks need to exist prior to disasters or be able to be quickly established particularly between habitual partners and these networks need to exist across organisational boundaries and need to facilitate information sharing and situational awareness information. The networks have to be easily extended to incorporate non-habitual partners, in this case such as the local Christchurch private companies and enterprises. Finally the network has to exist outside of the local infrastructure. It has to be established in the incident site in every location that needs to communicate and it has to be open to multiple organisations.

[37] Ibid., 4-5.

[38] Ibid., 7.

[39] Ibid., 4-5.

[40] Ibid.

Network communications established from the Commanders at the Military Command Posts relied heavily on cell phone communications which led to slow passage of information. This led to limits on the use of military forces because there was no specific way to create a common operating picture or situational awareness and understanding of the commander's intent was limited due to slow passage of information.[41] Commanders at the lower level seemed reluctant to make independent decisions without full awareness of the intent. Traditional military forces make use of highly secure expensive radio communications but, as discussed earlier, due to the task the forces were dispersed much more widely and in smaller groups than normal. The availability of radios would have been limited and the management of secure, expensive radio systems would have been a significant burden, if not impossible. Some units did not have organic radio systems, such as the part time territorial soldiers, and the dispersed nature of the forces made communications challenging.[42] This led to the use of cell phones however these as stated earlier were intermittent, due to severe stress on the infrastructure.

Some Headquarters were overwhelmed with information while some elements were starved from the lack of it. There were large amounts of information to deal with and manual systems were used to process this information. The ability to handle this information was limited and this meant handovers between shifts were difficult and there was a likelihood of omissions or loss of important information.[43] At the same time there was a lack of information at the lower levels and this information deficit prevented the Liaison Officers from understanding the big picture.[44] There was an attempt to alleviate this by using an intranet webpage to create a central repository for relevant information but this was stored on a secure internal military system (DIXS) so it was not available to anyone other than those military personnel that could access this system.[45] This was

[41] Ibid., 10.

[42] Ibid., 12.

[43] HQ Joint Forces New Zealand, "Op Christchurch Earthquake: Communications Observations Pd 22 Feb - 4 Mar 2011." Lessons Learnt. Wellington: New Zealand Defence Force, 19 April 2011 2011, 3.

[44] Ibid., 11.

[45] Ibid.

mainly at the military Command Posts. It is possible that this same information was repeated across a number of organisations and a central repository for all agencies would have enhanced the sharing of this critical information and ensured all that needed it had access to it. This information could not be disseminated down to the smaller teams and Liaison Officers as they were relying on cell phone communications.

Because the forces were deployed as individuals and small groups at each level communications was essential. The use of cell phones as a communications medium however was found to be lacking. Cell phone networks were fragile and overloaded easily.[46] This demonstrates a clear need to establish a network that cheap devices can easily attach to. Open systems such as the Internet and wireless networks can be just such a network. Internet based networks are in significant use around many cities in New Zealand and it is a simple matter to connect most smart cell phones, computers and other devices to hotspots to join an Internet based network. Scaled and resourced sufficiently a network consisting of interconnected hotspots at key locations and a connection to the internet might provide an opportunity to establish a connected network of devices that a physical network of organisations may be able to make use of.

At least one hotspot was set up after some time into the operation. Satellite communications proved to be insufficiently resourced in this situation. Flyaway type systems were performing badly for a number of reasons. The bandwidth was limited and the collocation of a number of the same types of systems by multiple agencies created interference reducing the overall effectiveness of the systems for all parties as each system competes with the others.[47] This was alleviated by taking a collaborative approach and providing multiple access to one satellite or two satellite systems for a small number of the responders and defence personnel, urban search and rescue in particular, in a central location by using satellite internet providers and a Wi-Fi hotspot

[46] NZCTC, Post Activiy Report, 12.

[47] (HQ Joint Forces New Zealand, Lessons Learnt, 4-5.

and cable connections.[48] This idea could be expanded on to enable a more collaborative approach to the provision of network services and enable a better networked approach.

The NZDF did make some use of the internet and social networking during the disaster relief operation in Christchurch. It made extensive use of Facebook but this was used by the communications unit to communicate with the media, not for command and control or coordination.[49] Email was used extensively both across the internet to other organisations and through a secure email transfer system called Seemail, using the internet as a medium between government departments. The establishment of networks using technology was almost exclusively concentrated within individual services to meet their own internal command and control needs, not on the establishment of networks across organisational boundaries.

[48] Ibid., 2.

[49] NZCTC, Post Activity Report, 6.

The US Experiences – Haiti Case Study: A Web 2.0 Based Response?

The US Military response to Haiti is a good case study. Arguable it is the first major deployment of forces where significant use of Web 2.0 technology was used. It was also a deployment where the use of Web 2.0 technology was not pre-planned. As such the deployment highlighted a number of successes, particularly around networking and the utilisation of Web 2.0 and networking concepts. It also had a number of difficulties that highlight aspects that need to be addressed to ensure the implementation of theses concepts can be maximised. The successful aspects and the problems will be examined in order to draw out the critical aspects that need to be considered to gain maximum benefit from the use of CIS capabilities in a disaster relief scenario.

On 29th August 2005 there was a magnitude 7.0 earthquake in Haiti which caused destruction throughout the country and significant loss of life. The death toll was well over 200 000 and over 1 million people were displaced. The Joint Task Force Commander gave some very clear direction to support the deployment into Haiti.

The JTF Haiti Commander's Intent[50] was to enable mobility for delivery of relief supplies, equipment, and personnel; support unity of effort by coordinating and collaborating with all partners; operate jointly and combined with all military forces in Haiti and execute a pro-active Strategic Communication program. His end-state was to have minimised immediate human suffering; provided survivors provided food, water; controled the critical health situations; provided survivors with essential medical care; ensured MINUSTAH[51] and GoH[52] authorities were capable of maintaining civil order and that GoH, UN and USAID had capacity in place to sustain long term recovery before the U.S. Forces Redeployed.

The US forces deployed significant military assets into Haiti to achieve this intent and were involved in many aspects of the relief operation in the country. There are several

[50] Walsh, Civilian Response Stakeholders.

[51] United Nations Stabilization Mission in Haiti

[52] Government of Haiti

aspects to the intent that signal a significant reliance on CIS. Firstly the focus is internal. Communications internally are critical to enable the coordination of the military effort to achieve the delivery of the military effort as you might expect. What is of interest is the external focus and the strong language used to indicated a focus on collaborating with partners, operating jointly with all military forces in Haiti and executing a strategic communications program. Without the enhanced CIS used in Haiti in the innovative ways it was used this intent would not likely have been met. Haiti showed some significant use of aspects of Web 2.0 networking to achieve success. Not everything worked however and there were also significant problems with the implementation, particularly around the ad hoc nature and unplanned employment of Web 2.0 capabilities. The use of Web 2.0 capabilities almost seem to grow with the mission as it evolved.

When the forces deployed they experienced first hand the "fog of relief". In the first week they were virtually the only people in country who had communications, food/water, transportation, tents and security[53]. They distributed nearly 45 000 hand crank radios to allow survivors to receive news and information. They also "provided internet and phone services to virtually every arriving unit and aid organization that showed up... ...without a plan."[54] The support provided by the US Forces in Haiti was a significant change from anything seen previously. They applied non-traditional and ad hoc approaches that "have the potential to be institutionalized as best practice for future crisis response models and response capabilities."[55] It is perhaps this fog and the innovation of a number of people in the mission response that moved the military to employ Web 2.0 type technologies.

Most operations are fought on classified systems that prevent the enemy from gaining valuable information. This has several effects, firstly the information moves more slowly and to a small audience because the systems used to encrypt data are expensive and restricted in their use, often restricted to individual nations or allied groups, for example

[53] Buck Elton, "Haiti: Boots on the Ground Perspective." In *Small Wars Journal*, 2009, 2.

[54] Ibid

[55] Wentz, Haiti Information and Communications Observations, 35.

the five-eyes community.[56] As a consequence most disaster relief partners, including embassy staff cannot see or access classified material.[57] Military personnel on the ground found the ability to pass timely and accurate information was as important as the availability of food and water.[58] They found that cell phones, and in particular blackberries became the primary means of communication as they were the most reliable means to correspond with the groupings in support of the operation. The Brigade Combat Team (BCT) in Port-au-Prince even purchased unclassified hard drives to place into their computers to allow personnel without security clearances access to their computer systems.[59]

The concept of information being as important as other commodities is a new concept and an extremely important one. It alters the mindset of the deploying forces and changes priorities and the focus and therefore redirects resources to this area. Larry Wentz advocates seeing ICT as an "essential service" and "critical infrastructure" but criticises the United States Government for not treating it this way.[60] He goes on to advocate an approach that plans ICT services as a key aspect of any response and recovery effort and remarks that the ICT support packages are more than just "fly away kits".[61] The military focus tends to be on the exchange of Liaison Officers to various organisations on the ground and providing these Liaison Officers with fly away kits to enable them to get access into military systems. While this approach is effective and important, eventually the force runs out of liaison officers and fly away kits and there is invariably more liaison requirements than liaison officers. A better solution seems to be the development of networks and opening up networks across boundaries to enable better information sharing and collaboration. In essence this opening up and willingness

[56] Five eyes refers to the Australia, Britain, Canada, New Zealand, and United States of America grouping.

[57] Kelly Webster, "Lessons From a MIlitary Humanitarian in Port-au_prince, Haiti." In Small Wars Journal, 2010, 1-2.

[58] Ibid., 1-2.

[59] Ibid., 2.

[60] Wentz, Haiti Information and Communications Observations, 31.

[61] Ibid.

to share information forms the basis for the move to using Web 2.0 capabilities on HA/DR missions.

The non-military responders were not much better prepared and only considered their own communications requirements. Most responders brought their own equipment including radios, cell phones and Internet satellite systems such as BGAN. There was no agreed response architecture, no spectrum management and coordination, no agreed on processes and procedures to guide the implementation and possible integration of independent networks to establish a wide area mission network to support mission activities.[62] The proliferation of satellite terminals, satellite phones, Wi-Fi networks and various radio and cell communications caused communications congestion and interference[63]. Without any coordinated operation management of ICT assets the individual networks operated at sub optimum efforts and the ability to collaborate and share information would have suffered overall due to the lack of integration. Larry Wentz notes that "most responders agreed that ICT is important in helping save lives and to help coordinate relief efforts but few treat it as an essential service beyond meeting their own needs."[64] This is exactly the mindset that the military brings. It is there as a service to allow the military to achieve its mission and the consideration of it as an essential service to aid in the response effort, including wider networking across multiple agencies has yet to become a common operating procedure. The effects that the existing ICT systems had in Haiti when information sharing and collaboration was achieved were significant.

The forces on the ground found that collaboration and networking created a significant advantage when responding to crisis in Haiti. This collaboration as the "eBay effect", named after the famous online auction website eBay.[65] The term "eBay effect" describes the solutions developed to solve a resourcing problem found in Haiti, utilising Web 2.0 concepts and capabilities. The US Government agencies, the international community

[62] Ibid., 8.

[63] Ibid., 20.

[64] Ibid., 8.

[65] Ibid., 2-3.

and NGOs all brought significant resources to the Haiti disaster relief operation. The problem or challenge that arose was to know where to apply these significant resources, matching supply with demand. The BCT developed a common operating picture based on Microsoft Excel spreadsheet that allowed the UN Office for the Coordination of Humanitarian Affairs (OCHA) to display information on Google Earth to create a humanitarian assistance common operating picture (HA COP)[66] to anyone who wanted access to the information[67]. This enabled suppliers and consumers of humanitarian aid to link together and allowed the resources to be allocated in a more effective way.

The All Partners Access Network (APAN) or as it was known then the Asia Pacific Access Network was used for online collaboration. APAN describes itself as an unclassified, non-dot-mil network providing interoperability and connectivity among partners over a common platform. [68] APAN is designed to foster information exchange and collaboration between the United States Department of Defence (DoD) and any external country, organization, agency or individual that does not have ready access to traditional DoD systems and networks. APAN was used as an information sharing portal "outside the wire".[69] APAN is a system that exists on the Internet and as such is able to be accessed by a wide variety of organisations and individuals as it operated without the same security restrictions as other military systems. It provided basic information sharing capabilities such as forums, blogs, media gallery, map, images, chat and wikis and is a Web 2.0 enabler. It was used for focus groups, situation updates/reports, mission briefs and requests for information/assistance. The particular benefits of APAN were the ability to operate a cut down version in bandwidth constrained environment and being hosted on the Internet allowed it to be accessed by a wide variety of people, not just those on a fixed, closed system. It was available to everyone who wanted to use it. APAN in the first three weeks attracted 1800 users and was USSOUTHCOM's chief means of sharing

[66] This can be accesses at http://oneresponse.info. With military input the UN database was populated with over 1500 separate data points using the OCHA web based application (Webster 2010, 3).

[67] Webster, Lessons from a Military Humanitarian in Port-Au-Prince, Haiti, 3.

[68] US Department of Defence, *All Partners Acess Network,* http://community.apan.org/.

[69] Wentz, Haiti Information and Communcations Observations, 32.

information outside of his command domain. USSOUTHCOM responded to requests for assistance, maintained situational awareness through user updates and shared imagery with the international community using APAN.[70]

The military, in most cases, is a supporting agency, not the lead agency. For Exercise Tropic Twilight, MFAT was the lead agency. For Operation Christchurch Earth Quake the lead agency was Civil Defence. In the case of Haiti, where there were multiple national and international organisations along with the UN and a crippled local government it was very hard to determine who, if anyone had the lead. The military has to take a supporting guiding role but it also has significant capabilities and skills including logistics, transport, communications, planning expertise to name a few. As such it is going to be expected to play a significant part in any recovery role. This means that the focus is on collaboration and working with others. As US Army General Simeon Tombitas said about Haiti, "instead of the from-the-military perspective of commanding and controlling, our forte now has to be coordinating and collaboration. In order to get things done, because we are not the lead agency, we have to work with and through others."[71] Major Webster also observed that when "faced with a humanitarian crisis of historic proportions, differences and longstanding misperceptions quickly faded into the background. Overtime, several of the NGOs became the [Brigade Combat Team's] closet relief partners."[72] As can be seen, working with and collaborating with other organisations becomes the prime responsibility and way of operating for all responders, through a process of networking.

Discussions with key New Zealand Defence Force personnel about Exercise Tropic Twilight confirmed this. Lieutenant Colonel Hart, who commanded the forces deployed on the exercise in 2010 confirmed that he took very much a supporting role, sitting in the background while MFAT and local Tuvalu Government Officials worked through the

[70] Douglas Fraserand Wendell Hertzelle, "Haiti Relief: An international Effort Enabled through Air, Space, and Cyberspace." In Air and Space Power Journal, 2010: 5-12, 9.

[71] Christopher Slagh, Managing Chaos, 140 Characters at a time: How the Usage of Social Media in the 2010 Haiti Crisis Enhanced Disaster Relief, (MA Thesis, Washington, DC: Georgetown University, 2010), 42.

[72] Webster, Lessons from a Military Humanitarian in Port-Au-Prince, 2.

details and requirements of the Exercise.[73] The lead planner for the exercise commented on a remark from the Red Cross representative that the NGOs were becoming more military in their outlook and the military was becoming more like an NGO.[74] What was meant by this remark was that the NGOs were becoming more organised and self supporting and the military were becoming more collaborative and becoming partner oriented in their approach to operations such as HA/DR operations. The collaborative approach with ambiguous authority is likely to be an ongoing situation in these types of operations.

Collaboration, where it was used, provided significant success. One such example was a Nethope/Inveneo collaboration[75]. Inveneo's long distance Wi-Fi links connected NetHope member organisations enabling dozens of nodes to utilise the same broadband internet link. Rather than a trying to independently deploy their own capabilities the NetHope group was able to get access to high speed Internet to eleven relief agency locations with a significant jump in capacity.[76] This collaborative approach allows for the best utilisation of existing bandwidth and capacity to ensure agencies are able to get usable capability without causing interference or degrading other's capabilities. The military have the expertise and a capacity to provide assistance in a number of these areas. They have expertise in spectrum management, often with experience in de-conflicting radio and satellite communications in large scale deployed environments. They also have the technical expertise to build large networks and have experience in doing this rapidly. These skills have the ability to reduce communications issues early on in a crisis event such as Haiti.

Open source civilian technology community and social networking support was unprecedented and extremely effective during the Haiti operation. Text messaging, while not always classified as social media, was arguably one such example. Text messaging

[73]Todd Hart, interview by Liam Jones, Exercise Tropic Twilight, 2012.

[74] Walters, interviewed by Liam Jones, Exercise Tropic Twilight, 2012.

[75] Inveneo Haiti Emergency Deployment. September 2009. http://www.inveneo.org/mission/

[76] Wentz, Haiti Information and Communications Observations, 17-18.

was used extensively as the primary means of communications when using cell phones.[77] Cell phone text messaging was also used extensively to for trapped individuals to make contact to bring attention to their plight. The Mission 4636 service allowed SMS data to be collected and assessed by thousands of volunteers to enable the provision of data to many systems. 4636 was a number established to text to and people on the ground could text to this number with all their immediate needs (medical care, food, water and shelter). Of particular importance was the ability of these volunteers to understand the language and translate from Creole and French to English.[78] Another example is the use of Voila Mobile phones and Haitian radio outreach. Daniel Kedar, was an ex-Israeli military member in Haiti who ended up working to assist the Israeli military efforts in Haiti. He provided a Voila phone number over the radio and this became the number for people to get in touch. The "Viola phones... ...was the only way he could manage control and command... ...during the critical first 72 hours. As the best communications Command Center working in the initial days Kedar dispatched not only Israeli forces, but also Russian, French and Greek rescue teams. Without the Voila phones... ...rescuers would have been 'totally lost'".[79] Essentially the Viola phone system had become an indispensable command and control tool for the effective tasking of a number of military organisations.

Social networking provided significant assistance enhancing on the ground operations. It dramatically improved the ability to locate missing people and provided intelligence to enable critical infrastructure repair efforts to be focused. Social networking applications, such as Facebook and twitter, were used to update on the status of family members. The ground truth was also reported by those that still had access to internet and power. Open source mapping was a critical to maintaining situational awareness with many online portals providing facilities to update data to enhance situational awareness. Blogs also provided critical information, especially for incoming personnel. Kate Moon, a physician's assistant said that "the UN representative at our clinic blogged daily to reach

[77] Ibid., 2.

[78] Ibid., 10.

[79] Ibid., 11.

out to groups coming in following ours. New Teams coming in were significantly better prepared than we had been; they knew what to bring, what they were going to do, what their roles would be. The blogging was amazingly helpful."[80]

In effect social networking enhanced Command and Control on the ground. It provided much needed intelligence and enabled information gathering from the wider community. The use of mission 4636 enabled information gathering that would not have otherwise occurred or that would have occurred at a much slower rate. This enabled the application of resources to issues at a much more rapid rate as is critical in any HA/DR situation. It also provided the tools to provide situational awareness through graphical mapping, but more importantly, because the information was available through open social media, it enhanced the overall affect on the ground through wide dissemination. Active use of this for command and control can be seen through the tasking of Israeli forces through the use of the Viola Cell phone network. The main power of the use of Web 2.0 social networking capabilities and harnessing the wider community to provide detailed situational awareness and to continue to maintain and update this awareness to keep it up to date. It also provided rapid and ongoing access to critical capabilities, such as language translation, a capability that would have been hard to provide otherwise and one that could have potentially slowed down the overall access to intelligence gathered from the local community had the responders on the ground had to rely on internal translation capabilities.

One organisation that enabled the use of crowd-sourcing data was Ushahidi[81], an open source internet based program. Ushahidi is an open source crisis mapping software originally developed in Kenya which provided a way to capture organise and share critical information coming directly from a variety of Web 2.0 sources including text message,

[80] Slagh, Managing Chaos 140 Characters at a time, 16-19.

[81] Ushahidi means "testimony" in Swahili and was crafted in the wake of the 2007-08 Kenyan postelection violence by a network of volunteers and powered by a community of citizen reporters and bloggers to give every day Kenyans a way to report incidents of violence using tools such as mobile phones, to archive news reports to create a historical record of the conflict and to provide the Kenyan community with up-to-date information about violence. (Heinzelman and Waters 2010, 4-5)

blogs, twitter and Facebook.[82] Disasters, such as Haiti have significant impact on the local geography and can make maps pretty much irrelevant and outdated. Roads are blocked by debris or destroyed, navigation points and landmarks are destroyed or changed and places of interest (such as IDP camps and hospitals) are established or change location. By use of collaborative platforms such as Ushahidi volunteers, geographical intelligence, mapping experts, the military and other international organisations were able to update maps of Haiti rapidly and accurately to assist responders on the ground. Organisations such as the World Bank, GeoEye and the US Government provided geographical information far superior to the original maps from Yahoo that were originally made available.[83] The main point here is the collaborative nature of the establishment of these maps across a vast range of organisations that are not normally used to working together. Military organisations and the US Government were prepared and able to provide information to the collaborative effort in order to achieve the overall aim to establish and maintain an accurate ground picture, which in turn aids situational awareness and command and control capabilities overall.

The US Marines made specific use of social of social networking while in Haiti in close cooperation with Ushahidi. Ushahidi, as a mapping platform, was critical to the US Marine activities. A civilian analyst working for the Marine Corps, Craig Clarke utilised Ushahidi and used information sourced from social networks and media outlets such as blogs, Twitter, Facebook and other major websites. He was able to translate this from Ushahidi format to Google Earth format to make it easier to distribute over the narrow bandwidths in use by the Marine Corps communications systems. The Marine Corps used this Ushahidi data to work out where best to deliver support. One such example provided by Clarke "involved reports from a displaced persons camp... ...that safe drinking water was in short supply. Once they received the information, the Marines delivered water to

[82] Jessica Heinzelman and Carol Waters, Crowdsourcing Crisis Information in Disaster Affected Haiti. Special Report, (Washington, DC: United States Institute of Peace, 2010), 1.

[83] Ibid., 11.

the camp and distributed devices to sanitize drinking water."[84] Another example given was the detection of violence and roadblocks the needed to be policed to ensure aid was able to reach victims. The US Marines realised that they needed to adapt in this situation in order to respond effectively so modified their command and control approach, utilising a civilian open-source tool as a command and control tool to allow them to effectively respond to the needs on the ground. Not only that they were also able to adapt the tool, through the use of in-house CIS expertise to suit their own circumstances adapting the Usahidi tool to their low bandwidth environment and integrating it into their command and control capabilities.

Radio proved to be an important command and control tool in the absence of more advanced capabilities. The "radio's importance as an information source was amplified because it complimented other critical information sources. Community networks... ...were able to distribute messages more effectively by working with radio. Other forms of media such as text messaging and social networking combined with radio improved delivery of key information."[85] With the use of radio key messages could be continually broadcast. This is particularly important in areas where other communications have been damaged or destroyed (such as the internet infrastructure in Haiti) or where more advanced technology might not be as prevalent. This was augmented by the military with the distribution of hand-cranked radios[86] to support the ability of the local community to receive messages. This highlights the critical role local communications play in the community. Many islands in the Pacific utilise HF radio networks. Also many communities now make use of the internet and cell phones as their primary means of communication. Warrant Officer Lancaster commenting on his experiences during the Christchurch Earthquake made reference to the need for the military to have access to

[84] Anne Nelson, Ivan Sigal, and Dean Zambrano, Media, Information Systems and Communities: Lessons from Haiti, Report based on International Relief Agencies Roundtable Discussion, (Miami: Knight Foundation, 2010), 13-14.

[85] Ibid., 11.

[86] Elton , Haiti: Boots on the Ground Perspective, 2.

these communication systems.[87] They have become an essential command and control situational awareness tool and a valuable source of information. Many of these tools are now utilising RSS[88] type mechanisms that allow the information to be ported directly into command and control tools automatically. In order to achieve this, however, the architecture and networks of the military organisation have to be flexible enough to access these sources of information.

Information sharing by the military was another area that saw benefit to the overall relief effort. This was a step forward from previous situations in that systems considered classified were able to supply imagery and support to the whole relief effort, the key point being that information contained within the military CIS zone was able to be moved outside of this protective area and shared with un-cleared non-military or non-government people. Haiti marked the first time the Predator Remote Piloted Aircraft was deployed in support of humanitarian operations. It was used to provide vital situational awareness and was able to pinpoint potential spots that might cause difficulties for humanitarian relief activities. What was of particular use was the ability to take this imagery, along with imagery from other surveillance assets and combine this with historical satellite imagery taken by Google to create a three dimensional picture of the Haiti earthquake effects[89]. This demonstrated a number of potential aspects to making use of CIS. Firstly the ability to declassify and distribute military data and secondly the ability for USSOUTHCOM to partner with commercial entities such as Google and produce an extremely important and useful product in a short space of time in support of the relief efforts.

Many of these initiatives were taken to overcome the initial problems found on the ground, many of which were significant. The response to Haiti was very large and the amount of chaos was commensurate with the size of the response. Larry Wentz describes

[87] Lancaster, interview.

[88] Really Simple Syndication. A standardised method of presenting information on the web that allows multiple information sources to be automatically aggregated into one place.

[89] Fraser and Hertzelle, Haiti Relief: An international Effort Enabled through Air, Space, and Cyberspace, 9.

this as "lots of noise in the system".[90] By this he is talking about the amount of information in the system and the lack of ability to process it which makes simple tasks, such as developing an accurate contact list, very difficult. He states that the ability to access significant chunks of open source data meant that there were multiple incidents of duplicate, conflicting and sometimes outdated information. Email and phone communications, became the primary means of communication, as was observed in the Christchurch Earthquake. Information overload from the overwhelming number of emails made information management almost impossible and there was a proliferation of internet based portals which meant many hours of surfing to find important information. Power was also a challenge with many organisations moving to manual means to collect and disseminate information such as the use of written forms. Cell phones provided a poor level of service but remained the primary source of communications for many, probably because it was a universal standard and everyone had a cell phone.

Haiti showed that there is significant risk to introducing new technologies in real world crisis situations and they need to be managed carefully. Users in stressful environments need to be managed and new initiatives can cause more problems than they fix. In a stressful environment if a system is not easy to use, does not work reliably or there are anomalies in its operation users do not respond well. Wentz observes that "once a user decides not to use the capability anymore it is very hard to win them back."[91] APAN required a registration process with no ability to browse information as a guest. This meant that many users preferred the UNOCHA OneResponse and ReliefWeb or the NATO CIMICWEB as an information source.[92] Knowledge about which website was being used and "there were many users who said they had never heard of APAN and for those that did, most did not use it."[93] So while online information sharing and collaboration sites might be seen as a "silver bullet" it is not that straight forward and there needs to be

[90] Wentz, Haiti Information and Communications Observations, 9.

[91] Ibid., 12.

[92] Ibid.

[93] Ibid.

some form of careful information management plan put in place allowing for multiple agencies to operate in a more collaborative way.

There was no comprehensive, centralised strategy or architecture guiding the deployment of CIS. This led to a deployment of stove-piped capabilities, supporting individual organisations and a rapid proliferation of independent crisis response web sites.[94] What was needed was some form of federated network of CIS or ICT organisations to improve the overall coordination of responders and enable a collaborative approach to the provision of CIS. This was observed in part in Haiti where the UN Emergency Telecommunications Cluster (ETC) attempted to improve coordination.[95] The UN operates a cluster system where individual UN organisations are given coordination responsibility to coordinate specific functional groups. UN ETC is given the responsibility to manage the telecommunications cluster. There were some sensitivities to the military participating in NGO based groups such as the ETC but the ETC leader was "most interested in having the [Joint Task Force – Haiti J6] participate and extended and invitation to have the J6 come visit the [World Food Program]/ETC compound."[96] In any HA/DR operation communications have been shown to be a critical aspect and coordination of communications is a significant factor. Without any agreed central coordination method the ability to operate communications effectively is going to suffer.

When there is limited coordination in the communications area issues arise and these were quite evident in Haiti. In a concentrated environment, with multiple responders, access to telecommunications services and to the radio spectrum becomes a real challenge. With the arrival of teams of responders comes a massive quantity of radios, satellites and cell phones. All this equipment puts demand on bandwidth and the potential to misuse spectrum and satellite bandwidth is very high. The proper process is to apply for and be allocated spectrum but in the case of a disaster such as Haiti, where

[94] Ibid., 15.

[95] Ibid.

[96] Ibid., 21.

the government apparatus is struggling to function the temptation to operate without such approval and therefore compound the issue is great. Wentz comments in his report that "often one could see several BGANs and VSATs within eye sight of each other and there were many cases of radio link interference on both voice and data networks."[97] This was particularly evident during US East Coast prime network broadcast times where peak satellite usage caused significant slowing of services over the period. The use of services such as BGAN satellite should be used with caution because their ease of use means the majority of responders will likely want to use the same services. This is fine during exercises with limited participants such as Exercise Tropic Twilight but it wasn't until the NZDF deployed in a BGAN heavy environment with the Christchurch Earthquake that they too observed a significant degradation in services[98]. In order to overcome these issues it is important to take a collaborative approach rather than a competitive approach to operating communication systems. Where the local government mechanisms are operating then the appropriate spectrum management and allocation needs to be followed. In the case of Haiti the government agency, Conatel, was non-functional then overwhelmed and the collaborative approach was tried with the UN cluster system trying to establish some form of control. Prioritising the use of cell phones is possible and can also be considered to ensure that those that need it are able to use this form of communications can get access to it, though this is an activity that only local government and local telecommunications companies can achieve and would take some pre-planning to achieve. There was limited success and ongoing communication issues were the norm in the initial stages.[99]

The Knight Foundation report also identifies problems. IT states that there was no "systematic technology-based connections between the media activists and the military or the large humanitarian organizations."[100] Mostly there was a dependence on personal contacts that took place on an ad hoc basis. Key facilities like Ushahidi remained

[97] Ibid., 15.

[98] Lancaster, interview.

[99] Wentz, Haiti Information and Communications Observations, 14-15.

[100] Nelson, Sigal and Zambrano, Media, Information Systems and Communities: Lessons from Haiti, 14.

relatively unknown. US Air Force Colonel Lee Harvis was relying on US Embassy GPS Coordinates to enable him to organise aero-medical evacuations. These proved to be inaccurate and he was forced to drive through the town to remap all the key facilities and rescue sites.[101] Had he had access to information systems such as Ushahidi he may not have needed to go to these efforts to gather his own data. A centralised approach to distribution of data or at the very least a centralised coordinating body, with representation from those agencies in the response may have created greater awareness of the tools in use and the availability of information.

Also identified were technical problems with systems being overloaded. Some estimates stated that SMS messages were only flowing 60-70 percent of the time. Also the nature of SMS messages mean that it is impossible to determine if a message has got through or not. Cell networks would go into sleep mode to save power resulting in backlogs of SMS messages and once the system "woke up" the backlog of messages would then overwhelm the system.[102] Sometimes these outages were for four or more hours at a time. While the cell phone systems proved to be a critical asset in a disaster relief type situation they are tenuous and fragile to use and unreliable at times. The use of SMS messaging seems to be a far more effective means of communication in these situations but the nature of the system means that the message cannot always assume to have been received by the intended recipient.

General Fraser and Major Hertzelle also identify issues. They highlighted the issue with the sheer quantity of information presented and the issues this created by highlighting comments of the USSOUTHCOM J2 (Intelligence) Officer, who said that the "huge volume of information presented the command with the challenge of mining, compiling, analyzing and disseminating both traditional and non-traditional data sources at the speed of the information environment."[103] They observed that if "we accept data from various sources, then we must take time to discern whether some of it might be

[101] Ibid.

[102] Ibid.

[103] Fraser and Hertzelle, Haiti Relief: An international Effort Enabled through Air, Space, and Cyberspace, 11.

disinformation if perceived in the wrong context. Therefore, peer review becomes important and the fusion of peer-reviewed data uploaded to a common point of reference gives participants a clearer picture of what is occurring."[104] In effect what they are saying is that data needs to be corroborated and analysed. Firstly through the use of crowd-sourcing the clustering of similar reports can be visualised by representing them graphically to pictorially show where clusters of similar reports are occurring, which could be a key indicated of ground truth. Secondly information can come from several different sources all saying a similar thing. For example an overhead picture such as a satellite or air photo in conjunction with several reports by SMS message may be enough to confirm information. However to achieve this level of capability the organisations must practice access to multiple information sources and be prepared to do it. USSOUTHCOM's comments that it is "utilizing Web 2.0 technologies such as portals, wikis, blogs, and chat rooms... ...[to build] a flatter, faster information environment for use in future relief operations"[105] would seem to indicate that it fully intends to leverage off web 2.0 technology in the future.

Larry Wentz identifies that there is a need to strengthen whole-of-government preparedness and crisis information management and international response actions, both on the military and civilian side.[106] By strengthening these capabilities the response to disaster can be better managed to enable a more effective response. It is important to look at it from both the military and civilian perspective as the skills and experience of these organisations are significantly different. Often the civilian organisations are dealing with situations that they have not been trained to respond to an have not experienced before. The military are expert planners but often have not had experience dealing in a support role with a civilian lead or with working in a multi-agency environment in a disaster relief role.

[104] Ibid.

[105] Ibid.

[106] Wentz, Haiti Information and Communications Observations, 40.

Overall the use of Web 2.0 during the response to Haiti was ad hoc trial and error. The US Forces and US Government brought with them the experiences from previous disasters including Tsunamis in the Asia and the Pacific along with their own Hurricane Katrina disaster on the US South Coast. These previous experiences had created a number of lessons learnt but as Larry Wentz notes, they were not well implemented and there is an ongoing issue in this area to capture lessons learnt. What the US Forces did find, however was that things had moved rapidly forward in the ICT world. They were able to quickly make use of newer web 2.0 technologies which led to an unprecedented level of interoperability between the military and civilian responder community. In addition there were significant mind shifts that enabled previously classified information to be shared and the integration of civil with military systems that enabled greater networking and coordination. While the response was not perfect there results were a significant advancement from previous experiences and without a doubt these initiatives saved lives on the ground that may have otherwise been lost. The closer integration and the opening up of military networks forms a basis for future HA/DR operations and the Haiti experience definitely foreshadows the future possibilities that can come from utilising strategic ICT assets more effectively in support of HA/DR activities.

It can be seen from the US experiences in Haiti that networking and the implementation of Web 2.0 technologies has to be planned and it has to be ingrained in the culture of the organisation. Networks have to pre-exist where possible and if not, responders have to understand and be comfortable with working in a Hastily Formed Network environment. It is clear from the lessons learnt from Haiti that there is an intention in the US Military, and in particular USSOUTHCOM, to move to a Web 2.0 type environment. Haiti highlighted the successes of implementing Web 2.0 concepts and technologies but also highlighted the dangers of doing so in an adhoc, unplanned fashion. The US Forces have taken a number of initiatives to change the culture of the organisation to gain significant benefit from long term strategies to exploit Web 2.0 capabilities. Initiatives such as Army Knowledge Online (AKO), command.com and NCO.com enable soldiers to ask questions, exchange information and knowledge in user communities on anything that the user community finds of interest or value have become great success stories and are adding

significant value to the organisation.[107] This shows that in order to gain any benefits, the moving to a collaborative, information sharing environment has to be done in a deliberate pre-planned manner and the culture of the organisation has to be capable of adapting to a collaborative, information sharing environment. The NZDF can learn significant lessons from the US Haiti Response. The examination of both Tropic Twilight and the Canterbury Earthquake response showed there is an under utilisation of networking and exploitation of CIS and Web 2.0 capabilities.

[107] Maryann Lawlor, "Web 2.0 Military Style" in Signal, 62, 7 (Mar 2008), 64.

Key Lessons for the NZDF

The case studies looked at so far have highlighted some important lessons that should be considered to enable the effective use of CIS capabilities during an HA/DR response that could be applicable to the NZDF. These can be broadly categorised into being prepared, having a culture that enables information sharing across organisations that are not usually used to working together, ensuring the deployment has an effective physical and conceptual network, capabilities to engage with the local population and having the ability to harness a wider population.

Being prepared to meet the collaborative CIS demands of a HA/DR deployment is key. Specific recommendations from Haiti suggest that responders that are involved in HA/DR response need to already have established coordination mechanisms. The way that ICT is employed within New Zealand and off shore needs to be planned before hand. The issues with not doing this are interference and degradation of ad hoc voice and data systems, a lack of joined up systems and therefore an overall lack of coordinated information sharing leading to ineffective allocation of resources. By coordinating across the range of responders and exercising in realistic situations standard ways of doing things can be established and agreed upon beforehand, relationships can be established and effective use of systems can be put in place. By achieving agreed coordination methods beforehand the response in a crisis can be a lot more effective and ongoing communication can be achieved before any actual event.

An effective way to achieving closer coordination between the military and other responders is through the use of preparation and simulation exercises across the spectrum of responders. As can be seen in Tropic Twilight, exercises tend to suffer from two specific issues. Firstly they have real world requirements that need to be achieved over and above the exercise objectives. Secondly they do not have the same level and number of responders that a real event attracts. The exercises, to be effective training mechanisms need to be more comprehensive than they are currently. This will enable the application and testing out of networks, inter-network connections and new ICT

capabilities to see how they fit and if they work as intended and to develop operation processes for inter-agency operations and not just intra-agency processes and procedures.

The use of internet based information sharing platforms were a significant benefit in Haiti. The Knight Foundation report also recommended that humanitarian and technology practitioners "should be proactive in promoting promising new platforms to governments, international organizations and private sector parties such as telecommunications companies."[108] By doing this it will enable the development of existing platforms to ensure they work effectively and will also remove the ambiguity about which systems do what and what systems exist at all. The APAN, Ashahidi and OneResponse, among others, were all used in Haiti and will continue to be promising capabilities into the future. Determining in advance which ones are used for what and when will go some way to removing the issues discovered in Haiti where there was significant confusion over which platforms are being used for what and by whom. Ongoing familiarisation and training prior to a crisis will also further enable their effective use once a crisis begins to unfold.

One small example of needing to be prepared is data tagging, as part of information management. This area is a small but critical function to enable better access to data. It is important to have tools, indexes and metadata tags on information to ensure users are aware of what information might be available to them. Online portals are starting to enable this with data tagging but there was no evidence of standardising or management of this information in any coordinated way. By effectively tagging data with key words that can then be used to classify and search on means that data is not lost in the white noise of the system and can be accessed in a meaningful way. In order for it to operate effectively however, it needs to be pre-planned.

Haiti also showed that there was little or no shared situational awareness between responders to enable a common understanding of what types of information is available

[108] Nelson, Sigal and Zambrano, Media, Information Systems and Communities: Lessons from Haiti,, 24

from where.[109] For example there were multiple internet portals, all of which were in use by parts of the response. Many of these portals were not known by many of the responders. Many responders, including the military, had information locked away in their own systems. This led to a duplication of effort. Organisations would likely have used old or outdated data and maps. By creating a unified or coordinated approach to the sharing and management of information this could be overcome. By decreasing the number of portals being used maybe through a mechanism of mandating or recommending specific portals for specific activities this could potentially be remedied. In addition adopting common international open architectural standards could potentially eliminate the requirement to limit the number of portals. Command and control systems and internet websites can be adapted to receive portals using standardised data interfaces such as the RSS feeds previously mentioned meaning the individual organisations can still utilise their own tools and websites but are able to import the data made available from other sources automatically with a minimum of technical work.

Stove piped and incompatible ICT systems across the responder community do not allow sharing of information between organisations.[110] In addition these systems end up with large amounts of data being moved independently, often over systems that are competing for bandwidth. This duplication of effort results in inefficient use of information and often these systems are being used without centralised coordination and management or permission from the local authorities to use the operating frequencies. There is a need to establish these functions and treat ICT as another resource that needs managing with the same effort given to managing issues such as supplies, transport and other critical infrastructure and capabilities.

Haiti showed that facilitating a mission network a function by the military can have significant benefit to the overall response. Inadequate communications capabilities on the ground including the lack of broadband internet mean that for many responders

[109] Wentz, ICT Primer, 25.

[110] Ibid., 35.

cannot access large amounts of data including maps and image files.[111] As a consequence of the lack of broadband and networking capability the default communications mode to allow for interoperability is the cell phone. Cell phones operate intermittently and are most effective in text mode but procedures have to be established and cell phones managed to ensure maximum use. In addition capabilities such as internet portals have to be cognisant of the issues and ensure that they are capable of being operated in low bandwidth environments.

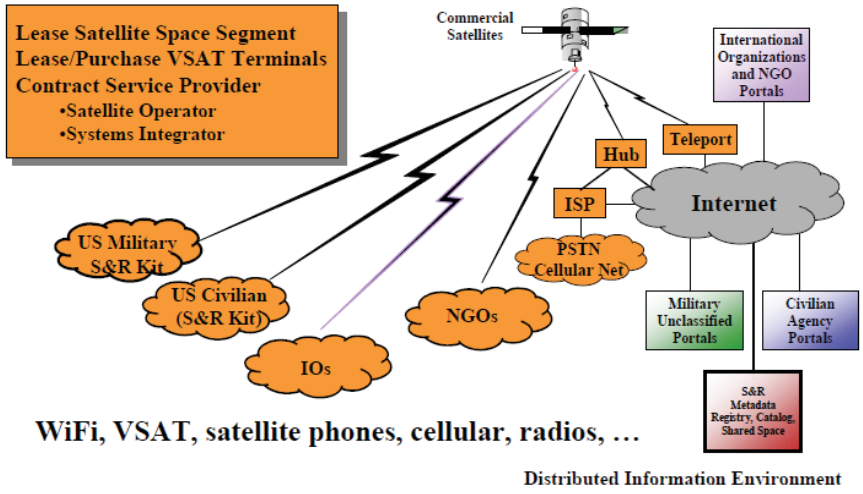

Figure 8. HA/DR Distributed Information Environment[112]

The internet has become the de facto network for information sharing. If a user does not have access to the internet they are not able to access the majority of information being created and are unable to share their own data. Figure 8 above is an illustration of the way that traditional HA/DR activities are now being networked, highlighting the internet at the centre of all systems and data sources. It is relatively easy and quick to establish internet access and many satellite options are no available to access the internet in a

[111] Ibid., 35.

[112] Ibid., 55.

situation where terrestrial communications has been damaged or destroyed by an event. In addition many Government and Non-Government organisations have networks that are routinely connected to the internet meaning it is a very effective network over which to connect multiple agencies together.

By establishing internet communications, the military can facilitate the flow of information in the same way it facilitates the flow of physical equipment and supplies. It has highly trained information technology individuals that can assist with the rapid deployment and operation of information technology. It has the ability to aid local telecommunications suppliers with access to key nodes and get them running again. It is able to provide key strategic communications capabilities that would allow for the rapid access to the internet without the need for multiple independent connections and thereby avoiding the inevitable interference problems that arise from multiple communications facilities in close proximity. It is able to provide assistance to the local organisations for the allocation of frequencies with expertise in spectrum management to enable multiple voice and data systems to operate in close proximity in a disaster area.

Haiti also highlighted the risks of implementing complex technology. Lieutenant Colonel Hart commented that "the Command Staff are so busy that often using complex CIS applications is not practical. Things need to be as simple as possible at the operational end."[113] The observations in Haiti show the same thing with difficulties experienced operating complex systems and the sheer level of staff capacity that is required to monitor multiple systems and the confusion that can arise. Lieutenant Colonel Hart went on to observe that NGOs may see military systems with suspicion as it may compromise their perceived impartiality.[114] This implies two critical things, firstly that it is not practical to expect all organisations to be part of a collaborative CIS environment. Further it suggests that the most successful collaboration platforms for HA/DR activities are likely to be non-military and open source, such as Ashahidi and OneResponse, so Defence Organisations need to be prepared to interface into these environments. Secondly these

[113] Hart, interview.

[114] Ibid.

interfaces have to be as simple as possible, pre-planned and developed as an ongoing capability. Finally the most successful collaboration capability will be with the traditional Government support organisations and this will likely benefit any national response. As Lieutenant Colonel Dragicevich observed "the response to the stranding of the container ship Rena in early October 2011 an open ad-hoc IT system was established in the response base in Tauranga into which anyone from Government could connect. This enabled a high level of collaboration, even though it was just simple file sharing and email, because everyone was connected to the same network"[115]. In order to respond internationally a military needs to be prepared to collaborate outside of their systems on open, internet based applications and be prepared to share their information in an unclassified way. In a national event or where there is a significant government response to an international event there will also be significant benefit gained from linking systems or sharing systems to allow collaboration and information sharing.

Harnessing the global population was a key aspect to initial success in Haiti. With modern communications capabilities and the exploitation of networks and Web 2.0 people can be harnessed and a global response can be mobilise. This can be achieved through a number of ways including passive and active responses. Passively the monitoring of social websites can allow spots to be identified that enable monitoring and control of situations. Measuring the density of Twitter or Facebook responses or references in a particular geographical area for instance could indicate a significant area that is potentially a problem. Ongoing multiple Twitter responses in a particular area could indicate water-shortages as the US Marines did when working closely with Ushahidi. The second more active approach is to use global populations to process complex or large amounts of data. The Haiti example showed an international effort translating French and Creole language texts and enabling these to be fed back into the system for the action of HA/DR responders. The New Zealand population has a significant population of Pacific Islanders and Asians so it is quite feasible to make use of this as a crowd resource when responding to a HA/DR situation in the Pacific or Asia to aide with providing contacts, information and translation services. The quick adaptation and reprogramming of online tools by

[115] Dragicevich, interview.

organisations such as local telecommunications companies such as Telecom and international organisations such as Google to enable the use of web tools, many of whom are prepared to offer their help in HA/DR situations, is another example.

Changing and adapting organisational culture is critical to achieving networks with other Responders. The military cultural response is to plan internally to manage its own response to the HA/DR situation. Haiti showed that the military needs to get used to operating collaboratively and in the absence of a clear chain of command in a HA/DR environment which is significantly different a war fighting environment where they have a specified role to play and a recognised chain of command. The US Forces in Haiti found they had to take the initiative and find creative ways to assist because there is no overall coordinating body. In essence there is a hastily formed network of ad hoc organisations. There is the need to become involved and join UN cluster type groups who are dealing with information technology. By doing so it is then able to actively apply the expertise and capabilities it is able to bring to the situation. These communications work more effectively if they have been established beforehand.

The culture of the military and non-military organisations, especially aid agencies and NGOs are significantly different and these will impact on the ability to establish and maintain networks outside of national boundaries and with international aid organisations. Aid agencies and NGOs want to maintain neutrality and are suspicious of the military.[116] Militaries are an arm of the Government and often there as suspicions because militaries are acting in accordance with their national government objectives which some NGOs feel may compromise their neutrality in some circumstances. A common perception among NGOs is that "the military is not a humanitarian actor."[117] Because of this, information exchange becomes difficult even after technical solutions are found. These differences, however, do not preclude the ability to exchange information. Where objectives and concerns coincide, effective civil-military cooperation can work. While connections between government agencies, allied militaries and the like can be

[116] Hart, interview.

[117] Wentz, ICT Primer, 27.

expected this need to maintain impartiality often this precludes direct connection between networks of the military and with NGOs where distance needs to be maintained. A humanitarian operating environment needs to be established to help maintain separation and impartiality. Larry Wentz refers to this as the "humanitarian space".[118] Civil and military organisations need to maintain their own networked operating environments but these can overlap or interconnect in specific ways to enable information flow to assist with the common goal of protecting and helping the victims of crisis events. Suitable, protected information sharing mechanisms need to be established and maintain to ensure effective information exchange.[119]

Coordinating with OGAs and NGOs requires a flexible approach to information management and communications security. Civil-military coordination needs to overcome significant differences in culture, language, organisation, training and education, doctrine, planning and analysis, communications and information systems.[120] Old business models and prohibitive policy, however continue to impede the ability to keep up with the "highly dynamic, collaborative needs and requirements of complex operations".[121] As mentioned previously, personal relationships, liaison officers and other informal and face to face mechanisms are a very important part of creating and maintaining effective information flow to overcome the "fog of relief"[122]. In order to bypass the difficulties associated with outdated policy and old business models, "sneaker nets" are established.[123] Sneaker nets refer to exchange of information via exchange of printed material or downloaded material on USB stick for instance and these become the only actual means of collaboration. This undermines the original intent of the policy and potentially does damage in the long run as there are no specific control mechanisms to

[118] Ibid., 28-29.

[119] Ibid., 29.

[120] Ibid., 35.

[121] Ibid

[122] Walsh, Civilian Response Stakeholders.

[123] Wentz, ICT Primer, 35.

track and manage this information exchange. It is important to recognise that this will happen and enable the information exchange in a more effective manner, recognising that this information flow is occurring due to immediate operational needs in highly complex environments, and in the case of HA/DR operations, usually in order to save lives. Recognising this needs to happen and changing organisational culture to allow it to happen effectively becomes a critical aspect to enabling technology to help with HA/DR operations.

Establishing a coordinated, cooperative information environment between civil and military organisations in HA/DR operations is an incredibly difficult and complex task to achieve. Compromise is going to be a critical factor as is collaboration to identify points of where agreement can be reached and areas where there are disagreement. There is also the potential for many organisations to be trying to solve the same issues at the same time and recognising these situations and allowing for eliminate situations where this is occurring is essential. Where resources are limited managing these resources becomes critical and sharing resources becomes critical to avoid redundancy or in the worst case avoiding conflicting use of resources such as demands on satellite bandwidth or radio interference.[124]

Connections with local people are as critical as networking across the responder community. This goes for both the local government and non-government organisations as well as with the victims and local people themselves. Communication with the local government proved to be a critical enabler in Exercise Tropic Twilight. The Knight Foundation report also identified that "the two-way flow of information between responders and affect populations is a critical element in humanitarian response."[125] As identified by Lieutenant Colonel Hart, there is no substitute for communications with the locals in situ and if this can be achieved face to face then even better, observing that "face to face communications with the local organisations is critical".[126] The military can

[124] Ibid., 44-45.

[125] Nelson, Sigal and Zambrano, Media, Information Systems and Communities: Lessons from Haiti. 25.

[126] Hart, interview.

achieve this by placing their Command and Control elements with local Command and Control elements. If this is not possible then well connected Liaison Officers can achieve this, as highlighted by the Christchurch earthquake experience. Good connectivity of systems between the locals and the incoming elements is also critical. However face to face communications is still a critical factor.

Haiti showed that simple communication systems were critical for communicating with the local population in the initial stages of an event. Radio was used extensively, as were cell phones and the internet. The ability for the Defence Force to gain rapid access to radio stations, cell phone networks and the internet is critical to establishing these initial links. Access to communications, and therefore information, is absolutely critical to enable effective command and control early in an HA/DR operations. Information becomes as critical as other needs, such as food, shelter and water because it allows for the effective application of resources. Without forming an understanding of where there resources need to go in a confusing, chaotic environment there is little point having the resources in location in the first place. As was the case in both Haiti and Christchurch the communications systems were down so taking things a step further the military could possibly play a role in establishing communications for the wider response group.

What Could an NZDF Response Look Like?

The response to an HA/DR relief using Web 2.0 technology by the NZDF can be broadly grouped into three phases. Initially the organisation needs to be operating in a Web 2.0 environment. The culture of the organisation and the information resources it use have need to meet the needs of providing a Web 2.0 response. The second phase is the response itself and providing support to enable the exploitation of technology as a multiplier to the effectiveness of the response. Being able to engage with the wider responder community and incorporate them into wider community networks is a key factor here. Finally, the withdrawal from an area after an HA/DR response is critical to ensure that CIS critical infrastructure support remains to minimising the impact of the withdrawal of military capability.

Initially the NZDF needs to ensure it's strategic and deployable CIS systems are capable of be used to respond to an HA/DR activity using Web 2.0 type capabilities. This requires some specific capabilities that are not yet in existence. Firstly the ability to operate widely across the internet as a planning tool is necessary. The Internet is the de facto medium for a civil-military Collaborative Information Environment and as such the ability to use the internet beyond just email means that collaboration across Military/Civilian Boundaries becomes more feasible. Civilian and military ICT capabilities share commonalities stemming from deployment of commercial ICT products and many initiatives, such as the US Military APAN network use the internet as a means of access. By having a network that facilitates information sharing at the unclassified level in addition to traditional military networks the NZDF opens itself up to enabling collaboration across organisational boundaries. Once it has the network capabilities it then needs to have the tools necessary to meet collaboration requirements.

Pre-established agreement to use online web portals are important. APAN, for instance, contains a broad range of Web 2.0 collaborative tool that provides all these capabilities and is able to assist with online across multiple agencies both nationally and internationally. It is one of many and it is quite feasible that the NZDF of the NZ Whole of

Government group develop their own. Stove-piped implementation of responder ICT capabilities and proliferation of web portals impeded relief efforts in Haiti by adding unnecessary duplication, fragmentation and complexity to difficulties with information discovery, information management and information sharing. By pre-planning the use of internet based portal systems and standardising on one or a few portals for the use of the majority of information sharing where New Zealand forces and/or Government Agencies will be the predominant elements in the area of operations will overcome some of these issues. It is also important is that the NZDF make regular use of these capabilities so it is familiar with the networking advantages of Web 2.0 type technologies before a disaster occurs. What is the key here though is that responders have to be used to the tools to make best use of them. As the Haiti example showed, ad hoc implementation after the event has its risks. It is not possible to do this in isolation and in order to take advantage of the network effects achieved by Web 2.0 cross boundary networks have to be grown. It may only feasible to negotiate within national boundaries initially thought there are a variety of forums where international agreements can be achieved. One such example is the Multinational CIS Interoperability Program (MCIP).

Engagement with key Asia-Pacific forums will enable engagement with regional countries and key participants in HA/DR responses and allow for the establishment of relationships with key participants in operations and plans type roles. The US Forces sponsored MCIP is almost exclusively focused on HA/DR activities and developing CIS support plans and principles for HA/DR events between regional militaries and was also the major instigator behind the establishment of the APAN portal which was used to great effect in Haiti.[127] Engaging with likely partners in HA/DR situation such as with UN OCHA and the ITU emergency ICT response elements and regional ICT organisations, such as within ASIAN will enable the military to establish a more informed understanding of and working relationship with these partners. The UN OCHA have a working group on emergency telecommunications (WGET) and run a UN OCHA Emergency Telecom Cluster concept[128].

[127] Drybrough, Interview.

[128] Wentz, Haiti Information and Communications Observations, 42.

Involvement with these groups would enable better development understanding of them and would help with the establishment of working relationships.

Sponsoring or participating in both realistic desktop and physical exercises that simulate HA/DR activities is also critical. The benefits of this are two fold. It allows for multiple agencies, both nationally and internationally to enable the growth of networks and to promote the advantages of collaboration and networking using Web 2.0 capabilities. Sponsoring and participating in realistic exercises also assists the NZDF with its own understanding of the internal cultural challenges of operating in an open collaborative environment in rapidly developing, leaderless environments where the NZDF is not necessarily the lead.

The complexity and different nature of HA/DR response operations mean that military force structure and capabilities will need to be flexible to meet the differing demands of HA/DR responses.[129] There is more likelihood that the forces will be operating in small groups and in conjunction with non-traditional partners such as local government organisations, aid agencies, commercial entities and victims. The traditional military communications solutions will therefore not necessarily meet the requirement and the CIS size, shape and function is likely to be different. The key point, however, is that to try and "separate... ...interactions [between the military and other partners] and ignore the need for coordination seems counter productive." By preparing the forces that are likely to deploy to operate on their own initiative, in small groups, within the guidelines of the Force Commanders Intent by interacting with other local agencies with access to critical information as it comes to hand using the collaborative tools of Web 2.0 will likely increase the effectiveness of the response by the military.

Adopting this command and control philosophy and providing the necessary tools to enable breakdown into small teams that are closely coordinated and can achieve self-synchronisation. The Christchurch Earthquake showed that the military is likely to want to operate in small, widely distributed teams. There was also evidence of this philosophy being adopted by the US Marines in Haiti. In order to facilitate this there needs to be a

[129] Wentz, ICT Primer, 33.

paradigm shift in the command and control philosophy to one of collaborative engagement at various levels through the hierarchy backed up by good communications infrastructure. By enabling the hierarchy to be informed and to maintain situational awareness of the activities of small teams and at the same time empower the small teams, working at various levels to other flat and hierarchical organisations will improve the effectiveness of the response. By enabling networking at multiple levels, through the use of communications systems the military is able to leverage the power of networks across organisational boundaries enhanced by a well distributed intent from higher in the hierarchy. Essentially this enables self synchronisation where individual components are aware of the activities of other components around them and are also aware of the overall intent and are able to work in synchronisation with other components or nodes within the network, both inside and outside of the military to enhance and speed up the response to rapidly developing situations. This goes against the hierarchical control mechanisms that exist in the military currently but are, in some ways, in the spirit of operating concepts, such as mission command, that were originally developed to work in uncertain information environments.

Through training, the NZDF culture can then be adapted to enable effective use of technology including operating in hastily formed networks in a collaborative environment. This affects two critical areas. The first is to recognise that the Military is a key information source and be prepared to share information and overcome the risk posed by the use of “sneaker nets” and other issues with informal information sharing. There has to be mechanisms to enable an organisation that is used to operating on classified networks to operating in a relatively unclassified environment. Militaries by their nature operate on classified, highly protected systems. This is extremely important in military type scenarios. In rapid response HA/DR operations this has shown to be counter-productive. There needs to be mechanisms to rapidly declassify information and distribute it widely and to do this quickly to enable the information to be used appropriately. There also needs to be mechanisms for the military to pull unclassified information sources into their own operating environment without too many policy restrictions on access to specific websites such as social networking sites. If there is

significant delay in obtaining access or significant restrictions on the use of the internet as both a communications medium and an information source then this will cause problems.

Secondly the military have to be aware and trained in how to deal with a hastily formed collaborative network where there is probably no organisation specifically in charge. The natural response is to expect an organisation to take the lead and be in charge. This organisation then requests support or provides overall guidance in the same way a higher HQ does in an operational environment. This is possible in a national disaster with an agency like Civil Defence in the lead but in a situation like Haiti where there is a multinational event coupled with the collapse of the local government, a collaborative group approach is more likely. In order to adapt to this environment the military has to know how to deal with organisations such as the UN and their cluster approach. Participants will be suspicious of the military and ignorant to their capabilities. In order to function effectively in this environment the military has to be prepared to become a partner and take the initiative. The approaches taken by various military organisations in Haiti to drive such things as data collection, networked collaboration and mapping show how this is possible and enables not only the effective use of military communications but to leverage of the collective communications capabilities of the responder community to enable a far more effective, collaborative, coordinated, timely response to the crisis situation that has arisen.

From a purely communications perspective it is important to also establish and maintain an understanding of affected nation information culture, ICT governance and ICT business culture. There are ongoing reviews of Pacific Island Nations and the MFAT mission preparedness to deal with crisis such as HA/DR incidents. These reviews sometimes include a communications review but the review is somewhat technical in nature and should be broadened to include cultural aspects of communications. Given the increased capabilities that HA/DR responses in Haiti have shown that communications technology can provide, what is needed is a thorough and comprehensive understanding of the information and communications space, not just a basic understanding of the physical infrastructure. Critical areas include such things as: the primary communications mediums in use by the population and how vulnerable this is to disruption during

disaster; how extensive is cell phone use and the availability, type of cell phone networks are in use and how the network is managed and controlled, particularly from the perspective of an organisation coming in and getting access to use the network; what government ICT exists and how is it used from a perspective of having to re-establish it to move from a relief to a recovery and reconstruction phase; the government mechanisms to control such things as frequency allocation and de-confliction; the penetration of internet into the community including the uptake of things such as social media and social networking sites such as Facebook and languages spoken and the type of languages used during communication. This information becomes critical to planning an effective CIS response and making this information available across the wider responder community will assist in making a response more effective.

A scenario will now be used to illustrate how a response might be formed to make effective use of key CIS capabilities in response to an HA/DR situation. A likely scenario is a tsunami in a South Pacific nation where an immediate response is required to get humanitarian assistance to the Island as fast as possible. The assumption is made that there will be a NZ military along with a New Zealand and international humanitarian response and that the local communications infrastructure is not functioning.

Having previously agreed on and exercised with an internet portal, New Zealand Government agencies start to collaboratively plan for deployment in conjunction with the NZDF. Pre-existing accounts on the portal allow for rapid connection of individuals in key locations across the New Zealand Government and Non-Government responder community. Additional agencies, not previously participants on the portal are able to rapidly join because it is internet based and is unclassified in nature and therefore only requires minimal security and access is granted once the identification is confirmed. These international agencies are encouraged to join because the direct and indirect network effects mean that there is already valuable, easily accessible information online on the portal.

Government contractors and New Zealand telecommunications and IT companies volunteer their help and begin to build interfaces that allow for the implementation of interfaces with other Web 2.0 Social Media such as twitter and facebook. Participants on

the web portal are able to access multiple, internet based, information sources without having to trawl through multiple web sites. The information available allows for informed collaborative planning across the whole of government and keeps other national and international responders informed.

Web 2.0 tools are used for a number of purposes. Online collaborative meetings are held across multiple agencies in New Zealand and recorded so that participants that are not available are able to review the meetings after the fact. Maps are made available online and situational awareness starts to increase as information is geographically placed on the map giving it some context. Military planning is enhanced because requirements can be priorities based on initial assessments. Initial assessment photos from Air Force over-flights are posted online and become instantly accessible by anyone who needs them.

A military group deploys to the Island as part of an advanced party of responders. Access to the internet using small, hand carried, narrow band satellite technology enables the advanced party start passing information back to New Zealand. Information is held in one place and all planners have access to it which ensures that everyone has the most up to date information. Because the planning data is placed onto an internet portal it is available to the wider community to aid the overall planning effort. Data tagging of information using pre-agreed data tags means that information can be quickly accessed and the most relevant information access by the planners. Forces that are in preparation are able to access online blogs from the advance party and prepare themselves with the most appropriate equipment for the situation. Instant messaging enables the deploying Force Commanders to communicate with key people in other agencies, NZDF planning personnel in the Joint Headquarters in Wellington and with the advanced party in the disaster location.

The main forces deploy on the naval ship HMNZS Canterbury, along with relief supplies, including critical communications. The deploying Force is able to keep themselves situational aware during the trip by maintaining close contact with other key players back in New Zealand and on the Island, using the internet facilities onboard HMNZS Canterbury. Ongoing collaborative planning is achieved by using the portal based Web 2.0 tools. This includes real-time voice chat and instant messaging with the advanced

elements on the Island as well as ongoing updates using the situational awareness tools based on the mapping held on the portal. The Force Commander is then able to formulate plans to best meet the situation that is likely to confront him or her on arrival at the Island.

On arrival at the Island the military deploy civilian off-the-shelf communication equipment to key locations across the Island including hospitals, police stations and other emergency responder locations. Recognising that ICT as an essential service, it is prioritised as critical infrastructure during the HA/DR operation and not just an enabler for internal command and control. With enhancements provided by the Internet and Web 2.0 applications the network becomes a significant multiplier during HA/DR the response by enabling networking between responder organisations. The hotspots at key locations are open wireless network access points that enable communication devices such as smart phones, computers and tablets to be connected. These hotspots are then interconnected with each other and connected to a broad-band internet satellite that gives basic internet capabilities across the island. Voice communications is then achieved using smart phones and skype by logging onto the network hotspots and key responders on the island are able to access the internet and start collaborating with the international responders using the online portal facilities. Responders that have arrived without any communications capabilities are able to make use of the military provided internet capabilities. At this stage careful control of the use of hotspots is required. Access to the hotspots is controlled and most internet portal website functions can be delivered via low bandwidth versions of the applications to keep traffic to a minimum.

Military Commanders, who understand the need to form networks quickly, use the rapidly deployed military communications capabilities, the online portal and face to face meetings to establish common interest groups. Operations people are able to communicate and plan operations based on the actions of other agencies and avoid duplication of effort and assisting each other where appropriate. Military logistics people are able to understand the needs of other agencies and start to respond by assisting with the movement of supplies both around the Island and, once the airport is open, from outside.

Internally the Headquarters makes use of Web 2.0 technology to keep itself updated. The headquarters is operating an intranet within the headquarters which enables the utilisation of Web 2.0 capabilities to make the staff function more effectively. Some information is kept internally on the network while others is linked externally enabling the information to be made available to the wider responder community. External information feeds are linked into the network and accessible by staff that need them. Links are setup on the main internal intranet website linking users to important pieces of information and giving structure to the intranet's online content. The most used pages are highlighted as important as the system tracks the information being accessed and as information becomes less important the links to it are automatically demoted or removed from the main pages. The intranet has the ability for key staff to create content to allow them to reach the wider force and an internal wiki creates convergent and accurate content about the operation as users across the force contribute to it. Content is categorised by creating tags that are simple, one-word descriptions by participants as they post content enabling relevant information to be found quickly. Extensions automate some of the work of categorisation and pattern matching of information online through the use of algorithms so that relevant information is presented without the user needing to search for it so when individual users log onto their intranet pages they are presented with information they are likely to need automatically. Signals provided instant notification when there are changes to important content so headquarters staff is kept up to date as information they are interested in changes for some reason. Overall this allows the staff to remain up to date and current and enhances the functionality of the Headquarters.

Small military teams deploy across the Island working independently with the local aid agencies in their locations. The military provide its own internal radio communications as a means of command and control but the with the addition of access to the internet and to the HA/DR portal the teams on the ground have access to the latest situational information from the wider responder community and are able to keep other organisations informed of the situation by providing situation reports and contributing to the common operating pictures held on the online portal. Local commanders are able to make decisions and operate independently because not only do they have access to the

military systems but they also have access to the latest information across the responder community which gives them an idea of the requirements in their area of operation. Because information is held centrally and is created by multiple users it forms a common source of accurate information created through consensus which means the teams are making decisions based on the same information that other organisations have access to.

The Tampere Convention[130] allows responders to rapidly import and operate communications capabilities without needing to follow the normal procedures usually required. While this decreases the time needed to respond it also increases the possibility of confusion, interference and duplication. In order to minimise this confusion the military communications experts make contact with the local communications managers and start to assist with the management of the electromagnetic spectrum to prevent interference across the island by the media, international responders, local communications and the military. This may include interfacing with the UN communications cluster as well as forming a network of interested parties. While this is not entirely successful the impact is reduced because of the rapid uptake of the military provided internet services and improves over time as the local government begin to function effectively again and gain control of the electromagnetic spectrum.

Military communications experts provide assistance to the local telecommunications companies to fix their infrastructure, aided by international donations of communications equipment and expertise. Priority is initially focused on the cell phone network which is eventually re-established and responders are now able to make use of this network for day to day coordination and management of their operations. This has the short term benefit of relieving pressure from the military provided capabilities and the long term benefit of beginning to re-establish revenue for the local telecommunications company which will contribute to the recovery of the Island. There is an ongoing dependence on the military internet capabilities and the internet portal remains a critical tool for ongoing collaboration and cooperation between responding agencies. Priority is then shifted to

[130] Intergovernmental Conference on Emergency Telecommunications (ICET-98), "Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations.", (New York: United Nations, 1998).

re-establishing local internet facilities to reduce and eventual cease reliance on the military provided network.

Once the cell phone network is established the local population begin to call for help. The local radio networks are used to publicise a text number that the local population can text into. This information is automatically entered onto a database for review. There are a significant number of local language texts which require translation so crowd sourcing back in New Zealand, utilising the Island's New Zealand based community, is used to rapidly translate the texts into English via online social media such as Facebook.

Social media such as Facebook and other social media, video and picture websites (such as YouTube and Flickr) provide valuable opportunities for public relations. Using these sites information is shared with the wider international public. They also provide a conduit for individuals to communicate where other avenues may have been cut off for some reason. The use of personal blogging provides information back to those that were following on, giving them critical information to enhance their situational awareness prior to them moving into the area of operations. Families in the international community are able to make contact with their loved ones and make contact with international aid agencies about lost relatives. Monitoring the content of social media sites and analysing the concentration of similar messages or information in specific geographical areas enables the military to identify potential target areas and deploy military assets to assist.

The Military Forces will eventually need to withdraw from the area of operation. It is critical at this juncture that the withdrawal does not affect the ongoing relief and subsequent recovery efforts. It may be appropriate to have mechanisms in place to handover the internet capabilities to the local telecommunications companies as part of the overall aid relief package. Planning with those agencies that are making use of military provided communications facilities should ensure that these agencies are capable of continuing their operations as they transition into the recovery phase of the HA/DR situation. Assisting the local telecommunications companies to recover from the disaster will also assist with this process and provide revenue into the Island to assist with the recovery. Ongoing access to the web portals may also be required for extended periods of time so clarity around the longevity of the facilities pertaining to the portal is

important. Transition to other more appropriate portals that are recovery focused, such as the UN portal oneresponse.info, may also be appropriate.

This example has painted a picture as to how the NZDF might adapt the commercial concepts of Web 2.0 and the subsequent network effects to achieve a more collaborative and therefore more effective response to a HA/DR incident. It requires a shift in focus from not only internal command and control support to the deployed elements but to a collaborative, outward looking focus where the NZDF focuses on leveraging the Web 2.0 network effects to increase the effectiveness of a response to an HA/DR incident as well. Military responses to HA/DR incidents have been common in the New Zealand area of interest in the South Pacific and South East Asian region and New Zealand has also suffered a number of HA/DR incidents onshore. This is likely to be an ongoing state of affairs and being able to achieve a rapid and effective response to these incidents will potentially aid the NZDF to contribute to an overall response and as a consequence save lives and minimise damage to the environment.

Bibliography

2nd Engineer Regiment. “Post Activity Report: Exercise Tropic Twilight 2010.” Linton: New Zealand Defence Force, 24 September 2010.

Australian Defence Force. ADDP 00.3 Multinational Operations. Canberra: Australian Defence Force, 2011.

Australian Defence Force. ADDP 3.8: Peace Operations. Canberra: Australian Defence Force, 2009.

Australian Defence Force, ADFP 6.0.1.1: CIS Planning. Canberra: Australian Defence Force.

Barber L. and Lord C., Swift and Sure: A history of the Royal New Zealand Corps of Signals and Army Signalling in New Zealand. Wellington: New Zealand Signals, 1996.

Clarke, Tim, interview by Liam Jones. National Crisis Management Centre Communications (9 February 2012).

Combined Communications-Electronics Board. ACP 200(C): Maritime Tactical Wide Area Networking. Washington, DC: Combined Communications-Electronics Board, 2010.

Denning, Peter J, and Hayes-Roth, Rick. “Decision Making in Very Large Networks.” Communications of the ACM, November 2006, Vol. 49, No. 11: 19-23.

Denning, Peter J. “Hastily Formed Networks.” Communications of the ACM, April 2006 Vol. 49 No. 4: 15-20.

Dick, Murray, interview by Liam Jones. Interview about the introduction of C-Band into the NZDF, 2012.

Dragicevich, Paul, interview by Liam Jones. 1 Signals Regiment Perspective of HA/DR Communications Support, (2012).

Drybrough, James, interview by Liam Jones. NZDF CIS Support to HA/DR Operations from a Joint Headquarters J6 Perspective (2012).

Dryburgh, Jim. “New Zealand Army's Command and Control (C2) Battle Lab” Asia Pacific Defence Forum. 2010. http://www.asiapac-defenceforum.com/2010-presntations.aspx (accessed November 12, 2011).

Dye, Jessica, “Collaboration2.0: Make the web your workspace” in EContent (Jan/Feb 2007), 32-36.

Elton, Buck. “Haiti: Boots on the Ground Perspective.” Small Wars Journal, 2009.

Foreign Affairs Defence and Trade Committee. Questions for Written Response - 2007/2008 Financial Review: NZDF. Wellington, 26 March 2009.

Fraser, Douglas M., and Wendell S. Hertzelle. “Haiti Relief: An international Effort Enabled through Air, Space, and Cyberspace.” Air and Space Power Journal, 2010: 5-12.

Hart, Todd, interview by Liam Jones. Exercise Tropic Twilight (2012).

Heinzelman, Jessica, and Carol Waters. Crowdsourcing Crisis Information in Disaster Affected Haiti. Special Report, Washington, DC: United States Institute of Peace, 2010.

Hinchcliffe, Dion, “Why all the fuss about Web 2.0?” in Infonomics, Jan/Feb 2010, 26-31.

HMNZS Canterbury. “Post Exercise Report: Exercise Tropic Twilight 10 (TTW10).” Auckland: New Zealand Defence Force, 10 August 2010.

Howard, Alex. Web 2.0 risks and rewards for federal agencies. 23 July 2010. http://radar.oreilly.com/print/2010/07/government-20-web-20-risks-and.html (accessed February 23, 2012).

HQ Joint Forces New Zealand. “HQ JFNZ CONPLAN 103: PLAN PACIFIC RELIEF (ISSUE 4).” Wellington: New Zealand Defence Force, 21 October 2010.

HQ New Zealand Defence Force. New Zealand Defence Force. 27 May 2011. http://www.nzdf.mil.nz/operations/deployments/east-timor/history.htm (accessed February 11, 2012).

InfoRM Project. “IMX Training Course.” Wellington, 8 February 2012.

Intergovernmental Conference on Emergency Telecommunications (ICET-98). “Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations.” New York: United Nations, 1998.

Invenio. Inveneo Haiti Emergency Deployment. September 2009. http://www.inveneo.org/mission/.

Koch, Mitchell T. HA/DR Lessons Learnt. Academic, Newport, R.I.: Naval War College, 2011.

Lancaster, Brent, interview by Liam Jones. NZDF Communications Planning for HA/DR Relief Operations (2012).

Lawlor, Maryann, “Web 2.0 Military Style” in Signal, 62, 7 (Mar 2008), 63-67.

Lee, Sang M., Kim T., Noh, Y. and Lee, B., “Success factors of platform leadership in web 2.0 service business” in Service Business. An International Journal (Jun, 2010), Vol.4, No. 2, 89-103.

Levy, Moria, “Web 2.0 implications on management” in Journal of Knowledge Management, Vol 13, No 1 (2009), 120-134.

Mills, Lyle. “Email Response to an Information Request by Liam Jones.” 8 August 2008.

Ministry of Defence. Defence Capability Plan. Wellington: Government of New Zealand, 2011.

Murugesan, San, “Understanding Web 2.0” in IT Pro, IEEE Computer Society, (July/August 2007), 34-41.

Nelson, Anne, Ivan Sigal, and Dean Zambrano. Media, Information Systems and Communities: Lessons from Haiti. Report based on International Relief Agencies Roundtable Discussion, Miami: Knight Foundation, 2010.

New Zealand Defence Force. “Op Christchurch Earthquake: Communications Observations Pd 22 Feb - 4 Mar 2011.” Lessons Learnt. Wellington: New Zealand Defence Force, 19 April 2011.

New Zealand Defence Force. 21 February 2010. http://www.nzdf.mil.nz/operations/hqjfnz/hqjfnz.htm (accessed February 11, 2012).

New Zealand Government. Defence Long Term Development Plan. Wellington: New Zealand Government, 2003.

New Zealand Government. Long Term Development Plan. Wellington: New Zealand Government, 2008.

New Zealand Defence Force, C4ISR Project Capability Requirements Document, 2011.

New Zealand Defence Force. IMX Overview and Progress Update. Wellington, August 2009.

New Zealand Defence Force Deployments. 10 February 2012. http://www.nzdf.mil.nz/operations/deployments/default.htm (accessed February 2012, 2012).

New Zealand Defence Force. “New Zealand Joint Service Plan No 102: Plan Awhina.” DFO 91(1). Wellington: New Zealand Defence Force, 10 August 2011.

New Zealand Defence Force. NZDDP-00.1 Command and Contol in the New Zealand Defence Force. Wellington: New Zealand Defence Force, 2008.

New Zealand Defence Force. NZDDP-3.0: Joint Operations. Wellington: New Zealand Defence Force, 2010.

New Zealand Defence Force. NZDDP–D: Foundations of New Zealand Military Doctrine. Wellington: New Zealand Defence Force, 2008.

NZCTC. “Lessons Learnt Collection: Operation Christchurch Earthquake February 2011.” Post Activity Report. Wellington: New Zealand Defence Force, 20 June 2011.

O'Reilly, Tim. Web Squared: Web 2.0 Five Years On. October 2009. http://www.web2summit.com/web2009/public/schedule/detail/10194 (accessed February 11, 2012).

O’Reilly, Tim. What is Web 2.0. 2005 September 2005. http://oreilly.com/web2/archive/what-is-web-20.html (accessed February 11, 2012).

Piers Reid, "Jointness: Lessons from Recent NZDF Peace Support Missions." in A Joint Future?: The Move to Jointness and its lmplications for the New Zealand Defence Force: The Proceedings of the Third Annual Conference, 26-27 August 2000, Palmerston North, NZ Defence and Strategic Studies Programme, 2000, 43-48.

Schmidtchen, David. The Rise of the Strategic Private: Technology, Control and Change in a Network Enabled Military. Canberra: Commonwealth of Australia, 2006.

Shuen, Amy, Web 2.0: A Strategy Guide. Kindle Version, O’Reilly Media, 2008.

Singh, T. and Cullinane, J., Surfing the rift: The Executive’s Guide to the Post-Web 2.0 World. Kindle Version, CullinaneMedia, 2009.

Slagh, Christopher Lawrence. Managing Chaos, 140 Characters at a time: How the Usage of Social Media in the 2010 Haiti Crisis Enhanced Disaster Relief. MA Thesis, Washington, DC: Georgetown University, 2010.

US Department of Defence. All Partners Acess Network. http://community.apan.org/ (accessed January 12, 2012).

Walsh, Jim. “Civilian Response Stakeholders.” Presentation to the New Zealand Command and Staff Course. Hawaii: Center for Excellence in Disaster Management and Humanitarian Assistance, 22 November 2011.

Walters, Mark, interview by Liam Jones. Major (10 February 2012).

Webster, Kelly L. “Lessons From a MIlitary Humanitarian in Port-au_prince, Haiti.” Small Wars Journal, 2010.

Wentz, Larry, “ICT Primer: An ICT Primer: Information and Communication Technologies for Civil-Military For Civil Military Coordination in Disaster Relief and Stabilization and Reconstruction” National Defence University. June 2006. http://www.ndu.edu/CTNSP/docUploaded/DTP31%20ICT%20Primer.pdf (accessed October 20, 2011).

Wentz, Larry. Haiti Information and Communications Observations. Trip Report, Washington DC: National Defence University, 2010.

Wilkins, Jesse, “Web 2.0: What does it mean and why does it matter?” in Infonomics (Jul/Aug 2007), 10-11.